

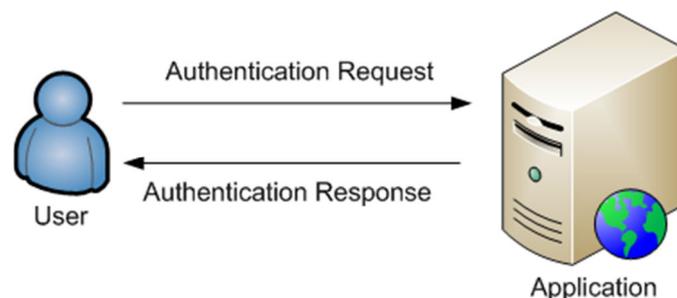
e-ID Federation: Security Token Service implementation using Windows Identity Framework

Today, enterprises have embraced a variety of enterprise applications for streamlining business operations, such as e-mail systems, Customer Relationship Management systems, Enterprise Resource Planning systems, and so on. However, the use of heterogeneous and, frequently, incompatible applications requires users to keep a set of separate authentication identities, resulting in complex and costly user profile management. The complexity of identity management is further amplified as businesses outsource certain operations, requiring agreements between business partners on the secure transport of user information over unprotected networks. Thus, businesses are burdened with increasing administrative costs in identity authentication management and the maintenance of a secure working environment.

Evolving identity management challenges, and especially the challenges associated with cross-company, cross-domain issues, has given rise to a new approach of identity management, known as Federated Identity Management, a set of technologies and processes that let disparate computer systems dynamically distribute identity information and delegate identity tasks across security domains. Federated identity offers users to authenticate once and access different resources from independent organizations through a cross-domain single sign-on (SSO).

The GIC demonstrator

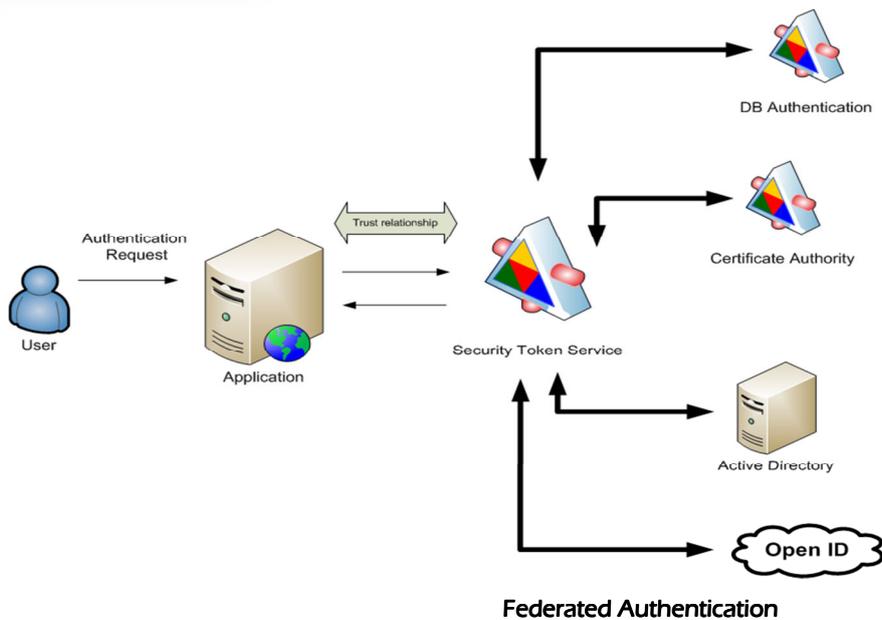
The e-ID Federation demonstrator utilizes the Windows Identity Framework to implement a Security Token Service (STS) that enables identity federation, providing a single sign-on web interface that allows users to authenticate against multiple identity management systems. Specifically, the e-ID STS supports user authentication through certificates, login forms, Windows Authentication and OpenID credentials. The STS assembles user information and provides a common interface for applications to authenticate users and access their profiles and security privileges, regardless of the authentication source. Therefore, the e-ID STS effectively allows disparate applications and identity systems to interoperate, acting as an intermediate security layer that abstracts the underlying authentication mechanisms.



Traditional Authentication

Business Case

Identity Federation significantly reduces the complexity and administrative costs associated with identity management and authentication, by providing a centralized identity management solution that allows applications and business partners to share and exchange user information and security requirements. The e-ID STS demonstrates how Security Service Tokens can be implemented to allow disparate applications and multiple identity management systems to interoperate. Providing a common identity management infrastructure has the added benefit of allowing organizations to outsource certain operations, without fear of breaching information security and privacy.



The World Wide Web Consortium released a report on the future of social networking, citing the need for an interoperable distributed social Web framework.

Interoperability Features

The e-ID Federation demonstrator deals with technical and semantic interoperability issues associated with the portability of identity information across disparate networks and applications. The Security Token Service acts as an intermediate security layer that abstracts the underlying authentication mechanisms and federates security requirements metadata, thus providing a common user authentication interface across multiple systems or organizations, as well as allowing the assembly and federation of user information across multiple identity management systems.

Standards & Technologies

The e-ID Security Token Service implementation is based on the WS-Federation specification, an open protocol maintained by the OASIS consortium as part of the Web Services Security framework, which defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication.

Tools

- Microsoft Visual Studio
- .NET Framework 3.5
- Microsoft Windows Identity Foundation library