centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1505

Procedimiento de Empleo Seguro
CRYHOD de PRIMX

Julio 2021

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.07.09 13:38:57 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-21-134-3

Fecha de Edición: julio de 2021

ÍNDICE

1. INTRODUCCIÓN

1.1 PROPÓSITO

1. Este documento contiene el procedimiento de empleo seguro del *software* de **cifrado de disco Cryhod de PRIMX** y su material asociado cuando se utilice para proteger el almacenamiento de información en sistemas bajo el alcance del ENS.
2. Todas las configuraciones de seguridad recogidas en este procedimiento de empleo seguro deben ser aplicadas para disponer de la versión del producto que ha sido cualificada.

1.2 APLICABILIDAD

3. Este documento es aplicable a la partir de la versión 3.0 de Cryhod.
4. Este procedimiento aplica a todos los usuarios del *software* y, por tanto, debe ser tenido en cuenta por todas las organizaciones que vayan a hacer uso del producto en sistemas bajo el alcance del ENS.

2. DESCRIPCIÓN DEL CRIPTOSISTEMA

5. Cryhod de PRIMX es un *software* de cifrado de disco *on-the-fly* o al vuelo que se ejecuta de forma transparente para el usuario y que permite el cifrado completo de discos, tanto internos como externos.

6. Se ejecuta sobre un sistema operativo *Microsoft Windows en sus versiones de 7 a 10* y permite añadir un paso de autenticación adicional en el *Pre-boot* (antes del arranque) del equipo.

7. Si bien Cryhod permite la utilización de varios mecanismos de autenticación, **solo se autoriza el empleo de mecanismos de autenticación fuerte** (*SmartCard* cualificada en el CPSTIC).

2.1 COMPONENTES DEL SISTEMA E INTERFACES

8. Los componentes básicos del *software* Cryhod de PRIMX son:

   a. Una aplicación *software* que, una vez instalada en el equipo, cifrará automáticamente toda la información que se almacene en su disco.

   b. Una tarjeta *SmartCard* cualificada que será utilizada para realizar la autenticación *Pre-boot* para poder acceder al equipo.

2.2 ESTADOS OPERACIONALES DEL SOFTWARE DE CIFRADO

9. Los posibles estados de Cryhod son:

   a. **APAGADO / CIFRADO:** El equipo está apagado y todo su contenido está cifrado. Cuando el dispositivo se encuentra en este modo:

      i. No es posible acceder a la información contenida en el equipo aunque sean extraídos físicamente sus discos y conectados a otros equipos.

      ii. Todos los parámetros críticos de seguridad (claves y certificados) con los que se cifran los archivos están protegidos.

   b. **PRE-BOOT**: El equipo está encendido pero no se han introducido las credenciales del acceso mediante la *SmartCard*. Cuando el dispositivo se encuentra en este modo:

      i. Es posible acceder a ciertas opciones de mantenimiento del software de cifrado.

      ii. No es posible acceder a la información contenida en el equipo aunque sean extraídos físicamente sus discos y conectados a otros equipos.

      iii. Todos los parámetros críticos de seguridad (claves y certificados) con los que se cifran los archivos están protegido.

c. **AUTENTICADO:** El equipo está encendido y la autenticación se ha realizado correctamente. Cuando el dispositivo se encuentra en este modo:

   i. Es posible acceder a la información contenida en el equipo. Cryhod cifra y descifra al vuelo los datos almacenados en el disco cuando el usuario accede a los mismos.

   ii. Las claves de cifrado se encuentran cargadas en memoria volátil del equipo.

2.3 PERFILES DE OPERACIÓN Y ADMINISTRACIÓN

10. Se definen los siguientes perfiles, todos ellos locales, en el dispositivo:

    a. **Usuario:** Se habilita después de superar la autenticación del usuario estándar con éxito. Permite acceder a la información contenida en el disco pero no tiene privilegios para descifrar el disco ni para administrar las opciones de configuración.

    b. **Administrador:** Se habilita después de superar la autenticación del administrador con éxito. Permite acceder a la información contenida en el disco y tiene privilegios para descifrar el disco de forma permanente. Adicionalmente también puede administrar las opciones de configuración que estén permitidas en las políticas configuradas en el equipo.

    c. **Recovery:** Se permite la utilización de usuarios de recuperación para poder realizar tareas de mantenimiento / recuperación del equipo en caso de fallo en el acceso mediante los usuarios estándar.

11. Adicionalmente se define el perfil de **administrador del equipo**.

    a. Este usuario administrador puede ser local o estar gestionado mediante un gestor centralizado de usuarios tipo LDAP, como por ejemplo, un *Active Directory* de Microsoft.

    b. El usuario administrador del equipo tendrá la capacidad de modificar las políticas del sistema, lo que determinará el funcionamiento del *software*.

3. CONFIGURACIÓN DEL *SOFTWARE* DE CIFRADO CRYHOD DE PRIMX

12. El software de cifrado Cryhod de PRIMX dispone de múltiples opciones de configuración que permiten activar o ajustar las funcionalidades del Sistema en función de las necesidades del usuario y sus requisitos de funcionamiento y seguridad.

13. Para la configuración de las políticas de seguridad se deben seguir las instrucciones incluidas el manual de configuración de la *herramienta "Cryhod 2020 Installation guide EN (PX18C964r3) [Ref 1.]".*

14. En este apartado se detallan aquellas opciones / políticas de seguridad que deben configurarse obligatoriamente para la utilización de Cryhod en sistemas bajo el alcance del ENS:

ID	Valor de la politica
P2	*<number>2</number> <label>Disable Private Policies</label> <bool>True</bool>*
P102	*<number>102</number> <label>Disallow password accesses</label> <bool>True</bool>*
P103	*<number>103</number> <label> Disallow key file accesses</label> <bool>True</bool>*
P104	*<number>104</number> <label> Disallow cryptographic tokens accesses</label> <bool>False</bool>*
P105	*<number>105</number> <label>Disable CSP accesses</label> <bool>True</bool>*
P140	*<number>140</number> <label>Relax certificate chain CRL control</label> <bool>False</bool>*
P141	*<number>141</number> <label>Certificates restricted to roots</label> <list> <name>Example CA</name> <val>sha256=XXXXXXXX</val> </list> <list>*
P142	*<number>142</number> <label>Allow out-of-date certificates</label> <bool>False</bool>*

P144	*<number>144</number> <label>Force CRL refresh (hours)</label> <int>1</int>*
P146	*<number>146</number> <label>Relax key usage control for certificates</label> <bool>False</bool>*
P261	*<number>261</number> <label>Code attempts</label> <int>3</int>*
P264	*<number>264</number> <label>Emergency access mode (SOS/TP)</label> <int>1</int>*
P292	*<number>292</number> <label>Hash algorithm</label> <int>4</int>*
P383	*<number>383</number> <label>RSA encryption mode</label> <int>3</int>*
P801	*<number>801</number> <label> Enable standby mode </label> <bool>False</bool>*
P802	*<number>802</number> <label>Do not chain preboot credentials</label> <bool>True</bool>*
P803	*<number>803</number> <label>Preboot credentials chaining to ZoneCentral</label> <int>2</int>*
P804	*<number>804</number> <label>Preboot credential chaining period</label> <int>1</int>*
P805	*<number>805</number> <label>Delete after first chaining</label> <bool>False</bool>*
P822	*<label>Mandatory accesses options</label> <int>1</int>*
P825	*<number>825</number> <label>Enforce users rules</label> <int>0</int>*
P820	*<number>820</number> <label>Encryption directives</label> <list> <name>mount="C:"</name> <val>num=20;crypt=1;user=0;auto=1;mode=full</val> </list>*

```
<list>
        <name>mount="D:"</name>
        <val>num=30;crypt=1;user=0;auto=1;mode=full</val>
</list>
```

Nota: Completar con las unidades disponibles en el equipo.

15. Excepcionalmente, cuando Cryhod se configure **en sistemas aislados** que no dispongan de un sistema de gestión de credenciales de Cryhod centralizado *on-line* u *off-line* se permitirá la utilización de un usuario de recuperación cuyo acceso se realice mediante contraseña (P102). Esta contraseña debe ser modificada regularme (al menos cada 3 meses) o en caso de que haya sido comprometida. Los criterios de contraseña mínimos serán (P712 a P720):

    a. 10 caracteres de longitud
    b. 2 mayúsculas.
    c. 2 minúsculas.
    d. 1 carácter especial.
    e. 1 número.

4. GESTIÓN

16. Cryhod puede gestionarse tanto en modo local, mediante las políticas de equipo de Windows (*gpedit.msc*), como en modo centralizado, utilizando las políticas de seguridad de grupo del Directorio Activo.
17. Las operaciones de administración en el sistema quedan limitadas al usuario administrador del equipo y se requerirá autenticación para la realización de las mismas.

4.1 ACTUALIZACIONES

18. Cryhod permite la actualización de *software* sin necesidad de reinstalación.
19. El perfil Administrador puede actualizar el *software* del sistema si se proporcionan los ficheros de actualización adecuados.
20. Las actualizaciones de *firmware* y/o *software* solo deben ser realizadas por el administrador del equipo y se entregarán por medio del distribuidor a nivel nacional de Cryhod.
21. Las actualizaciones pueden afectar a la compatibilidad con versiones anteriores, por lo que en caso de duda se deberá consultar al distribuidor nacional de Cryhod.
22. Siempre debe realizarse una copia de seguridad de la información contenida en el equipo antes de proceder a una actualización.

5. SEGURIDAD

23. El equipo debe permanecer apagado cuando no esté en uso, es decir, Cryhod debe permanecer en estado **AUTENTICADO** solo cuando se está operando con él.

5.1 SMARTCARD PARA AUTENTICACIÓN

24. La tarjeta *SmartCard* utilizada para autenticarse en el equipo cifrado deberá cumplir las siguientes características:
    a. Estar cualificada para su utilización en sistemas del ENS nivel alto.
    b. Estar certificada, al menos, CC EAL4+ aumentado con ALC_DVS.2, ATE_DPT.2 y AVA_VAN.5.
    c. Algoritmos de hash SHA256 o SHA512
    d. Algoritmos de firma electrónica RSA, PKCS#1, RSASSA, PSS y ECDSA.
    e. Algoritmos de cifrado simétricos AES-192 y CMAC AES-192.
    f. Algoritmos de cifrado asimétricos RSA, clave entre 3072 y 3840 bits.
    g. Algoritmos de cifrado asimétricos ECC NIST P256, P384 y P521.
    h. Algoritmos cifrado asimétricos ECC *Brainpool* 256r1, 384r1 y 512r1.
25. La tarjeta criptográfica de la FNMT cumple con los requisitos exigidos en el párrafo anterior.
26. Los certificados digitales almacenados en la *SmartCard* deben tener las siguientes características:
    a. Algoritmo de hash SHA256 o SHA512.
    b. Algoritmo de cifrado asimétrico RSA con longitud de clave entre 3072 y 4096 bits.

5.2 ACCIONES TRAS UN COMPROMISO DE SEGURIDAD

27. Se considera un compromiso de seguridad la pérdida o sustracción de un equipo cuando se encuentra en estado **AUTENTICADO** aunque el equipo este hibernado, suspendido o bloqueado.
28. Adicionalmente a las acciones establecidas en la normativa vigente y documentación de procedimientos de emergencia del sistema. Cualquier compromiso deberá ser comunicado inmediatamente al Centro Criptológico Nacional, Departamento PYTEC (C/ Argentona 30, 28023 Madrid, soporte.ccn@cni.es) indicando en el asunto el termino Cryhod entre corchetes como se muestra a continuación **[CRYHOD]**.
29. Como norma general, si un equipo en estado AUTENTICADO se pierde, el usuario lo debe notificar lo antes posible a su AOSTIC y a la Autoridad Criptográfica Nacional (CCN) y enviar un informe del incidente por medios seguros.

30. Como norma general, si un equipo en estado APAGADO o PRE-BOOT se pierde, el usuario lo debe notificar lo antes posible a su AOSTIC.

31. En todo caso, la Autoridad Operacional del sistema deberá estar debidamente informada, y se llevará a cabo una investigación del incidente y una evaluación de daños.

6. REFERENCIAS

32. A continuación se indica la documentación del fabricante necesaria para la operación del software de cifrado de disco Cryhod de PRIMX y los documentos que han sido referenciados en este procedimiento:

	Referencia	Título
REF.	*PX18C964r3*	*Cryhod 2020 Installation guide EN (PX18C964r3)*
REF.	*PX18C960r3*	*Cryhod 2020 Memento Policies EN (PX18C960r3)*
REF.	*PX18C963r3*	*Cryhod 2020 Quick starting guide EN (PX18C963r3)*
REF.	*PX18C965r3*	*Cryhod 2020 User guide EN (PX18C965r3)*
REF.	*PX19A1161*	*PRIMX Cryhod PoC Tutorial (PX19A1161)r2.9*
REF.	*PX141438*	*Signing policies - Implementation Guide EN (PX141438) r2*
REF.	*np_cryhod_notetech*	*Recommandations pour une utilisation sécurisée de Cryhod*

7. ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad TIC
ECC	*Elliptic Curves Cryptography*
ENS	Esquema Nacional de Seguridad
NIST	*National Institute of Standards and Technology*
TIC	Tecnologías de la Información y las Comunicaciones

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL