Does OCLC have to share a key for encrypted SIP2 connection?

Last updated: Fri, 15 Jan 2021 16:03:40 GMT

Applies to

- WorldShare Circulation

Answer

For SIP2 connection, OCLC does not use any encryption key. The server is a simple IP authentication only. For encrypted connection, you need to run SSL tunneling software, such as stunnel, locally, configure that to connect to the WMS SIP2 server, and then configure the SIP2 device to connect to the SSL tunneling software. This will then allow an unencrypted connection from the SIP2 device to the SSL tunneling software to be converted into an encrypted connection from the SSL tunneling software to WMS. All of this set up is done locally, and no keys are passed between you and OCLC.