IdPproxy (Social2SAML)

Roland.Hedberg@adm.umu.se

Date

Architectural Model

- Appears as a SAML2 IdP to a SAML2 SP
- Allows for the use of several Services (Facebook, Google, OpenId, LiveID, Twitter) for authentication.
- Maps information received from the authentication service to SAML2 response
- Works more like a WAYF then a SSO service

Information

- Locally stores information about the person.
  - Stored forever but has a valid-until timestamp
- Has a map (SAML SPs -> Social service) for each person.
  - The connection person -> info is cookie based.

Return information

- Configurable mapping of authn service identity information -> SAML assertion
- Information about which social service was used returned in AuthnContext (AuthenticatingAuthority)

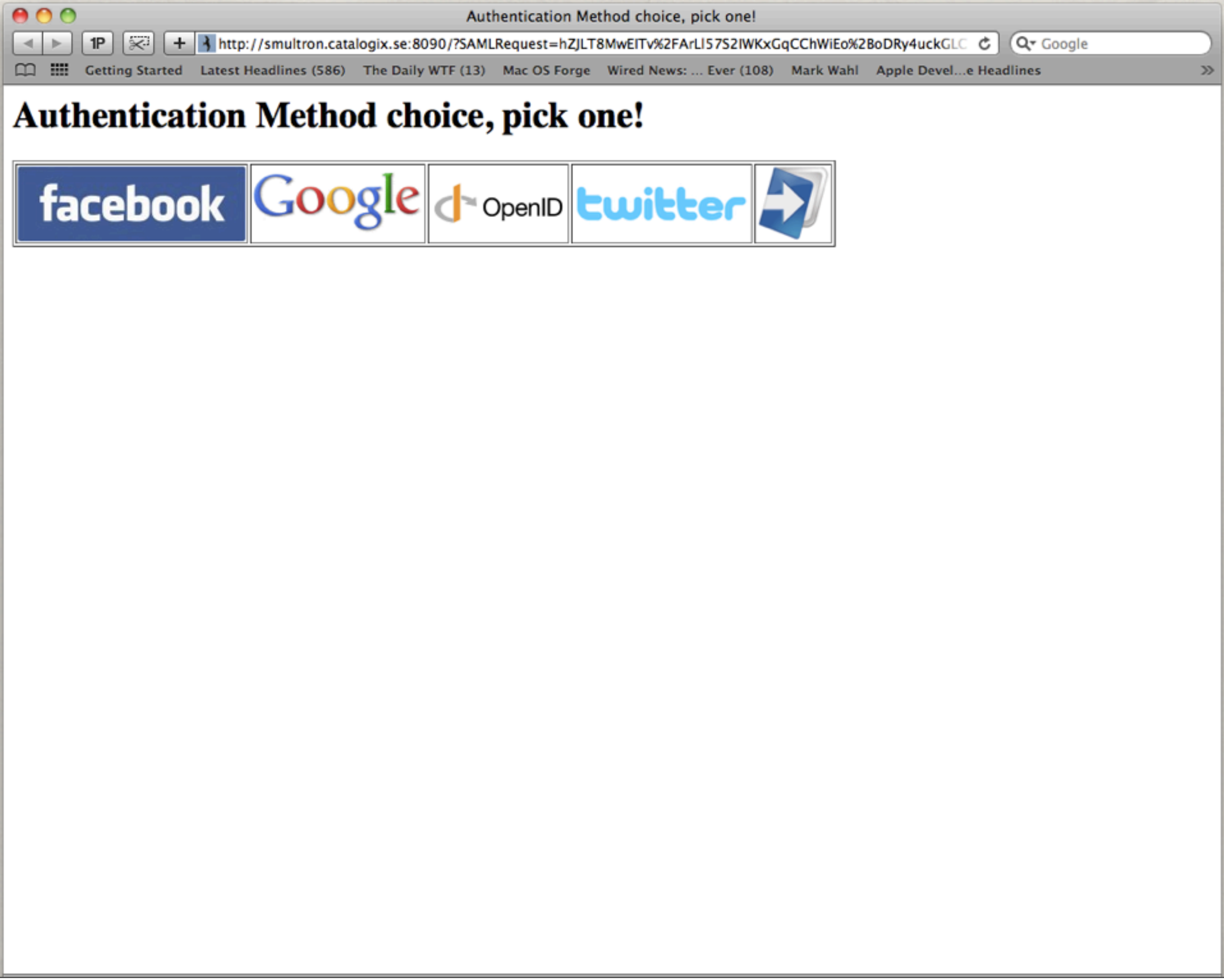
Person identifier

- For the services where the user might know her identifier (Twitter, Facebook, Google) that is used.
- eduPersonTargetedID and eduPersonPrincipalName are always created. Using a 'permanent' identifier returned by the social service

Invitation mechanism

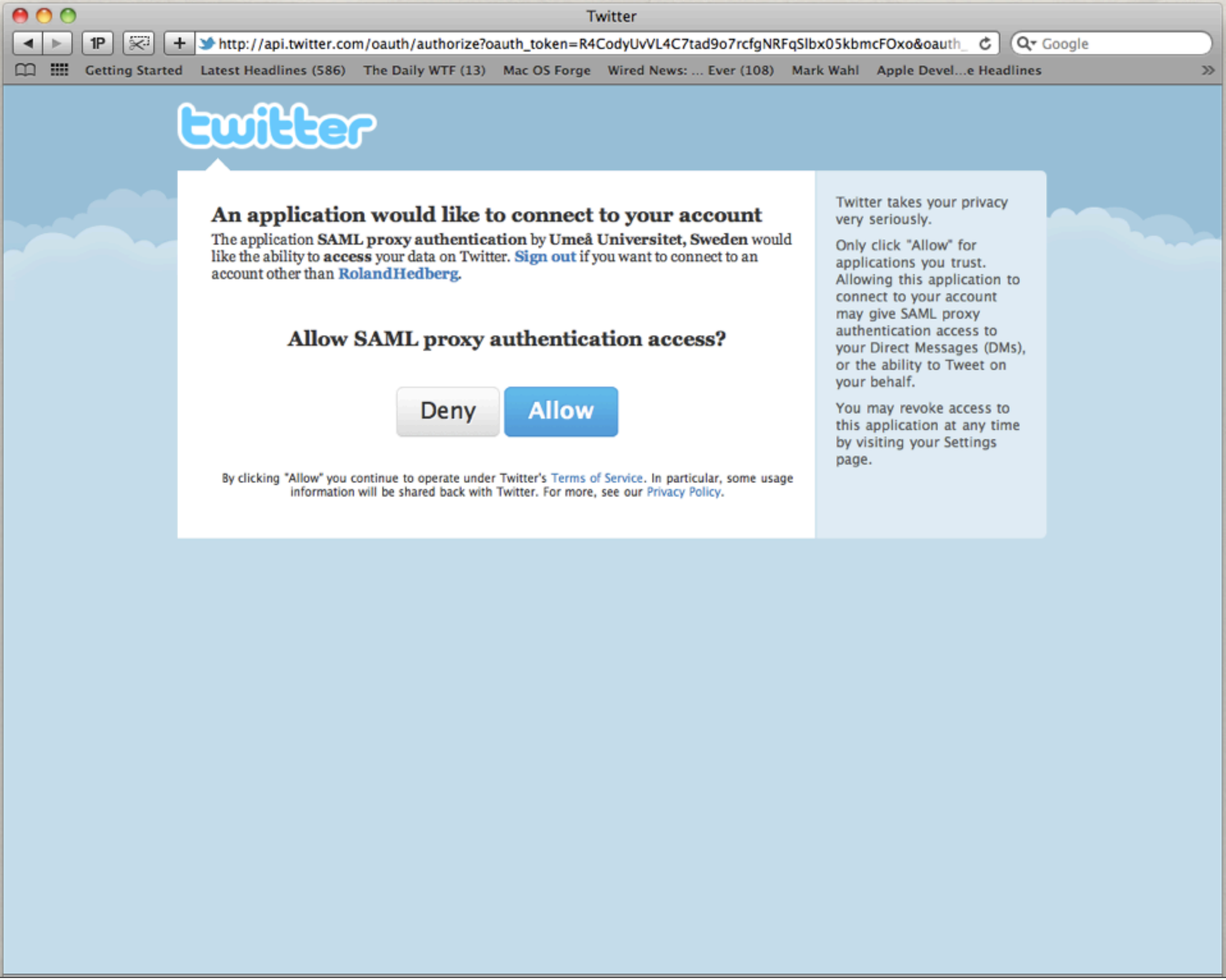
- Not implemented

Demo


Authentication Method choice, pick one!
1P
+
http://smultron.catalogix.se:8090/?SAMLRequest=hZJLT8MwEITv%2FArLl57S2lWKxGqCChWiEo%2BoDRy4uckGLC
Google
Getting Started
Latest Headlines (586)
The Daily WTF (13)
Mac OS Forge
Wired News: ... Ever (108)
Mark Wahl
Apple Devel...e Headlines

Authentication Method choice, pick one!

facebook
Google
OpenID
twitter


Twitter
http://api.twitter.com/oauth/authorize?oauth_token=R4CodyUvVL4C7tad9o7rcfgNRFqSlbx05kbmcFOxo&oauth_
Google
Getting Started
Latest Headlines (586)
The Daily WTF (13)
Mac OS Forge
Wired News: ... Ever (108)
Mark Wahl
Apple Devel...e Headlines
twitter
Deny
Allow

An application would like to connect to your account

The application **SAML proxy authentication** by **Umeå Universitet, Sweden** would like the ability to **access** your data on Twitter. **Sign out** if you want to connect to an account other than **RolandHedberg**.

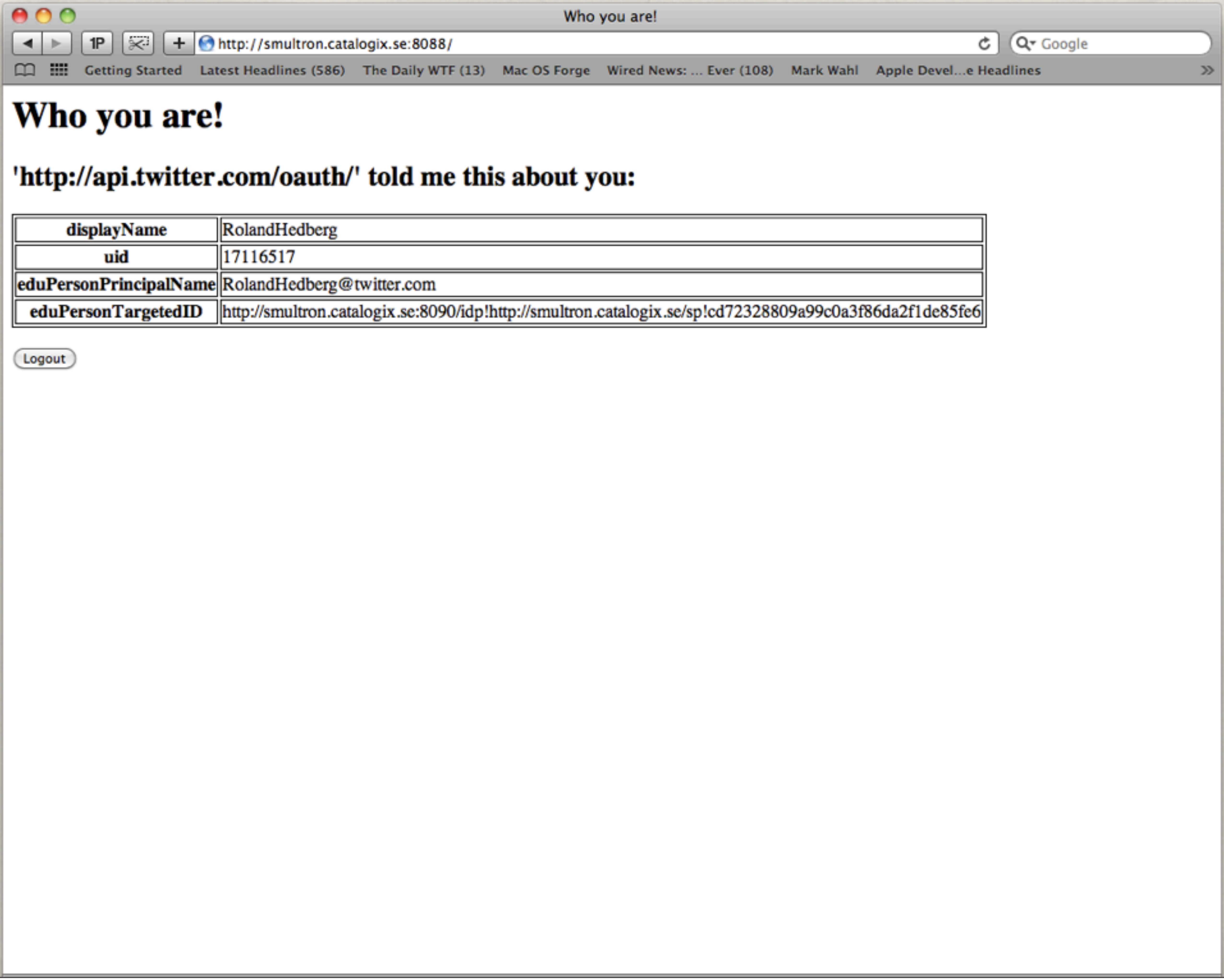
Allow SAML proxy authentication access?

By clicking "Allow" you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy.

Twitter takes your privacy very seriously.

Only click "Allow" for applications you trust. Allowing this application to connect to your account may give SAML proxy authentication access to your Direct Messages (DMs), or the ability to Tweet on your behalf.

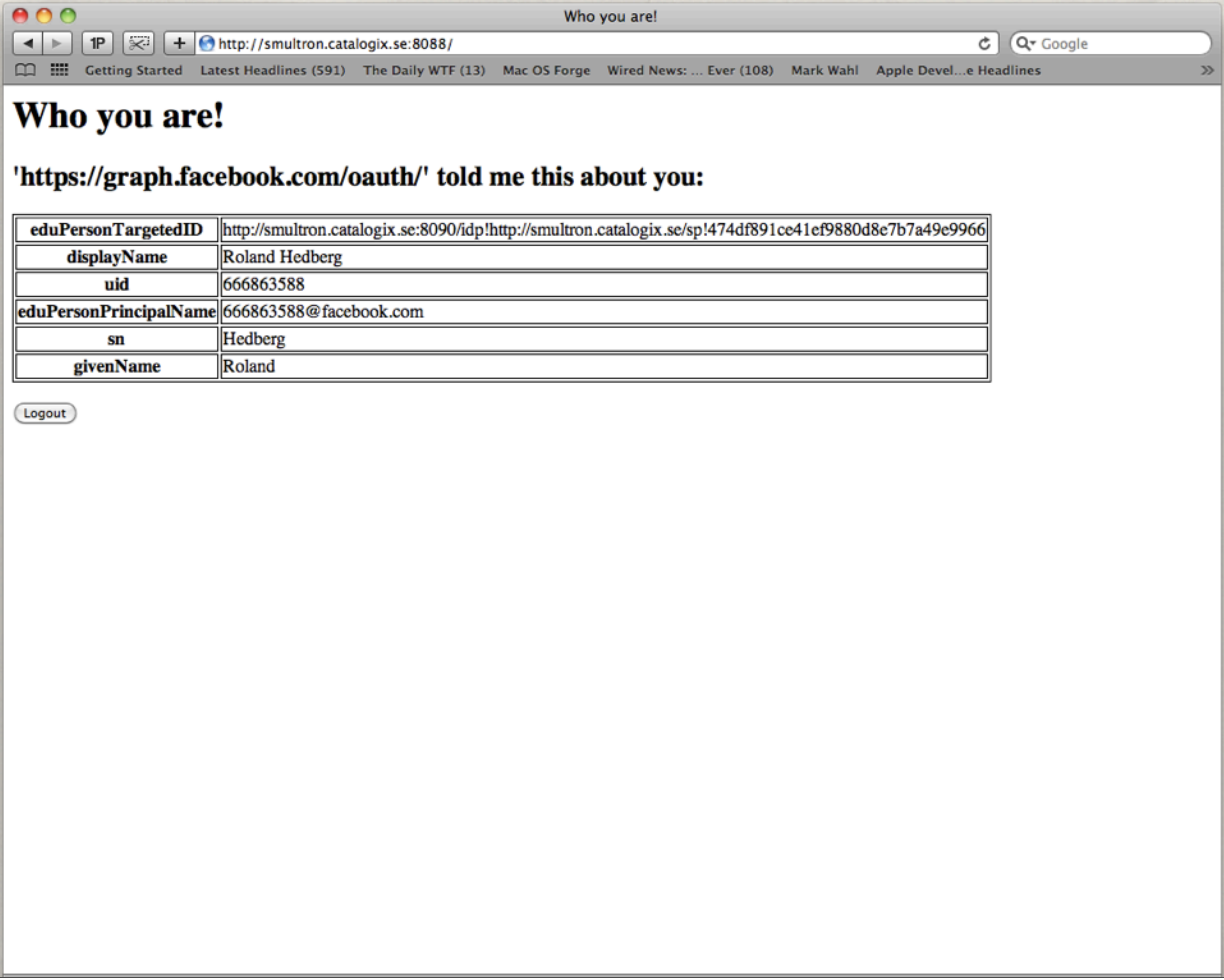
You may revoke access to this application at any time by visiting your Settings page.



Who you are!

'http://api.twitter.com/oauth/' told me this about you:

displayName	RolandHedberg
uid	17116517
eduPersonPrincipalName	RolandHedberg@twitter.com
eduPersonTargetedID	http://smultron.catalogix.se:8090/idp!http://smultron.catalogix.se/sp!cd72328809a99c0a3f86da2f1de85fe6



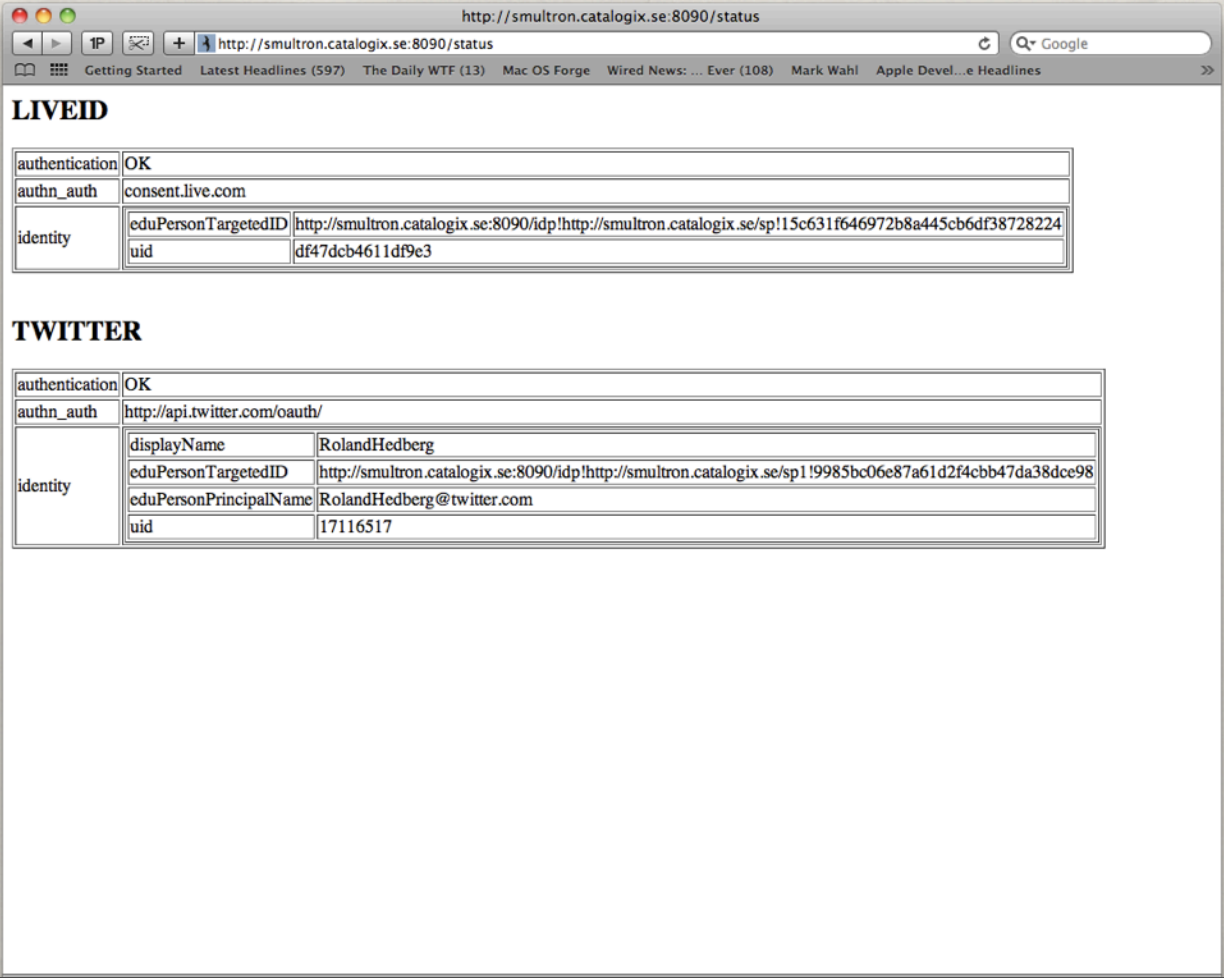
Who you are!

'https://graph.facebook.com/oauth/' told me this about you:

eduPersonTargetedID	http://smultron.catalogix.se:8090/idp!http://smultron.catalogix.se/sp!474df891ce41ef9880d8e7b7a49e9966
displayName	Roland Hedberg
uid	666863588
eduPersonPrincipalName	666863588@facebook.com
sn	Hedberg
givenName	Roland

Status view

- Allows you to see which social services you have used for authentication and what was sent to the SAML SP.



http://smultron.catalogix.se:8090/status
1P
Google
Getting Started
Latest Headlines (597)
The Daily WTF (13)
Mac OS Forge
Wired News: ... Ever (108)
Mark Wahl
Apple Devel...e Headlines

http://smultron.catalogix.se:8090/status

LIVEID

<table>
<tr><td>authentication</td><td>OK</td></tr>
<tr><td>authn_auth</td><td>consent.live.com</td></tr>
<tr><td>identity</td><td><table>
<tr><td>eduPersonTargetedID</td><td>http://smultron.catalogix.se:8090/idp!http://smultron.catalogix.se/sp!15c631f646972b8a445cb6df38728224</td></tr>
<tr><td>uid</td><td>df47dcb4611df9e3</td></tr>
</table></td></tr>
</table>

TWITTER

<table>
<tr><td>authentication</td><td>OK</td></tr>
<tr><td>authn_auth</td><td>http://api.twitter.com/oauth/</td></tr>
<tr><td>identity</td><td><table>
<tr><td>displayName</td><td>RolandHedberg</td></tr>
<tr><td>eduPersonTargetedID</td><td>http://smultron.catalogix.se:8090/idp!http://smultron.catalogix.se/sp1!9985bc06e87a61d2f4cbb47da38dce98</td></tr>
<tr><td>eduPersonPrincipalName</td><td>RolandHedberg@twitter.com</td></tr>
<tr><td>uid</td><td>17116517</td></tr>
</table></td></tr>
</table>