centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos de STIC -
Anexo H: Requisitos para mecanismos criptográficos

Febrero de 2023

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.03.01 11:12:03 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5.
Fecha de Edición: febrero de 2023

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. La utilización de mecanismos criptográficos es habitual en la mayoría de productos y servicios IT que se utilizan en la actualidad. Sin embargo, la elección de los mecanismos es crítica para garantizar la confidencialidad e integridad de la información.
2. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a mecanismos criptográficos para ser incluidos dentro de los productos y servicios aprobados dentro del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el Centro Criptológico Nacional.
3. Dichos requisitos son **aplicables** a cualquier producto y servicio de seguridad y deben ser entendidos como **requisitos adicionales** que complementan a los requisitos definidos para cada una de las familias de productos incluidas en la taxonomía detallada en la presente guía.

2. DESCRIPCIÓN DE LOS REQUISITOS

2.1 REQUISITOS PARA CRIPTOGRAFÍA SIMÉTRICA

4. Se deberán emplear algoritmos con al menos 256 bits de seguridad.
5. Cualquier método de cifrado deberá incluir mecanismos que permitan garantizar la integridad de la información (cifrado autenticado).

2.2 REQUISITOS PARA CRIPTOGRAFÍA ASIMÉTRICA

6. La confidencialidad de un sistema o la integridad a largo plazo no deberán depender exclusivamente de criptografía asimétrica vulnerable a la computación cuántica.
7. Los protocolos de acuerdo de claves deberán hacer uso de esquemas híbridos para la derivación de claves. Se considera un esquema híbrido aquel que emplea una combinación de al menos dos de los siguientes mecanismos:

    a) Establecimiento de claves clásico (ej. DH, ECDH, etc.).

    b) Establecimiento de claves resistente a la computación cuántica.

    c) Claves pre-compartidas que puedan ser actualizadas.

    y los utiliza como entrada a una función KDF o en capas de acuerdo a metodologías de defensa en profundidad (securizando cada capa).
8. Si se utilizan algoritmos basados en factorización, como por ejemplo RSA, el tamaño mínimo del módulo deberá ser de 3072 bits.
9. En caso de utilizar algoritmos basados en curvas elípticas, estas deberán estar definidas sobre GF(p) y además el orden de los subgrupos usados será un primo de al menos 384 bits.

2.3 OTRAS REQUISITOS

10. El tamaño mínimo de bits para una **función de hash** deberá ser, en general, de al menos 384 bits, salvo en el caso especificado en el siguiente párrafo.
11. En el caso de que **la función de hash se utilice en funciones HMAC**, en funciones de derivación de claves o en funciones DRBG se aceptará el uso de tamaños de funciones de hash de 256 bits.
12. Se deberá proteger la integridad de la implementación de los mecanismos criptográficos en el producto de cifra.

3. ABREVIATURAS

CC	Common Criteria
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
DH	Diffie Hellman
DRBG	Generador de bits aleatorios determinístico
ECDH	Elliptic Curve Diffie Hellman – Cuvas elíptocas de Diffie Hellman
ENAC	Entidad Nacional de Acreditación
ENECSTI	Entidad Nacional de Evaluación y Certificación STIC
ENS	Esquema Nacional de Seguridad
GF(p)	Campo de Galois sobre primo “p”
HMAC	Código de autenticación de mensaje basado en funciones resumen.
KDF	Función de derivación de claves.
RFS	Requisitos Fundamentales de Seguridad
RSA	Rivest Shamir Adleman

PUBLICACIONES DE DEFENSA

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