Seguridad para mensajes EDIFACT

SeguriEDIFACT

SeguriEDIFACT forma un buzón en donde mensajes EDIFACT son procesados de forma segura, introduciéndoles elementos de seguridad, o bien, retirándolos para su uso.

SeguriEDIFACT funciona revisando los mensajes que interactuan en un sistema, insertando sólo mensajes válidos e imprimiendo características de seguridad a los mensajes que así lo requieran. Los elementos que determinan qué tipo de tratamiento se le debe dar a cada mensaje son especificados según las necesidades de cada organización configurando el manejo de llaves.La configuración se realiza una única vez, indicando de qué manera deben ser tratados los elementos de seguridad, como por ejemplo la forma de proteger la llave privada del usuario mientras el programa está corriendo. Sólo el password con que el usuario protege su llave privada queda asilado del sistema. De la misma manera se especifican qué mensajes se deben asegurar y cómo, a través de una gran variedad de posibilidades a elegir.

Su interfase gráfica JAVA, Graphic User Interfase (GUI), asegura su portabilidad a un gran número de plataformas. Una vez configurado, el programa corre de manera automática, sin necesidad de mostrar su inteface gráfica al usuario, aunque es posible correrlo de forma manual. SeguriEDIFACT está capacitado para utilizarse dentro de una infraestructura de clave pública(PKI, Public Key Infraestructure) ; las políticas de configuración de llaves le indican qué pasos debe de seguir al requerir un certificado o verificar el estado de un certificado. Dichas políticas se establecen por tipo de mensaje.

SeguriEDIFACT realiza dos tipos de procesos interactuando con el módulo mapeador EDIFACT y con el módulo de comunicaciones EDIFACT:

Proceso outbound

Por cada interchange outbound que entra en SeguriEDIFACT, se produce un interchange con el mismo número de mensajes, pero algunos serán estructuras EDIFACT seguras.

1. SeguriEDIFACT examina cada tipo de mensaje, verificando en sus tablas de configuración qué mensajes deben de ser asegurados.
2. Cuando un mensaje no ha de ser asegurado se entrega el interchange de salida en el mismo mensaje.
3. Si el mensaje debe de ser asegurdao, se aplican las políticas de seguridad configuradas para este particular mensaje, generando una estructura EDIFACT segura que se agrega al interchange de salida.
4. El mensaje puede incluso requerir de Acknowledgment (ACK) del receptor, almacenándolo en una tabla de mensajes pendientes; o requerir conocer el estado de un certificado digital antes de enviar información confidencial. Ambas funciones son posibles con SeguriEDIFACT

Proceso Inbound

Por cada interchange inbound que entra en SeguriEDIFACT, se produce un interchange que remueve las estructuras EDIFACT de seguridad en aquellos que sean válidas

1. Cada interchange de entrada es revisado por SeguiEDIFACT. Los mensajes pueden ser de tipo Authentication and Acknowledgment (AUTACK) o EDIFACT.
2. Cuando es un mensje AUTACK, este será buscado en una tabla de mensajes pendientes de ACK, cambiando de pendiente a reconocido dicho mensaje. De esta manera el AUTACK ya no pasa al intechange de salida.
3. Cuando se trata de un mensaje de estructura EDIFACT de seguridad, se verifican criptográficamente los servicios de seguridad que se han determinado para dicha estructura.
4. Esta revisión puede arrojar dos resultados: criptográficamente válido de inmediato o criptográficamente inválido de inmediato. El tratamiento del mensaje varía en cada caso.

SeguriEDIFACT brinda ventajas de seguridad de estándar internacional EDIFACT, que rige los intercambios electrónicos para la administración, el comercio y el transporte a nivel mundial.

Plataformas

Windows NT
Solaris
HP-UX

Unix

Para otras plataformas UNIX se requiere:

ANSI C
JDK JAVA 1.1.5 o mayor
Manejador de base de datos relacional con drivers de JDBC (ej. Oracle 7.x)

Contáctenos

+(52)-5575-3407
info@seguridata.com
SeguriDATA
www.seguridata.com