Federation

17.05.2024 11:52:30

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Glossary	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	12:00:23 - 28.06.2010

Schlüsselwörter

identity

Symptom (öffentlich)

Problem (öffentlich)

Lösung (öffentlich)

A method of linking together the Identities of an Entity, to provide shared services as a matter of convenience, efficiency and trust.

The main methods are:
the Gateway / Key-store approach
Identities from different platforms or organisations are permanently related to each other by "keys" that are stored in a centralised vault. Think of non-bank ATMs, or telecom accounts. Identities usually choose to become a member (and can later opt out?) in order to access shared services on a LAN or externally that have been designed with interoperability in mind, usually (but not always) via a single authentication. It may allow the Entity to choose which organisation and which Identity will be used, or there may be a single authentication gateway or portal and a single (new) Identity required. The benefits may be related to only having to do something once, such as change password or mailing address. Depending on the number and type of shared attributes, as the scale of this federation increases their management can become burdensome, and the risks can outweigh the benefits.

the Passport / Wallet approach
This is (or was) similar to the key-store approach but limited to authentication, by a central authority (eg Microsoft). It aims to achieve universal single sign-on to do open and federated authentication among organizations, thus avoiding the user proving an assertion to each participating site. The service may be free to users, but the relying business may pay a fee. There are significant privacy and security issues related to this approach.

the Single Sign-on approach
for temporary access to multiple internet domains, via a single authentication, where separate organisations have agreed to provide common Identities with shared access (and thus provide reciprocal hyperlinks on their web site). Identities usually choose to access the other organisation(s) simply by clicking a link on the web-page of the original organisation. This method re-establishes the trust in each session, and shares a set of common pre-determined attributes between organisations (including identity, channel, location and credential used). It allows the Entity to choose which organisation will be the entry point and which Identity it will use, for each session. For example; SAML assertions.

the Invitation approach
An Identity who is an Owner of a resource invites one or more Identities to accept access to the offered resource (ie to join their user list). Each invitee's positive response creates or updates access, based on a shared identifier, between the invitee's service provider and the owner's service provider. This is actually the federation of the invitee's identity between two service providers, for the specified purpose of using a People Service (PS) web-service. It does not federate the inviter (unless inviting one of its own identities). It is a means of allowing identities that are members of a community of interest (eg a circle of friends) to share resources, without needing to remember the URL, as the hyperlinks will usually not be hosted by either service provider. This approach could also be seen as a combination of both i) and ii) above, but with few (if any) attributes shared; it may become burdensome to maintain if the membership and reciprocation multiplies significantly.

the Open Identity
or "Identity v.2" or "User-Centric" approach, where an entity authenticates itself (maybe even to itself) by choosing which identity it wishes to use this time, and then provides the required attributes to the relying party. Some propose OpenID be based on ownership of a URI/URL, or even a GUID. One of the tenets (and security issues) of OpenID is that there should be nothing installed on the client-side. It embodies the idea that you don't need to be issued a new identity or credential if you already have one that can be trusted (see ID Law 5 in The Identity Laws). Proponents are yet to overcome the question of trust, the lack of incorporation of a formal assurance framework (a common standard assurance is implied), and the legal/policy aspects, before it is applicable to anything other than sites who don't really care who you are. Yadis (Yet Another Decentralised Identity Interoperability System), Sxip, MS-Cardspace and Liberty ID-WSF protocols are related to this approach. But is it a new era, or is it simply an example of the evolution of a generalised federation beyond SAML and single sign-on? And can it become applicable to more than one credential type? This may depend on the degree of support recently announced by Microsoft (see [[glossar#Cardspace|Cardspace]]).

NOTE - Many SSO solutions involve replacing the native Windows GINA logon screen that is invoked at startup or by CtrlAltDel (eg Win2K, XP) with a different one. This is usually done to manage, recover and snynchronise the AD password with other platforms. However that is no longer possible - the GINA concept was abandoned in Vista. You now need to create a "Credential Provider" to run code before a user logs on; the provider object stays alive until the user logs off. You may need to deal with multiple instances (if fastswitch is invoked).

Another common technique for SSO, for browser-based applications, is SPNego (Simple and Protected NEGOtiation mechanism) a Microsoft protocol that allows for HTTP negotiation between the client browser and the web server. Sometimes referred to as 'spengo', and as "Windows Integrated Authentication". The client identity presented by the browser can be verified using Kerberos authentication mechanisms.

Source: http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html