

CryptoSignServer INFORMACIÓN TÉCNICA

El Sistema CryptoSignServer consiste en una plataforma hardware/software, que garantiza la seguridad sobre los procesos de firma electrónica y su validación en sistemas informáticos orientadas a servicios.

Especificaciones Técnicas

Sistema HSM

Esta constituido por la integración de un Modulo de Almacenamiento criptográfico y una plataforma de administración de claves, que permite realizar múltiples operaciones administración y configuración, relacionadas con la generación de claves y la importación de certificados electrónicos. El dispositivo criptográfico esta certificado por la norma FIPS 140-2 Nivel 3.

Características:

El HSM cumple con la certificación del estándar FIPS 140-2 nivel 3.

El firmware del módulo impide la salida de datos confidenciales.

Se imposibilita el acceso a las diversas partes del HSM con sensores que detectan intrusiones o anomalías, borrando la información.

El HSM está cubierto por una resina epoxi opaca, una cubierta metálica protege el conjunto.

Sistema Servidor

Procesador con arquitectura Intel.

Una conexion ETHERNET 10/100/1000 Mbps.

Sistema en rack.

Características Funcionales

Configuración mediante protocolo seguro HTTPS, donde se dispone de la capacidad de realizar:

- a) Generación de claves privadas RSA, desde 1024 hasta 2048 bits.
- b) Generación de peticiones de certificados desde un dispositivo acreditado de forma segura.
- c) Importar certificados hacia la placa criptográfica.
- d) Configurar las direcciones de red, re-inicializar los servicios del sistema y re-inicializar las funciones criptográficas inmersas en el dispositivo.

Acceso al Sistema

A nivel de administración, se presenta un modelo de autenticación basado en una autoridad de certificación embebida en el propio dispositivo. En esta CA, se generaran los certificados electrónicos que verificarán la identidad de los administradores del sistema.

A nivel del componente cliente, se provee una API, desarrollada en tecnología Java, que puede ser integrada mediante simples sentencias en plataformas de TI, herramientas de seguimiento de tareas o en componentes embebidos en aplicaciones clientes y es independiente de la plataforma utilizada.

Funcionalidades Incluidas

Funcionalidades disponibles

- a) Firma Electrónica en formato XAdES, con capacidades de personalizar e integrar atributos no obligatorios dentro de su estructura.
- b) Firma Electrónica en formato PKCS#7 RSA.
- c) Firma Electrónica en formato nativo PDF.
- d) Verificación de firma(s) electrónica(s) en formato nativo PDF.
- e) Verificación de firma electrónica en formato PKCS#7 RSA.
- f) Firma Electrónica con soporte para estampado de tiempo en formato PKCS7 RSA.
- g) Firma Electrónica con soporte para estampado de tiempo en formato nativo PDF, con soporte de validación nativo.

Prestaciones

Procesos de firma electrónica ejecutadas por hora.	1024	2048
PDF nativo (a)	189.473,00	132.410,00
PDF nativo con sellado de tiempo (b)	105.882,00	90.000,00
PKCS#7 RSA	302.740,00	276.000,00
PKCS#7 RSA con sellado de tiempo (b)	190.217,00	165.120,00
XAdEs	246.780,00	211.457,00

Verificación de firma electrónica

PDF nativo(a)	210.631,00
PKCS7	190.974,00

- a. Depende del número de firma electrónica que disponga el documento.
- b. El sellado de tiempo es de longitud de 2048 bits