SeguriDATA

SeguriEDIFACT

Altos estándares de seguridad para mensajes EDIFACT

SeguriDATA Privada S.A. de C.V. Amores 1003-1. 03100, México D.F. México
Teléfonos: (525) 575-3407 / 6385 / 9658 / 9761 Fax: 559-5887

http://www.seguridata.com

SeguriEDIFACT

Descripción

SeguriEDIFACT consiste en un programa ejecutable que recibe *interchanges outbound* del mapeador EDI for administration commerce and transport (Edifact), generando mensajes seguros para el módulo de comunicaciones.

De la misma manera, recibe del módulo de comunicaciones archivos con *interchanges inbound,* validando y removiendo los elementos de seguridad para suministrarlos al mapeador Edifact.

SeguriEDIFACT cuenta con una interface gráfica Java, asegurando su portabilidad un gran número de plataformas.
Sin embargo, para equipos que no trabajan bajo la plataforma de Java, siempre se recomienda utilizar SeguriEDIFACT en una plataforma que sí lo soporte aunque el resto de los componentes Edifact radiquen y se ejecuten en otra computadora.

Proceso outbound

En este primera versión, SeguriEDIFACT alimenta los intercambios contenidos en el archivo. Por cada *interchange outbound* que entra a SeguriEDIFACT se produce un *interchange* que contiene el mismo número de mensajes que el de entrada pero quizás algunos de ellos como estructuras Edifact seguras. Por cada mensaje en el *interchange* de entrada, SeguriEDIFACT examina el tipo de mensaje y verifica en sus tablas de configuración si el mensaje tiene que ser asegurado. En caso de no tener que ser asegurado simplemente agrega al *interchange* de salida el mismo mensaje. En caso de tener que ser asegurado, entonces aplica las medidas de seguridad configuradas para ese tipo particular de mensaje produciendo así una estructura Edifact segura la cual se agrega al *interchange* de salida. En caso de que para un tipo de mensaje en particular se especifica que se debe de requerir *acknowledgement* (ACK) del receptor, entonces formula la estructura segura solicitando dicho ACK y lo almacena en una tabla de mensajes esperando ACK con estado de pendiente.

Cuando se requiera de obtener el estado de un certificado con el objeto de enviar información confidencial y es indispensable estar seguro de la no revocación de dicho certificado se podrá realizar desde las opciones de *graphic user interface* (GUI) de SeguriEDIFACT.

Proceso inbound

En esta primera versión, SeguriEDIFACT alimenta los intercambios contenidos en el archivo. Por cada *interchange inbound* que entra a SeguriEDIFACT se produce un *interchange* que contiene, a lo más, el mismo número de mensajes que el de entrada pero remueve las estructuras Edifact de seguridad en aquellos que las contengan y sean válidas en el sentido criptográfico y elimina otras de control criptográfico. Por cada mensaje en el *interchange* de entrada, SeguriEDIFACT examina el tipo de mensaje.

Si el tipo de mensaje es *authentication and aknowledgement* (AUTACK) entonces busca en la tabla de mensajes pendientes de ACK se cambia de pendiente a reconocido dicho mensaje. El AUTACK como tal ya no pasa al *interchange* de salida.

Cuando el tipo de mensaje es una estructura Edifact de seguridad entonces, SeguriEDIFACT verifica criptograficámente los servicios de seguridad establecidos en dicha estructura y se puede obtener cualquiera de los dos siguientes resultados:

- Criptográficamente válido de inmediato,
- Criptográficamente inválido de inmediato,

Cuando se obtiene el estado de válido de inmediato entonces el mensaje original se pasa al *interchange* de salida.
Al obtener como resultado inválido de inmediato entonces no se pasa al *interchange* de salida sino que se agrega a la tabla de inválidos.

Interacción con PKI

En el manejo de llaves SeguriEDIFACT se configura para informarle de las políticas que tiene que seguir al requerir un certificado o verificar el estado de un certificado. Estas se especifican por tipo de mensaje y pueden ser las siguientes :

Únicamente verifica que la llave pública de la AC autentica el certificado, Verifica CRL si este tiene menos de *n* días de emitido. En el caso de que no se elija la primera opción en la segunda opción $n = 0$ o el CRL tiene mas de *n* días o no se encuentra el CRL entonces es posible obtener la operación de manejo de llaves mediante el procedimiento en línea del IES, en cuyo caso la entidad puede decidir si en caso de que el IES no este disponible se debe pasar de inmediato a inválidos.

Interface gráfica

SeguriEDIFACT una vez configurado, puede correr en forma automatizada sin necesidad de mostrar su interfaz gráfica, sin embargo para ciertas tareas administrativas la interface gráfica es un elemento insustituible.

SeguriEDIFACT se configura -una única vez- por el usuario mediante de su interface gráfica para especificar los parámetros bajo los que debe de operar. La configuración del sistema instruye a SeguriEDIFACT en el sentido de los datos de seguridad del usuario excepto el password. La forma en que se desea proteger la llave privada mientras este corriendo SeguriEDIFACT. La forma de operar el sistema manual o automática y parámetros relacionados.

Asímismo se especifican que mensajes se deben de asegurar y cómo, esto incluye si los mensajes *outbound* exigen de un AUTACK de reconocimiento o si los mensajes *inbound* que requieren de AUTACKs se generen automáticamente o manualmente y si estos se deben de generar por cada *interchange* o después de *n interchanges* de un socio comercial o después de haber transcurrido *n* minutos después de haber recibido un *interchange* de un socio comercial.

Plataformas

Las plataformas en las que SeguriEDIFACT esta disponible son:

Windows NT
Solaris
y HP-UX

SeguriDATA esta interesado en portar SeguriEDIFACT a otras plataformas UNIX para lo cual requerimos:

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

Estándares

SeguriEDIFACT soporta el conjunto de algoritmos criptográficos mas utilizados internacionalmente como RSA para criptografía de llave pública, y TripleDES-CBC para criptografía simétrica. En algoritmos de digestión se proveen MD2, MD4, MD5 aunque este último es el más recomendado. Cuenta además con una sólida base para generación de números aleatorios entre otras cosas.
En la codificación y descodificación de mensajes SeguriEDIFACT se basa en los estándares ISO 9735-5, ISO 9735-6 e ISO 9735-7.

SeguriSERVER, el sistema de Autoridad Certificadora de SeguriDATA complementa a SeguriEDIFACT mediante la emisión y control administrativo de certificados Edifact. De hecho SeguriSERVER es un sistema de Autoridad Certificadora que produce certificados para los estándares public key cryptography standard (PKCS) y Edifact.
Como parte de SeguriSERVER, SeguriDATA provee el software de Agente Certificador y provee el software de usuario para generación de llaves y requerimiento de certificación.