What is it about?
HTTP cookies are the commonly used method for Single Sign-on (SSO) session identification, but the usage of cookies have some known weaknesses like XSS or CSRF. Unique-Session binding use the SSL/TLS resume-session functionality to reuse an old SSL/TLS session. This project will investigate how far Unique-Session binding can be used for SSO session identification.

Goals?
» Analysis of Unique-Session binding
» Analysis of SSL/TLS resume with respect to browser and web-server support
» Demonstrator

Skills?
» Basic knowledge of SSL/TLS and Single Sign-on.
» Scientific methods
» Interest in the development and implementation of new concepts

Contact: thomas.lenz@egiz.gv.at