



MUNICIPALIDAD DE ROSARIO

Sistema Integrado de Administración Tributaria SIAT

Arquitectura SWE Seguridad Web Extendida

Agosto de 2007

Contenido

Seguridad Web Extendida - SWE3

 Versiones.....3

 Objetivos del documento3

 Introducción3

 Objetivos de SWE.....3

 Premisas3

Vista lógica4

 Descripción general4

 Entidades de datos de SWE4

 Auditoria5

 Login / Autenticación5

 Información de Contexto de Aplicación.....5

 Administración de Entidades6

Vista Física7

 Estructura deploy.....7

 Despliegue de GUI Administración de Entidades.....7

 Despliegue de jar en aplicaciones Cliente7

Seguridad Web Extendida - SWE

Versiones

Fecha	Version	Descripcion	Autor
01/08/07	1.0	Inicial	tecso:
12/11/07	1.1	Actualizacion de nombres de acciones	tecso:

Objetivos del documento

Describir la arquitectura y diseño del modulo de Seguridad Web Extendida. Construido para el control de acceso de usuario y roles a funcionalidades de la aplicación SIAT' asi como cualquier otra que use SWE.

Introducción

Entendemos por Arquitectura del Software a la organización fundamental de un sistema en términos de: sus componentes, las relaciones entre ellos y el contexto en el que se implantarán, y los principios que orientan su diseño y evolución. (IEEE Std 1471-2000)

Objetivos de SWE

A continuación, las enunciamos:

- Proveer una interfaz gráfica para administrar usuario, permisos y estructura menú de aplicaciones.
- Proveer una API para consultar la estructura de menú y verificar credenciales de usuario para ejecutar acciones sobre las aplicaciones.
- Proveer mecanismos para auditar eventos críticos ocurridos durante el uso de una aplicación.
- Autenticar usuarios en las aplicaciones que utilizan SegWeb.

Premisas

Para el diseño y programación del Administrador de Procesos se tienen en cuenta las siguientes premisas:

- Se plantea SWE como una extensión al actual modulo de seguridad SegWeb.
- Se delega en SegWeb la autenticación del usuario.
- SWE se desarrolla dentro del marco general del proyecto SIAT.
- SWE se realiza basándose en la experiencia adquirida durante la construcción de la aplicación APS.

Vista lógica

Descripción general

Para una comprensión conceptual y de construcción, es útil distinguir las siguientes partes de SWE:

- Entidades de datos de SWE
- Login/Autenticación de Usuarios
- Auditoria
- Información de Contexto de Aplicación
- Administración de Entidades

Las *entidades de datos de SWE* tratan sobre el modelo de datos de la aplicación. La *autenticación* trata sobre los mecanismos para autenticar a usuarios de aplicaciones registradas en SWE.

La *Información de Contexto* de aplicación se refiere a datos específicos de SWE para una aplicación como lista de accesos a acciones y estructura de menús.

Por último la *Administración de entidades* se refiere a la manera de administrar el modelo de datos relacionados con una aplicación.

Entidades de datos de SWE

Aplicaciones

SWE organiza las entidades en Aplicaciones. Una aplicación posee Módulos, Roles, Usuarios, Items de Menú.

Módulos

Un Módulo de SWE posee un nombre y posee Acciones. En lo que respecta a SWE un módulo es solo un agrupador de acciones.

Acciones

Una Acción pertenece a un Módulo y representa la ejecución de alguna funcionalidad de una aplicación. Por ejemplo “Alta de una Aplicación” es una acción para SWE, o para SIAT “Alta de Recurso” podría ser una acción de SIAT del módulo Padrón, etc.

Una Acción posee un Nombre de Acción, Nombre de Método, y una Descripción, los dos primeros atributos describen de forma única a la acción en una aplicación. Y se corresponde con la forma en que esta programada la aplicación. La descripción de la acción se utiliza como una representación humana de la acción y es usada por ejemplo durante la auditoria.

Por ejemplo: la acción de Alta de Aplicación en SWE posee los siguientes atributos:

Nombre de Acción:	ABM_Aplicacion
Nombre de Método:	agregar
Descripción:	Alta de Aplicación

Roles

Una aplicación posee muchos roles. Los roles agrupan un conjunto de Acciones validas, las cuales podrán ejecutar los usuarios.

Usuarios

Una aplicación posee muchos usuarios. Un usuario posee un nombre de usuario y un conjunto de roles asociado al que pertenece.

El nombre de usuario tiene que corresponderse con un usuario de SegWeb.

Los roles al que pertenece el usuario determinan las acciones a las que tendrá acceso el usuario.

ItemMenu

Esta entidad representa los ítem de menú de la estructura de menú de una aplicación.

Básicamente un ItemMenu representa un nodo en la estructura de menú de una aplicación, posee un nombre descriptivo, una Acción asociada o un lista de ItemMenu hijos.

El nombre descriptivo puede ser utilizado por una aplicación para armar en forma gráfica su menú. La acción asociada sera utilizada para disparar acciones desde el menú. La lista de ItemMenu hijos pueden representar un SubMenu de forma gráfica.

Un ItemMenu no puede poseer Acciones e Hijos al mismo tiempo. La estructura de menú así formada puede tener infinitos niveles de profundidad.

Auditoria

SWE realiza registros para para posterior auditoria mediante una funcionalidad AuditLog añadida a Demoda.

AuditLog en Demoda provee una interfaz para logear registros con el siguiente formato:

[hora del evento][usuario][Desc.Acción][Detalles del Evento]

Para los fines de persistir los registros de log, AuditLog utiliza log4j. Log4j puede configurarse para generar logs en archivos locales, en Base de Datos vía JDBC y/o syslogd.

Login / Autenticación

SWE provee una Interfaz que permite autenticar un usuario mediante el método login.

Actualmente el método login delega la actividad de autenticar el usuario en SegWeb.jar implementado por la Municipalidad de Rosario.

Información de Contexto de Aplicación

El contexto de una aplicación en SWE contiene el conjunto total de acciones y la estructura de Menú de la aplicación en particular. Comúnmente una aplicación obtiene su Contexto de aplicación por única vez invocando a un método de la Interfaz de SWE.

A través del Contexto de aplicación se puede realizar las operaciones:

1. Obtención de Menú en Base a un usuario.
2. Verificación de permisos a acciones solicitadas por un usuario.

En el caso 1) el menú obtenido posee solo los nodos que poseen acciones permitidas por el usuario de acuerdo a sus roles.

En el caso 2) la verificación se realiza comprobando que un determinado Nombre Acción y Método, pertenezca al grupo de acciones que puede ejecutar ese usuario. Dicho grupo de acciones queda determinado por los roles a los que pertenece.

En caso de que se solicite verificar por un Nombre de Acción y Método que no existan en la aplicación, el contexto retorna un valor que permite manejar este caso.

Administración de Entidades

SWE posee una interfaz gráfica WEB que permite administrar las entidades. Desde aquí se pueden dar de alta Aplicaciones, Usuarios, Roles, ItemMenu y asociarlos entre ellos para determinar la configuración de seguridad de las aplicaciones.

Vista Física

Estructura deploy

Los script de compilación de SWE generan dos formatos para desplegar:

Despliegue de GUI Administración de Entidades

Aplicación GUI de Administración de Entidades se despliega mediante **swe.war** generado a partir de la invocación a al comando ant

Despliegue de jar en aplicaciones Cliente

Cualquier aplicación que desee utilizar las API de SWE, debe agregar **swelface.jar** y **sweBuss.jar**. Dichos jar también son generados a partir de la invocación a al comando ant