

## **Biblioteca de Servicios Criptográficos de Bajo y Alto Nivel**

### **Beneficios**

SeguriLib consiste en una completa biblioteca (API) que proporciona una gama de servicios criptográficos, que van desde las operaciones más elementales como encriptar y desencriptar, hasta ejecuciones de alto nivel como generar requerimientos de certificación o formar y procesar mensajes criptográficos bajo el estándar PKCS (Public Key Cryptography Standard).

Desarrollado completamente en lenguaje C, SeguriLib puede portarse a una gran variedad de plataformas. Idealmente, por cuestiones de seguridad, SeguriLib debe ser utilizado como una biblioteca estándar aunque también puede utilizarse como DLL.

### **Funcionamiento**

SeguriLib implementa dos tipos de funciones básicas:

- Servicios criptográficos de bajo nivel como:
  - Criptografía simétrica: Algoritmos RC2, RC4, DES, DESX y TripleDES en distintos modos de operación.
  - Criptografía asimétrica: Funciones básicas como encriptación, desencriptación, firma y verificación primitiva de firma usando el algoritmo RSA.
  - Esquemas de criptografía: Esquemas de firma y encriptación usando el algoritmo RSA.

- Funciones auxiliares: Funciones Hash como MD5 y SHA-1. Generación de números pseudo aleatorios (PRNG: Pseudo Random Number Generation).

- Servicios criptográficos de alto nivel como:

- Generar requerimientos de certificación PKCS.
- Certificación de requerimientos PKCS.
- Firmado, ensobretado, apertura y autenticación bajo el estándar PKCS.

### **Nivel de Seguridad**

El Código de implementación de PKCS es creado y mantenido por Seguridata. Gracias a esto, SeguriLib utiliza llaves simétricas de 128 bits y RSA de 2048 bits o mayores, sin restricción alguna.

### **Plataformas**

SeguriLib se encuentra disponible para las siguientes plataformas:

- Windows 95, 98, NT, 2000 y XP
- Solaris
- HP-UX
- AIX
- Linux

## **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**