ColectivosVip

Generación de URLs para SSO

Título: ColectivosVip: Generación de URLs para SSO
Autor: Jordi Lagunilla
Versión: 1.4
Fecha de última modificación: 01/08/2018

Cambios

Versión del documento	Descripción	Fecha Modificación
1.0	*Jordi Lagunilla. Edición inicial*	11/12/2012
1.1	*Javier González. Añadida clarificación sobre el parámetro sso_token. Cambios en el formato.*	15/03/2017
1.2	*Salvador Lidón. Añadidas opciones de encriptación*	30/08/2017
1.3	*Jordi Lagunilla. Mejora del ejemplo de encriptación*	14/09/2017
1.4	*Javier González. Se añade una sección de testing que indica la URL de pruebas.*	01/08/2018
1.5	*javier Gonzalez. Se añade el parámetro “” para poder escoger el algoritmo de hash.*	20/11/2018

Descripción

ColectivosVIP proporciona **un mecanismo de generación de URLs seguras** para que un usuario autenticado en un sistema externo pueda autenticarse de forma transparente para él en la plataforma ColectivosVip. Se suele hablar de este mecanismo como ***Single SignOn*** (SSO), ya que en este escenario el usuario percibe que se autentica una única vez.

Parámetros

Campo	Descripción	Obligatorio
sso_token	Identificador único del usuario en el sistema externo (45 caracteres máximo)	Si
sso_email	Correo electrónico del usuario	No
sso_name	Nombre del usuario	No
sso_surname	Apellidos del usuario	No
sso_sex	Género (1 = hombre, 2 = mujer)	No
sso_timestamp	Fecha de generación de la URL (en milisegundos)	Si
sso_hash	Resultado de codificar en MD5 ó SHA(256, 384 ó 512) la cadena siguiente (sso_token=xxx&sso_timestamp=xxx&secret=xxx), donde el valor de "secret" es una palabra clave acordada entre ambas partes)	Si
sso_auth	Resultado de encriptar los parámetros del SSO	No

Los parámetros opcionales resultan útiles por ejemplo, de cara a que el usuario no tenga que rellenar tantos parámetros en el formulario de activación de cuenta que se le presenta la primera vez que accede a la web del club.

Título: ColectivosVip: Generación de URLs para SSO
Autor: Jordi Lagunilla
Versión: 1.4
Fecha de última modificación: 01/08/2018

Conformación de la URL para SSO

Imaginemos que la URL del club de descuentos es:

http://www.colectivosvip.com/demosso/

Una URL SSO básica tiene entonces el formato siguiente (tomando 12345 como palabra clave):

http://www.colectivosvip.com/demosso/?**sso_token**=ABCDE&sso_email=jlagunilla@colectivosvip.com&**sso_timestamp**=1354721155329&**sso_hash**=702b6010c3bccf0eaeb4d37c51a77253

Encriptación

Opcionalmente para mejorar la seguridad se pueden encriptar los parámetros de forma que no viajen en claro.

Para ello, partiendo del ejemplo anterior:

http://www.colectivosvip.com/demosso/?sso_token=ABCDE&sso_email=jlagunilla@colectivosvip.com&sso_timestamp=1354721155329&sso_hash=702b6010c3bccf0eaeb4d37c51a77253

Cogeríamos la parte de los parámetros:

sso_token=ABCDE&sso_email=jlagunilla@colectivosvip.com&sso_timestamp=1354721155329&sso_hash=702b6010c3bccf0eaeb4d37c51a77253

Y encriptaríamos toda la cadena utilizando el algoritmo de encriptación pactado. El resultado lo codificamos en Base64 y lo concatenamos a la URL de la siguiente forma. Si usamos el algoritmo **AES** con palabra clave **111122223333444** para la encriptación, obtenemos la URL siguente:

http://www.colectivosvip.com/demosso/?**sso_auth=**4QlenYN2p8WT+qVf9yP+6xKd+ktEMoBVu/S590Q4Azm0I5+0YsnptcL+6ZN41c+MHDQ0q4rqxh4jOqsNVx60ls47xtc0crWRCgFcKQm+6pvkXPO46OaNgMdaDKJPWQprxv5jvuPKZDlVVthCV7GJN5lYPvJVmZJI92d6G+3nBck=

Niveles de encriptación:

Estándar:
AES ECB con clave de 16 bytes.

Título: ColectivosVip: Generación de URLs para SSO
Autor: Jordi Lagunilla
Versión: 1.4
Fecha de última modificación: 01/08/2018

Alto:
AES CBC con clave de 32 bytes y con IV de 16 bytes. El IV se concatenará al principio del resultado de la encriptación antes de codificarlo en Base64.

Testing de los enlaces SSO:

ColectivosVip proveé de una utilidad http://ssotest.colectivosvip.com/ en la que:

- Podrá consultar código de ejemplo (en PHP)
- Podrá generar URLs para comprobar que el acceso es correcto y así entrar en el portal.

Título: ColectivosVip: Generación de URLs para SSO
Autor: Jordi Lagunilla
Versión: 1.4
Fecha de última modificación: 01/08/2018