SmartCard

Tarjeta criptográfica QSCD

Aplicaciones

Intranet corporativa con procesos de autenticación y firma electrónica.
Internet, plataformas con servicios de alto valor añadido.

Sectores de alto interés:

Institución pública, Banca electrónica, eCommerce, eProcurement, Despachos Profesionales con acceso a información confidencial, Salud, Fuerzas de Seguridad. Interoperable con equipos de escritorio y portables (Smartphone, tablet).

Seguridad jurídica en las Transacciones electrónicas.

La información de este documento se proporciona "tal cual" y queda sujeta a modificaciones sin previo aviso. ANF AC no es responsable de los errores u omisiones de este documento.

Consultar última versión en http://www.anf.es/es/publicaciones/

Dispositivo Cualificado de Creación de Firma/Sello, oficialmente certificado como QSCD.

Este instrumento está específicamente diseñado para mejorar la seguridad de las claves y realizar operaciones de firma electrónica cualificada.

Es interoperable con la suite de aplicaciones Critical Acces®, funcional con toda la gama de certificados de ANF AC.

Las SmartCard son personalizables con la imagen corporativa del cliente.

Características técnicas

La SmartCard Sign de ANF AC ensambla chip de primeras marcas internacionales con certificaciones de seguridad y reconocimiento QSCD. Opcionalmente puede incluir MIFARE RFiD / NFC® ANFAC08

Dispone de middleware, Minidriver CSP y PKCS # 11. Incluye ANF CT y ANF WSI CA que habilita control de acceso y firma en Web con navegadores y sin precisar componente Java.

Características CHIP

- Memoria EEPROM *1. 64 Kb. hasta 80 Kb
- Alta velocidad de transmisión (9600 a 614.400 BPS*1)
- Ciclos de lectura/grabación: 500.000 EEPROM
- 5 ms de tiempo de escritura
- ATR configurable
- Número serie unívoco
- Función anti-tearing *2
- Retención de datos de 10 años
- Protección ESD de 4.000V min.
- Protección mayor a 6kV (HBM) en descargas electroestáticas (ESD).

Capacidad criptográfica

- Algoritmos criptográficos:
- DES/3DES ECB y CBC (hasta 192 bits),
- AES (128/192/256 bits),
- RSA (1024 / 2048)
- Seguridad hardware mejorada de acelerador DES.
- Algoritmo de Hash: SHA1, SHA-2, SHA512.
- Generación aleatoria de números (TRNG) AIS-31 clase P2.

Funciones de seguridad

- Proporciona identificación segura en control de accesos
- Soporte de firma electrónica
- Generación de pares de claves RSA (hasta 2048 bits) y EC (hasta 521 bits)
- Contenedor seguro de certificados electrónicos
- Contenedor seguro de claves simétricas
- Cumple con las Guías de Seguridad contra ataques DFA (Differential Fault Analysis)
- Contramedidas contra los ataques de canal lateral mediante análisis de grado de poder (DPA).
- Protección contra-ataque reiterado PIN
- NFC ® para aplicaciones de control de acceso lógico y físico.

Conformidad y certificaciones

- ISO 7816-1 Partes 1-4,8,9
- ISO 7816-3 protocolos*1 T=0 y T=1
- Certificación del Chip*1: CC EAL4+ o superior
- Certificación SO*1: CC EAL4+ o superior
- Certificación FIPS 140-2
- Generador aleatorio*1: FIPS 186-2
- Algoritmo de checksum*1 ISO 3309 CRC-16, CRC- 32.

**1 Según modelo*

**2 Sistema de seguridad contra la retirada prematura de la tarjeta*

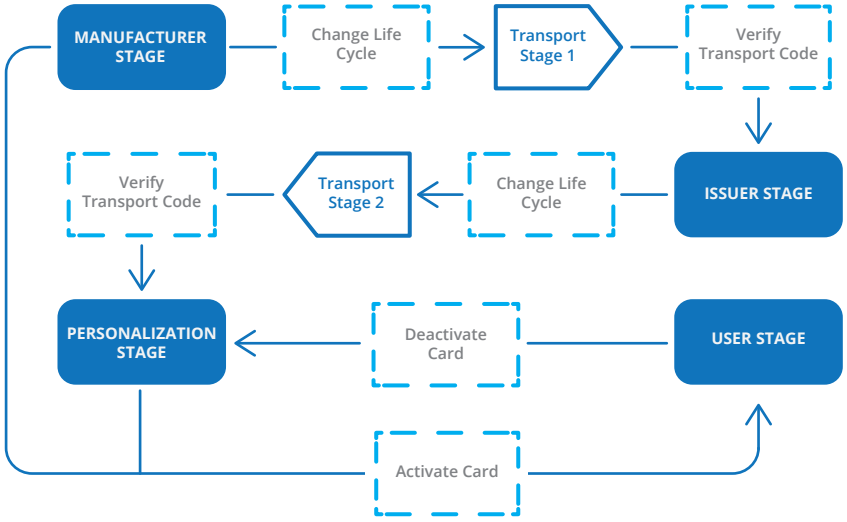
Escenarios de uso habitual

- Tarjeta profesional
- Tarjeta corporativa alta dirección
- Cumplimiento RGPD – Credenciales
- Identificación local y remota.
- Sector Salud
- Sector Seguridad
- Monedero electrónico

Ciclo de vida de la SmartCard

SmartCard Sign tiene las siguiente etapas durante su ciclo de vida:

0= Etapa de fabricación
1= Etapa de transporte
2= Etapa de inicialización
3= Etapa de transporte
4= Etapa de personalización
5= Etapa de usuario



0 **Etapa de fabricación**
Es el estado inicial de la tarjeta en estado desactivada. En esta etapa es posible acceder al bloque de cabecera de la tarjeta y puede ser referenciado utilizando el Read Binary o el Update Binary. Todos los comandos están permitidos en esta etapa. SmartCard Sign no permite volver a esta etapa una vez que el ciclo de vida ha cambiado.

1 **Etapa de transporte**
El único comando que se puede utilizar en esta etapa es VERIFY TRANSPORT CODE,
Una vez que el código de transporte se ha introducido con éxito, la tarjeta puede pasar a las siguientes etapas.

2 **Etapa de inicialización**
En esta etapa se permiten una serie limitada de comandos, como el cambio del código de transporte, la inicialización de la tarjeta, etc. Una vez inicializada el ciclo de vida cambia de estado.

3 **Etapa de transporte**
En el segundo transporte el único comando que puede ser utilizado es VERIFY TRANSPORT CODE.
Una vez que el código de transporte se ha introducido con éxito, la tarjeta puede pasar a las siguientes etapas.

4 **Etapa de personalización**
En esta etapa el usuario procede a personalizar su tarjeta. Llegados a esta etapa ya no es posible retroceder a etapas anteriores.
El usuario genera sus claves y certificados de petición, selección el PIN secreto de activación, e incluso instala los certificados una vez han sido emitidos.

5 **Etapa de usuario**
La tarjeta esta lista para ser utilizada. El usuario tiene la capacidad de borrar certificados instalados en su SmartCard e, incluso, volver a la etapa de personalización para tramitar nuevas claves y certificados.

Requerimientos de SmartCard

Este instrumento requiere funcionalmente interoperar con un dispositivo lector PC/SC de SmartCard.

ANF AC pone a disposición de sus clientes dos modelos:
- Token SIM Reader
- Lector SmartCard Basic.