SMEStorage Appliance Security Integration

The purpose of this document is to describe an approach to security integration with the SMEStorage Appliance.

Ultimately there are many different security mechanisms that organisations use, and the use case below is an example of where the SMEStorage appliance has been integrated into an organisations identity management system

Understanding SMEStorage authentication

SMEStorage provides a stateless REST API to integrate with external systems, this is the same API used internally by SMEStorage and is also used to provide our data access components. A component needs to authenticate the user first with SMEStorage before he can use any of the REST services. A component authenticates a user with SMEStorage by calling a REST service with user's login name and password, after successful authentication a token is returned. This token is passed in all the REST calls to SMEStorage for any operation performed by the component on user's behalf.

The assumption for this whitepaper is that the SMEStorage platform will run on-premise as an appliance and describes one approach to integration.

Example SMEStorage Integration with OAuth

OAuth is an open protocol that allows a user to grant a third party site access to their information stored with another third party site, without divulging their access credentials or even their identity. Designed to complement OpenID industry insiders believe OAuth will play a key role in the development of secure REST-based Web Services.

Components

OAuth Proxy

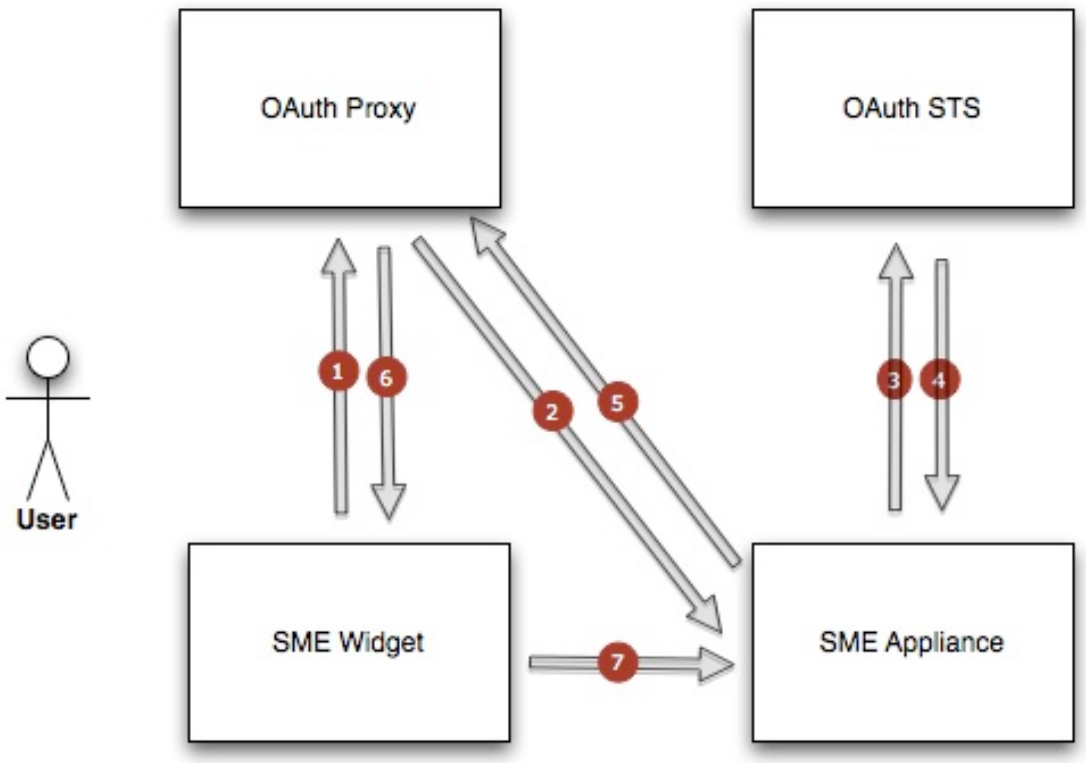
OAuth Proxy is a service that is provided by OAuth security vendors.. This service is passed a REST service URL. The OAuth Proxy adds OAuth headers for the logged in user and call the passed web or REST service and return the response.

OAuth Secure Token Service (OAuth STS)
Decrypts the headers added by OAuth Proxy and returns user attributes including the users identity.

SMEStorage Widget
Refers to a SMEStorage client

SMEStorage Appliance
An onsite appliance that provides an application which encompasses a users access to the federates SMEStorage storage services.

Call Flow



A user logs into an SSO system and is authenticated. The user role is authorized to use SMEStorage widgets/clients.

Lets looks at a flow for such an interaction:

1. The SME widget is invoked and calls the OAuth Proxy by passing the SMEStorage login service URL

2. The OAuth proxy service will automatically add the OAuth headers for the

logged in user and will call the http://smeloginurl hosted on the SMEStorage appliance
3. The SME appliance will call the OAuth STS with the received OAuth headers. This will involve just copying the headers and calling OAuth STS service.
4. The OAuth STS service will parse the headers and return user attributes to the SME appliance including the users identity
5. If the response from STS was successful the SME Appliance will generate the SME token using the user identity, map it to the SMEStorage user and return the token
6. The user is authenticated and mapped, SME has generated the token and returned the token to the widget
7. All the subsequent REST calls to SME appliance from the SME widget will use the returned token for authentication and authorization

Time Estimate

For us to integrate into an OAuth identity management system the bulk of the time will be taken in setting up the environment and testing. We are confident that the integration can be completed and tested in 5-10 working days having had experience of doing this previously.

Additional to this we may also need to change some authentication details on the SMEStorage clients. The time required for this depends on the number of SMEStorage clients required but should not take longer than 3-5 days.

Other Security Models

Other Security models can also be embraced, such as OpenID and Kerberos.

OpenID is an open identity federation standard originally designed to allow consumers to register with one OpenID provider, then use that same identity to log into a variety of Websites. While currently there are a number of barriers preventing widespread corporate adoption of OpenID, security being a primary concern, enterprise adoption of OpenID is expected to expand in the future.

SMEStorage is already expanding it's web platform to enable OpenID authentication to be used for cloud providers that support it.

Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server.

There are a variety of ways that SMEStorage could work with a Kerberos based Architecture. SMEStorage can work with NTLM authentication and can also be setup to enable SMEStorage to authenticate users on Active Directory.