▪ Tarjeta STARCOS SPK 2.3 ITSEC E4 HIGH

La tarjeta STARCOS está especialmente diseñada para infraestructuras de clave pública en las que se requiere autenticación de una entidad, integridad, confidencialidad de datos y el no repudio en origen. Mantiene el material sensible criptográfico siempre interno a la tarjeta y, protege su uso mediante control de acceso. De esta forma, se obtiene una considerable ventaja en términos de seguridad y portabilidad sobre las soluciones software.

Las características del procesador de Philips P8WE5032VOG certificado ITSEC E4 High, consigue una herramienta eficaz que dificulta ataques basados en fuerza bruta y análisis diferencial.

El chip proporciona 32 Kbytes de EEPROM. Este espacio de memoria puede ser utilizado para extender la funcionalidad de la tarjeta por el emisor de una forma segura y, se convierte en un amplio soporte de información de usuario protegido y portable.

El SO prevé la posibilidad de definir una estructura de ficheros acorde a la recomendación PKCS#15 de RSA con el fin de facilitar la interoperabilidad entre aplicaciones basadas en tarjeta inteligente.

Otras características son:

- Compatible ISO/IEC
- Compatible EMV ’96
- Comunicación segura
- Estructura jerárquica de ficheros ISO
- Protocolos de cifrado simétrico. DES, DES-3
- Maquina de estados
- Generación de claves RSA hasta 1024 bits
- RSA/DSA para cifrado y descifrado
- Algoritmo hash SHA-1
- Autenticación asimétrica
- Firma digital:
  - RSA firma y verificación hasta 1024 bits
  - DSA firma y verificación hasta 1024 bits

Características principales del chip Philips P8WE5032VOG

- CPU de 8 bits de alto rendimiento.
- 32 Kbytes de ROM para código
- 256 bytes IDATA RAM, 2048 extended
- 32 Kbytes de EEPROM
  - Tiempo de borrado-escritura de EEPROM de 4.0ms.
  - Retención de datos en EEPROM de un mínimo de 10 años.

- Periféricos integrados
    - Cripto-procesador específico para encriptación triple-DES (<0,2ms)
    - Cripto-procesador específico para operaciones de pki, claves de 1024 bits en <160 ms.
    - Generación real de números aleatorios.
    - Generador de frecuencia de trabajo interna.
- Características de seguridad
    - Cifrado dinámico de memorias y buses
    - Sensores para control de tensión y frecuencia
    - Escudo activo sensible a manipulaciones del hardware
    - Generador aleatorio de estados de espera y picos de consumo
    - Identificación única para cada chip
    - Modo de ahorro de energía.
    - Rango de frecuencia externa 1-5Mhz.
    - Frecuencia interna de hasta 10Mhz.

Características del sistema operativo STARCOS / SAFESIGN

Una tarjeta completa con el sistema operativo STARCOS SPK2.3/2.4 ofrece alrededor de 20/25 Kbyte libres de EEPROM. La tarjeta inicializada puede contener los siguientes objetos:

Objetos	**SAFESIGN for STARCOS v1.0.9**
Número de PINS /PUKS	1/1
Min/max longitud de PIN o PUK	4/8 caracteres
Longitud de la etiqueta identificativa	0/37 caracteres
Número de parejas de claves de 1024 bits RSA	de 0 a 6
Número de certificados (max. depende del tamaño de los certificados).	0-aprox. 10
Tamaño de los objetos públicos	0-9166 Bytes
Tamaño de los objetos privados	0-1348 Bytes

El software está homologado para un gran número de aplicaciones y sistemas operativos, destacando los navegadores, clientes de email y VPN más comunes del mercado (Microsoft, Netscape, Eudora, Lotus Notes; CheckPoint,…)

Software

- El fabricante proporciona una colección de librerías (SAFESIGN) que facilitan la integración de la tarjeta en otros sistemas. Estas

librerías resuelven de una forma eficiente y sencilla la mayoría de las tareas con las que se tiene que enfrentar un integrador en un entorno Windows: Multitarea y multiproceso, conexión a lectores PC/SC, creación, lectura y escritura de ficheros, gestión del control de acceso, operaciones criptográficas, servicios de autenticación,... etc.

- Las interfaces PKCS#11 de RSA permiten el uso de la tarjeta STARCOS a una gran variedad de aplicaciones criptográficas entre las que se encuentran productos como Safelayer, Entrust, Baltimore, Netscape, APIs de JAVA, etc.
- Con el CryptoAPI de Microsoft se consigue una completa integración de la tarjeta STARCOS en el sistema operativo Windows en las tareas clásicas: autenticación de usuario, correo electrónico, seguridad en redes abiertas, etc.

Software disponible para la tarjeta STARCOS

- Proveedor de recursos a bajo nivel basado en tecnología COM.
- Librerías estándar PKCS#11 versiones 1.0 y 2.01.
- CryptoAPI de Microsoft.
- Token management, para gestión de claves y registro de certificados.
    - Permite almacenar hasta 5 parejas de claves y 10 certificados, incluyendo diferentes certificados de CA
    - Gestión de PIN y PUK
    - Aviso de caducidad de certificados
- Software para la activación de Claves y generación de peticiones de certificados.