

eSign® USB

Token MicroSD de firma electrónica

¡Mucho más que una tarjeta de memoria!



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/>

Este documento es propiedad de ANF Autoridad de Certificación. Se autoriza su reproducción y difusión siempre que se reseñe:

2019 Copyright © ANF AC

PenDrive criptográfica con capacidad para generar claves de firma y seleccionar PIN sin intervención de terceros, garantía del no repudio. Cuenta con almacén seguro de certificados de firma electrónica, e incorpora suite de aplicaciones CriticalAccess® para la completa gestión del ciclo de vida, incluida renovación y revocación. Mantiene completa funcionalidad de un simple Pendrive.

eSign® USB es un avanzado dispositivo de creación de firma electrónica avanzada de larga vigencia, que incluye servicio de validación cualificada de firma y sellos electrónicos. Se suministra con Middleware de ANF AC, con capacidad de ser utilizado en procesos de 2FA (Doble Factor de Autenticación).

Tratamiento de la Memoria

eSign® USB define dos zonas de memoria:

- Pública. El usuario puede almacenar todo tipo de información.
- Propietaria. Inaccesible para el usuario.

Capacidad disponible 8 Gb. 16 Gb. 32 Gb. 64 Gb. 128 Gb.

Funciones de seguridad

- Proporciona identificación segura en control de accesos.
- Realiza firma electrónica avanzada.
- Contenedor seguro de certificados electrónicos.
- Contenedor seguro de claves simétricas.
- Protección contra-ataque reiterado PIN.
- Incluye capacidad de obtener TimeStamping.
- Actualizaciones automáticas.

Cumple normativa UE 910/2014

Permite cumplir ISO 27001 SGSI.

Cumple RGPD (UE) 679/2016

Capacidad criptográfica

- Algoritmos criptográficos:
 - AES (128/256 bits).
 - RSA (1024 bits / 2048 bits).
- Algoritmo de Hash:
 - SHA1, SHA-256.
- Generación aleatoria de números (TRNG) AIS-31 clase P2.

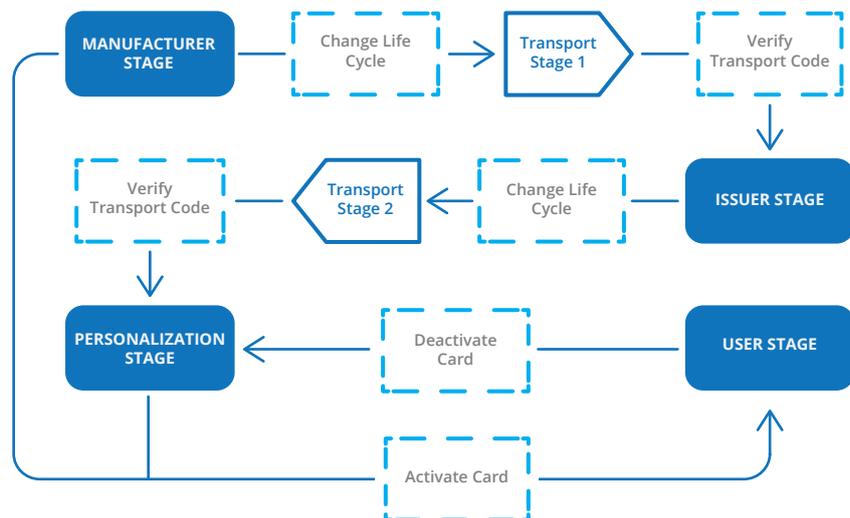




Ciclo de vida del PenDrive eSign® USB

El PenDrive eSign® USB tiene las siguientes 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.