

Comparison of Alternative Federated Wireless Authentication Strategies

Comparison of Alternative Federated Wireless Authentication Strategies

This page provides pros and cons for the three federated wireless authentication strategies discussed in [UCTrust Wireless Notes - 2010-07-26](#).

	eduroam	ucroam	Captive Portal
Contact information	Eduroam provides only minimal contact information to the hosting campus. This may cause problems in the event of infringement notices, legal investigations, and or vulnerabilities detected in guests' computers.	ucroam could be built to support sending contact information. This could cause problems for future interoperability with Europe, because of their privacy laws. Depending on the authenticating campus to send supporting details may not be viable.	UCTrust Wireless could be built to support sending contact information. This would not cause interoperability problems with Europe, as Shibboleth can obtain end-user permission to release contact information. NOTE: This is dependent on the structure of the authenticating site's Shibboleth service - it may not be a generally true statement
Campus readiness	UCD will likely join eduroam, as will UCLA. UCB and UCR do not currently support 802.1x, a prerequisite for eduroam.	UCD and UCLA should be able to join without much effort. UCB and UCR do not currently support 802.1x, a prerequisite for ucroam.	UCLA has integrated Shibboleth into a test/demonstration captive portal but would need to add attributes for contact information. Other campuses would need to integrate Shibboleth and the contact attributes.
Automatic presentation of host campus policy, etc.	The 802.1x technology used by eduroam does not include an automatic presentation of policy and other information about the host campus. Presenting such information could be done by associating a captive portal with the 802.1x guest network. (This may be precluded by eduroam policy.)	The 802.1x technology that would be used by ucroam precludes automatic presentation of policy and other information about the host campus.	The "captive portal" technology that would be used by UCTrust Wireless would allow host campuses to present arbitrary information at login time.
Consistency of user experience	Access would be the same regardless of location	Access within UC would be the same regardless of location	Experience would vary in every location; access method in some locales may be less than obvious
Breadth of solution	Global	UC	UC
Participation in larger community	UC would be part of a global effort	UC would be copying a global effort, but limiting extent to UC	UC would be going it alone
Ease of implementation	Trivial (or next to it) for environments already running 802.1x and RADIUS	Trivial (or next to it) for environments already running 802.1x and RADIUS; more configuration work than with eduroam	Potentially significant portal code development; likely significant coordination work for SAML attribute sharing
Global benefits to users	Users gain access to eduroam hot spots world-wide	none	none