Signature Based Single Sign-On Framework

Documentation Sheet

SSO Agent –php-

The content of this document is related to the
Signature Based Single Sign-On Framework
available from **www.single-signon.com**

Product Website	http://www.single-signon.com
Version and Status	0.61
SSO Frame-work Version	1.0
Author	D. Heise, net&works GmbH sso (at) naw.de
License	GPL
Verified to Work with SSO-Server Versions	TYPO3 : **Single Sign-On** (naw_single_signon) 0.1.3
Prerequisits	• OpenSSL, preferrably compiled into PHP [otherwise the OpenSSL executable currently needs to be in the searchpath of the webserver's uid] • currently only tested on Unix Servers. • currently only tested with Apache.
General Remarks	
Installation + Configuration	Download sso-agent-php_latest.tar.gz unpack where needed (depending on your implementation) cd htdocs tar -xzfv sso-agent-php.tar.gz This will extract sigsso.php and sigsso.conf to the current directory. set the file access rights as needed Example (Unix): chmod 500 chown wwwrun:nogroup sigsso.php Now you need to deploy the OpenSSL public key file from your SSO-Server. You may put it in any place accessible from the SSO Agent. Finally, configure the SSO Agent.

Although by time there may be more then one implementation of the SSO Agent, there is a common set of configuration options, typically to be defined in a file called sigsso.conf.

In the current sigsso.php, the location of the config file is coded in the php script. To change the location, you need to change the line

```
$configfile="/usr/local/sigsso/etc/sigsso.conf";
```

to the proper value.

The sigsso.php configuration file is divided into subparts:

```
[global]
[errorcodes]
[main]
```

Every part has different options and values, separated by a colon (":"). Whitespaces (blanks etc.) are allowed.

Comments are prefixed by the pound sign ("#").

SSO Agent - The [global] Section

Key:	Possible Values:
loglevel	0: no logging 1: errors (tpa_id + user) 2: success and errors (tpa_id + user) 3: errors (tpa_id + user + expires + signature) 4: success and errors (tpa_id + user + expires + signature)
public_key	/path/to/your/public.key
tokensfile	/path/to/your/tokensfileused to store the data of used links
logfile	/path/to/your/logfile

[configuration of sigsso.conf, [global] section]

Example:

```
[global]
loglevel:2
public_key: /path/to/your/public.key
tokensfile: tokensfile.txt
logfile: sigsso.log
```

sigsso.conf [main] section

For each TPA_ID (as configured in the Single Sign-On content element in Typo3), you need to add one line here.

Currently this SSO Agent supports two types of TPA Adapters: command line and PHP scripts.

The syntax for command line scripts is

<tpa_id> followed by ": cmd://" (colon, some optional whitespace, "cmd", colon", slash, slash) and the system call to the TPA Adapter, including parameters.

The syntax for PHP scripts is identical, but "php" instead of "cmd".

Normally, each call will require specific parameters, some of them dynamic (i.e. server variables). These can be given, represented by keywords in percent signs. Currently, the following variables are supported by this SSO Agent:

Variable Name:	Explaination:
%remote%	The IP address of the browser
%agent%	The browser's user agent identification string
%user%	The user name to be logged on to the TPA

[configuration of sigsso.conf, [main] section, cmd:// call]

Example (command line invocation):

```
[main]
MyOwnApp: cmd:///usr/lib/java/bin/java /path/to/tpa_adapter --remote_addr=%remote%
--url=https://redirect.url/index.jsp --uid=%user% --moreparameters=anything_you_need
```

Example (PHP invocation):

```
[main]
MyOwnPHPApp: php://www/my/script.php --url=https://redirect.url/index.jsp
--moreparameters=anything_you_need
```

The PHP-based TPA Adapter does not need to receive the server variables (as listed above) explicitly, since the PHP script will be included and thus the parameters are available directly to the TPA Adapter.

SSO Agent - The [errorcodes] Section

This section allows you to override the default messages that are displayed to the browser in case of an error.

Instead of a different message text, you may also give a URL to redirect to; this is recognized by the leading "http://" or "https://".

The following table gives the keyword and default message text for each error situation:

Key:	Default Value:
user_missing	sigsso: Invocation error - missing USER
tpaid_missing	sigsso: Invocation error - missing TPA_ID
expires_missing	sigsso: Invocation error - missing ExpirationTime
signature_missing	sigsso: Invocation error - missing signature
sslkey_missingconf	sigsso: error in configfile - missing public_ssl_key
usedtokens_missingconf	sigsso: error in configfile - missing tokensfile entry
logfile_missingconf	sigsso: error in configfile - missing logfile
sslkey_missingfile	sigsso: file access error - SSL public key file
usedtokens_missingfile	sigsso: file access error - UsedTokens file
logfile_missingfile	sigsso: file access error - log file
tpaid_unknown	sigsso: validation error - TPA_ID is invalid or not configured
usedtokens_allreadyused	sigsso: validation error - SSO Link has been used before
signature_invalid	sigsso: validation error - signature invalid
expires_exeeded	sigsso: validation error - SSO Link expired (or system clock out of sync?)!
tpa_error	sigsso: An error in the Third Party Application Adapter occurred. It said:

[sigsso: default errorcodes]

	See 3.4.2 for an explaination of the error messages.
	
	Example:
	
	`[errorcodes]`
	`signature_missing: An error occured while trying to access the application. Please contact your system administrator.`
	`expires_exceeded: http://my.errorpages.de/why_expired.html`

Return Values in case of error	
Logging + Debugging	**Increase Logging** If a request does reach the SSO Agent, then most likely you will be able to find helpful information by increasing the log level. See "Understanding SSO Agent Error Messages" in the "Signature-Based Single Sign-On Framework" document for details. The place of the logfile is configured in the sigsso.conf. The Log for a successful use of the link/redirect looks like this (loglevel:2) Wed Oct 22 11:29:16 CEST 2003 IP:192.168.1.59 USER:kasper TPA_ID:MyOwnApp At the beginning, the date followed by the users IP, the username itself, and the accessed tpa_id. If something goes wrong the errorcode is attached at the end of the line followed by the errordesciption. Looks like: Wed Oct 22 13:31:19 CEST 2003 IP:192.168.1.59 USER:kasper TPA:MyOwnApp ERROR:31 ERRORTEXT:sigsso: validation error - SSO Link has been used before For a higher loglevel the expiration time and the full signature will be logged too.
Implementation Details [optional]	./.
Limitations, Known Problems, To-Do	

Sample Config File

```
# sigsso.conf sample file
# 2004-07-04

[global]
loglevel:4
#       0: no logging
#       1: errors (tpa_id + user)
#       2: success and errors (tpa_id + user)
#       3: errors (tpa_id + user + expires + signature)
#       4: success and errors (tpa_id + user + expires + signature)

public_ssl_key: /usr/local/sigsso/etc/sigsso_public.key
tokensfile:     /usr/local/sigsso/tmp/usedtokens.txt
logfile:        /var/log/sigsso/sigsso.log
externalOpenssl: 1
tmp_signature_dir: /tmp
tmp_signature_prefix: sign_

[errorcodes]
user_missing:
tpaid_missing:
expires_missing:
signature_missing:
tpaid_unknown:
sslkey_missingconf:
sslkey_missingfile:
usedtokens_missingconf:
usedtokens_missingfile:
usedtokens_allreadyused: The link to this application has been used before. Please reload the
original page, and please do not double-click!
signature_invalid:
tpa_error:
logfile_missingconf:
logfile_missingfile:
expires_exeeded:

[main]
owl:     php://www/owl/htdocs/index_sso.php --url=http://www.my.server/owl/browse.php
chat:    php://www/chat/htdocs/phpopenchat/index_sso.php --url=http://www.mychat.server/index.php
phpbb:   php://www/phpbb/htdocs/index_sso.php --url=http://www.myphpbb.server/index.php
wbboard: php://www//wbboard/index_sso.php --url=http://www.my.server/wbboard/index.php
otrs:    cmd://opt/otrs/bin/cgi-bin/index_sso.pl --remote_addr=%remote% --agent=%agent%
--url=http://www.my.server/otrs/index.pl --user=%user%
olb:     php://www//olbookmarks/index_sso.php --url=http://www.my.server/olbookmarks/index.php
#
# Note: Although in this example some redirects point to different hostnames,
# these hostnames all have to point to this machine.
#
# If you want to integrate applications on different server machines:
# Deploy and configure the SSO Agent on each.
```