

Criptología de empleo en el ENS

Anexo 1 - Prestadores de Servicios de Confianza





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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025



CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2025.10.15 12:18:31 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 4

2. AUTORIZACIÓN Y RECOMENDACIÓN 4

3. REFERENCIAS 5

1. INTRODUCCIÓN

El Centro Criptológico Nacional, en el marco de las competencias atribuidas en materia de seguridad criptológica, y tras la correspondiente evaluación técnica del sistema RSA y del grado de implantación del mismo en los prestadores de servicios de confianza, se informa lo siguiente:

- Se ha llevado a cabo un análisis de las vulnerabilidades existentes en el algoritmo.
- Se ha revisado el estado del arte de la seguridad del algoritmo RSA, tanto con medios tradicionales de cómputo, como bajo el supuesto de la aparición de un ordenador cuántico criptográficamente relevante.
- Asimismo, se ha considerado el grado de madurez del mercado y la disponibilidad de soluciones alternativas que permitiesen una transición algorítmica de firma electrónica con eficacia.

Una vez recopilados los resultados de las acciones descritas, se ha determinado extender el tiempo de autorización definido en las guías CCN-STIC 221 y CCN-STIC 807, para el algoritmo RSA con módulos de tamaño superior a 1900 bits pero inferior a 3000 bits, que actualmente figura con la fecha de 31/12/2025.

2. AUTORIZACIÓN Y RECOMENDACIÓN

Por lo tanto, se autoriza a los prestadores de servicios de confianza, el uso del algoritmo RSA para servicios de firma y autenticación con módulos de tamaño entre 1900 bits y 3000 bits hasta el 31 de diciembre de 2026, con una validez máxima de los certificados emitidos con este algoritmo y longitud, hasta el 31 de diciembre de 2028. A partir del 1 de enero de 2027, si aún se emiten certificados basados en RSA, se deberán emitir con módulos de al menos 3000 bits.

Asimismo, para los algoritmos de firma digital basados en RSA, se recomienda el uso del esquema RSA-PSS tal y como está definido en la CCN-STIC-221, aunque conviene aclarar que también se acepta, al menos hasta el 31 de diciembre 2030, el uso del algoritmo RSA-PKCS#1v1.5.

No obstante, en virtud del principio de mejora continua de la ciberseguridad y de las recomendaciones técnicas emitidas por organismos internacionales y del propio Centro Criptológico Nacional, se insta a los organismos responsables a proceder a la implementación de mecanismos más robustos para mecanismos de clave asimétrica (RSA de mayor longitud y algoritmos postcuánticos) a la mayor brevedad posible.

3. REFERENCIAS

- [1] CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad.
URL: <https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>

- [2] CCN-STIC-221 Mecanismos criptográficos autorizados por el Centro Criptológico Nacional.
URL: <https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6954-ccn-stic-221-guia-de-mecanismos-criptograficos-autorizados-por-el-ccn-1/file.html>

- [3] ECCG Sub-group on Cryptography. Agreed Cryptographic Mechanisms - version 2. 2025.
URL: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

