Security in XL-Connector (formerly Enabler4Excel)

SECURITY ASPECTS OF INTERACTING WITH SALESFORCE.COM USING XL-CONNECTOR ADD-IN

XL-Connector Overview

XL-Connector is a COM add-in to Microsoft Excel created using the following technologies:

- Microsoft .NET 4.5 platform
- VSTO (Visual Studio Tools for Office) 2010 interop assemblies for interaction with Excel spreadsheets.
- Partner WSDL for communication with the Force.com platform using SOAP API v. 56 (with every Salesforce release the solution is rebuilt to support the latest API version).

Authentication with Salesforce

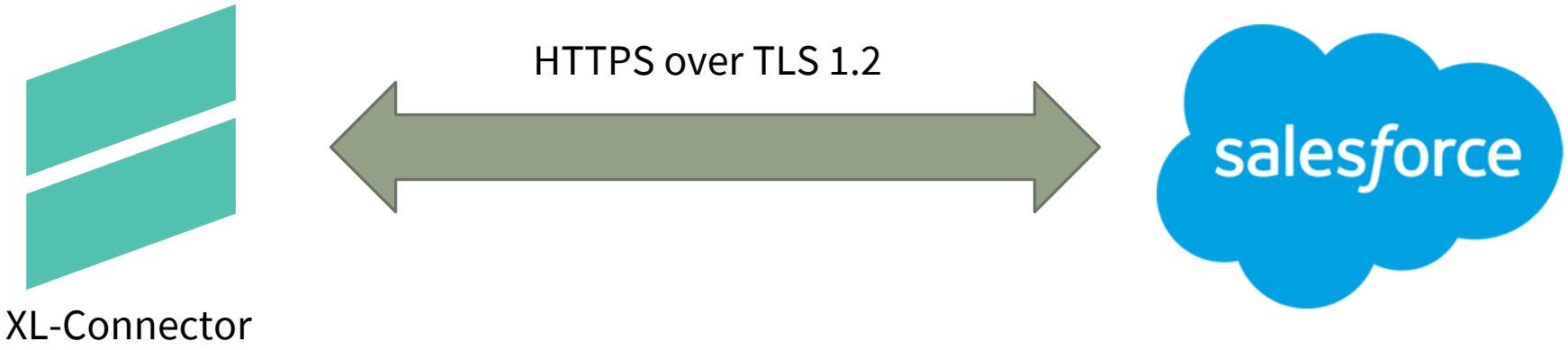
XL-Connector uses three types of user authentication with the Force.com platform:

- Auth2 client-server authentication – takes the user to a salesforce.com login url to authenticate using their username and password. If authentication is successful the user is granted an authentication token that is used throughout the user session with salesforce.com
- 2-factor authentication with username, password, and security token previously generated by the user from their Salesforce.com account.
- Single Sign-On Authentication – takes the user to the single sign-on provider to authenticate and if successful, redirects to the Force.com authentication page to grant an authentication token.

Secure transactions

After a successful authentication with Salesforce.com, access to data is controlled by the Role/Profile combination of the specific user. Roles and profiles are assigned to users by their Salesforce admins.

All communications between XL-Connector and Salesforce.com are encrypted, performed over a secure HTTPS connection over the latest TLS protocol enforced by Salesforce (at the moment of writing this it's TLS 1.2).



Secure local storage

XL-Connector users have the ability to remember their login credentials to facilitate easier log in to different Salesforce instances.

To achieve this, sensitive user information (password and security token) is stored locally in a settings file. All user sensitive information that is written to a settings file is first encrypted to prevent unauthorized access in case an attacker gains access to the user's computer.