

TYPO3 Single Sign-On

Ekkehard Guembel, net&works GmbH

A net&works TYPO3 Partner Network Whitepaper
<http://typo3.naw.de>

This document is published under the Open Content License
available from <http://www.opencontent.org/opl.shtml>

The content of this document is related to TYPO3
- a GNU/GPL CMS/Framework available from www.typo3.com

Introduction

TYPO3 Single Sign-On provides seamless integration of Third Party (i.e. non-TYPO3) Web Applications into the TYPO3 frontend. This includes

- access to "Third Party Applications" (TPAs) with no additional logon (for authenticated TYPO3-users),
- role-based integration of the TPAs into TYPO3 navigation or content,
- a sophisticated three-layer security architecture,
- no need for server-to-server communication, no need for central reverse proxies
- no need for a common/shared/synchronized password database or even user database.

Architecture

TYPO3 Single Sign-On allows direct access to the Third Party Application (TPA) by securely passing a one-time-token to the browser (via URL). Thus, TPAs may be distributed across the net.

Basically, we find a 3-layer architecture:

- TYPO3 dynamically creates a link that includes the desired TPA, user name, and various security information.
- The SSO Agent, located on each target system (the machine where the TPA lives), validates the incoming browser request, talks to the TPA Adapter, and gives back an HTTP redirect to the browser that points to the TPA itself.
- The TPA Adapter is invoked by the SSO Agent. It creates a valid user session ("logs on the user") by application-specific means, and returns all information needed to the SSO Agent (in a defined format).

This adapter is TPA-specific - this means that you need to find or develop an appropriate adapter for every TPA that you wish to integrate. It may be written in any language you favour.

See www.single-signon.com (available after the TYPO3 extension has been released) for existing TPA adapters.

Security

Security has been the major objective throughout the development of the TYPO3 Single Sign-On extension. As of today, a carefully configured system is considered safe due to the following measures:

- No TPA passwords are stored in or even known to TYPO3 and the SSO Agents.
- The SSO Link (providing TPA access without password) has a limited lifetime (configurable).
- The SSO Link cannot be faked (it is signed by the TYPO3 server using an OpenSSL signature).
- Each SSO Link can only be used once (replay protection).
- Since the transmission of the SSO Link should be protected (otherwise it may potentially be wiretapped and used by an offender), the usage of SSL can be enforced by the TYPO3 extension.

Single Sign-On is complex business by nature, so please make sure to read and understand the documentation including the "additional security measures" section before using it in a life environment.

Licensing and Availability

TYPO3 Single Sign-On is a free and Open Source extension to TYPO3.

It is scheduled to be released during the 2004 CeBIT exhibition in Hannover, Germany.