Deployments have encountered use of 1.6 to 1.9 applications per login session, and logout, when supported, is only used by roughly a quarter of users. While deployment of applications and user education may make a difference, this raised questions about the value of a WebISO to the user community.

There are multiple approaches to who can run a client WebISO server based on campus structure; application servers may need authorization to do so, or anyone can run a client server.

Backup servers and hot fail service are important since authentication is a critical campus function; however, load balancing may not work in some architectures.

One of the benefits of a WebISO is that no additional client application needs to be deployed beyond a functional browser.

Different identifiers may be useful in different instances, and delivery of just an identifier may be insufficient or excessively identifying, depending on the application; linking the WebISO system to the LDAP directory is useful to supply more attributes or other identifiers if applications can understand them.

Nobody has seen a browser hack or a browser mishandle a cookie so badly as to release one that's not supposed to be released, and if a WebISO application server is compromised, the infrastructure itself is generally safe.