T for a par

Authorisation and access granularity From IdentitySociety Jump to: navigation, search Assertions are ways of extending statements about a person or thing into an action.

Permissions management to data is currently handled in mostly proprietary ways, among tightly coupled modules in a single security domain.

The web, where most peole and data are moving, is loosely coupled, and consists of many security domains. A standard is needed to govern the transfer of assertions between domains.

In Identity terms assertions are most commonly associated with SAML - an XML standard for exchanging authentication and authorisation information across security domains. The content has now expanded to incorporate greater richness and functionality in the handling of identity information. SAML describes three assertion levels:

1 Authentication Statements - the Authentication decision can be decoupled from the more granular permissions management, and in fact this is an important distinction. SAML must be used in the context of a pre-existing trust relationship between asserting and relying parties A Trust relationship may be established using mechanisms such as SSL, signatures, encryption, etc., effectively security frameworks that are not part of SAML - all we need to know to go on and use SAML for more granular access is that the subject was authenticated using a particular technique at a particular time.

2 Authorisation or Attribute Statements particular attribute values are associated with the subject, as a simple example, that the value of the attribute "Department" associated with the assertion?s subject is "Accounting"

3 Authorisation decision Statements: the subjec????t is authorized to perform certain actions, or more precisely, Asserting that the enclosing assertion?s subject?s request for a particular action at the specified resource has resulted in the specified decision ????

The closest analogy is in the entry of a familiar person to your home. The???? Authentication Statement would be sufficient to allow them through the front door.

If you knew them well and they had a specific purpose th????en an authorisation statement may allow them into a specific room (I am Bob, I have come to watch the world cup with you, may I enter the TV room?) If you had a group of people coming to watch the football you ????may not know them all directly. Someone you trust may then provide a supporti????ng Authorisation decision statement (Bob says, t????his is my friend Ted, he is a good guy, he's with me and can join us).

The point with Authorisation statements and Authorisation???? the respective rooms and therefore communities on the web using mechanisms that are commonly recognised and broadly understood.

Helpfully, SAML Profiles define commonplace message exchange patterns that illustrate how SAML assertions can be exchanged to achieve particular goals in a particular context, and in????olving the use of SAML protocols. In our example above of access to the TV room for example, contributing a particular "Profile" or framework for this action.

Authorisation statements are therefore reflective in s????ome ways of people's "personality" in terms of their community access and interaction capability, arguably this is why the subject has such competitive importance and political as well as commercial energy - this is the holy grail of identity and access management in terms of realising a more granular and personalised form of access. </snazzybot>Retrieved from "http://www.identitysociety.org/index.php?title=Authorisation_and_access_granularity"