

Integridad, Autenticidad, No-Repudio de Origen y Confidencialidad para sus archivos

Descripción

SeguriDoc es una aplicación para Microsoft® Windows, desarrollado con el propósito de brindar Integridad, Autenticidad, No-Repudio de Origen y Confidencialidad de archivos bajo el estándar PKCS (Public Key Cryptography Standard) que utiliza criptografía de llave pública (RSA) y algoritmo de criptografía simétrica (TripleDES-CBC).

Funcionalidad

SeguriDoc realiza cuatro funciones fundamentalmente:

- Firmado digital
- Autenticación de archivos
- Encriptación de archivos
- Desencriptación de archivos

Cualquier archivo es susceptible de ser firmado digitalmente y/o encriptado.

Para imprimir a un archivo las características de Integridad, Autenticidad y No-Repudio de Origen se hace uso del firmado digital a través de la criptografía de llave pública bajo el estándar RSA. Cuando a un archivo se le aplica el proceso de firmado digital, SeguriDoc usa la llave privada del suscriptor, asegurando así la Autenticidad, Integridad y No-Repudio de Origen del archivo en cuestión.

Quien recibe el archivo firmado, debe de conocer el Certificado Digital del suscriptor para proceder a la

autenticación del mismo. En este caso SeguriDoc trabaja con el certificado digital del suscriptor, extrayendo su llave pública para autenticar el mensaje.

Adicionalmente es posible utilizar los servicios de SeguriServer para realizar las funciones de autenticación de usuarios y verificación de Certificados Digitales. Para que la autenticación del archivo sea positiva es indispensable que:

1. La firma digital contenida en el archivo concuerde con el certificado del suscriptor, por lo que el archivo auténticamente ha sido firmado por el suscriptor.
2. No exista modificación alguna en el archivo posterior a su firmado, por lo que el archivo es íntegro. Estas dos condiciones a su vez implican el No-Repudio de Origen del archivo firmado digitalmente por el suscriptor, ya que se han comprobado de forma positiva la autenticidad de la Firma Digital contenida en el archivo así como la integridad del mismo, por lo que el suscriptor está conforme con el contenido.

Por otra parte, la confidencialidad se logra por medio de la encriptación del archivo con el algoritmo Triple DES-CBC.

Para encriptar un archivo es necesario conocer el certificado digital del

destinatario. Es posible generar archivos encriptados cuyo destinatario es la propia persona que lo encripta, o bien señalar múltiples destinatarios.

Cuando se decide encriptar un archivo, el usuario señala el certificado digital del destinatario y SeguriDoc aplica el proceso extrayendo la llave pública del certificado digital.

El archivo encriptado sólo puede ser abierto por el destinatario, ya que únicamente él tiene acceso a su llave privada, contraparte de la llave pública contenida en su certificado digital; sin la llave privada del destinatario no es posible conocer el contenido del archivo.

Adicionalmente SeguriDoc es un servidor OLE que permite a las aplicaciones propietarias hacer uso de la funcionalidad del mismo.

Operación

Las cuatro funciones de SeguriDoc se llevan a cabo desde una interfaz gráfica. Para firmar digitalmente y encriptar el procedimiento se debe seleccionar un archivo desde sencillas cajas de diálogo, o simplemente arrastrar el archivo seleccionado hasta la interfaz de SeguriDoc (funcionalidad conocida como Drag & Drop). Así mismo permite el almacenamiento y lectura de la llave y certificado digital desde una tarjeta inteligente.

El usuario decide en cada ocasión si desea firmar digitalmente, encriptar o firmar digitalmente y encriptar el archivo. También es posible seleccionar más de un archivo a la vez, generando un solo archivo final, o tantos archivos finales como archivos fuente haya seleccionado. SeguriDoc también ofrece compresión de datos.

Para autenticar y descryptar un archivo es necesario seleccionarlo desde las cajas de diálogo de SeguriDoc o hacer doble clic sobre él.

Certificados

SeguriDoc requiere que el usuario cuente con su propio certificado digital.

Los certificados X.509 son emitidos por diversas autoridades certificadoras; el usuario puede certificarse ante la Autoridad Certificadora que considere conveniente.

Llaves

El usuario puede generar de forma personal y secreta su par de llaves así como su requerimiento de certificación. La llave privada se protege por medio de una clave de acceso que sólo el propietario conoce. La llave pública se incluye junto con los datos del propietario en el denominado requerimiento de certificación, dicho requerimiento debe ser entregado a un Agente Certificador para su certificación.

Beneficios

El uso de SeguriDoc incrementará su productividad permitiéndole:

- Reducir costos de impresión y mensajería
- Transmitir cualquier tipo de archivo a través del Correo Seguro
- Encriptar y descryptar el documento desde el mismo mensaje de correo
- Firmar y encriptar archivos creados desde Microsoft® Word se lleva a cabo sin salir del procesador de textos
- Incorporar el No-Repudio de la información a los mensajes y contenidos transmitidos por correo electrónico

- Consultar el estado de los certificados digitales en línea, a través del cliente OCSP (Online Certificate Status Protocol)
- Proporcionar la Evidencia Forense Electrónica necesaria para realizar una auditoría basada en la información que se transmitió a través del Correo Seguro.
- Facilitar la auditoría de procesos al hacer transparente la gestión administrativa

Integración con Microsoft® Office y Lotus® Notes

SeguriDoc, se integra completamente a la interfaz de estos productos, permitiendo acceder a las operaciones de firmado y ensobretado directamente desde una barra de herramientas dentro de las aplicaciones.

Plataformas

SeguriDoc está diseñado especialmente para ambientes Microsoft® Windows 98 / 2000 / XP / 2003. Funciona con Microsoft® Outlook 2000/XP/2003 y con Lotus R5/R6 y R6.5

SeguriData

www.seguridata.com
Insurgentes Sur 2375 3er. Piso,
Colonia Tizapán,
01000, México, D.F.
Tel +52(55)3098 0700
Fax +52(55)3098 0702
ventas@seguridata.com