

together the distinct systems to a single, distributed, cross-domain single sign-on solution that keeps the customer data secure. Once logged into Insursave, they want customers to have the ability to easily move from service to service.

EXAMPLE 2

[0198] Company A would like to create a joint customer relationship management (CRM) application with Company B. The CRM application requires a customer to have an authenticated identity with both companies. They want to create a simpler model for their joint customers by offering cross-domain single sign-on to either site.

EXAMPLE 3

[0199] Company A would like to simplify employee access to over 12 different internal services. These include expense reporting, travel requests, editing/changing of benefits, access to employee discount services, etc. These systems are run by different web groups, so they would rather use a distributed system to link their different data sources together with single sign-on.

[0200] Having described embodiments of distributed network identity (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed that are within the scope and spirit of the invention as defined by the appended claims and equivalents.

What is claimed is:

1. A method for providing user authentication to a service provider, the method comprising:

receiving, at an identity provider, an identifier that indicates the service provider, wherein the identifier includes an assertion of an identity of a user;

requesting an identity credential from the user;

authenticating the identity credential to produce an authenticated credential; and

passing the authenticated credential to the service provider.

2. The method of claim 1 further comprising:

providing to the service provider user profile data.

3. The method of claim 2 wherein at least one of the receiving, requesting, authenticating, and passing is performed using web services.

4. The method of claim 1 wherein the identity credential comprises a username and a password.

5. The method of claim 1 wherein the identity credential comprises a certificate.

6. The method of claim 1 wherein the authenticated credential comprises a transient token.

7. The method of claim 1 further comprising:

passing an identity provider preference to a common domain, wherein the identity provider preference facilitates selection of the identity provider for authenticating the user.

8. A method for delegating a service, the method comprising:

authenticating a user with an identity provider;

requesting, by a first service provider a ticket from the identity provider for the delegated service, wherein the delegated service is performed by a second service provider;

receiving the ticket at the first service provider, the ticket for authorizing the second service provider to perform the delegated service on behalf of the user; and

presenting the ticket at the second service provider to use the delegated service.

9. The method of claim 8 wherein the ticket comprises a transient token.

10. The method of claim 8 wherein the ticket is encrypted with a key corresponding to the service provider.

11. The method of claim 8 wherein the delegated service is a payment service.

* * * * *