PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 15 MAI 2024
N° 920 /ANSSI/SDE/NP

NOTE

relative à la délivrance par les prestataires de services de confiance qualifiés par l'ANSSI de certificats électroniques mettant en œuvre des clés cryptographiques RSA 2048 bits après le 31 décembre 2025

Références :

1. Règlement européen n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Disponible sur https://eur-lex.europa.eu.
2. Référentiel d'exigences, prestataires de services de confiance qualifiés, version 1.2 du 5 juillet 2017. Disponible sur https://cyber.gouv.fr.
3. *SOGIS Agreed Cryptographic Mechanisms*, version 1.3 de février 2023. Disponible sur https://sogis.eu.
4. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, référence ANSSI PG 083, version 2.04 du 1er janvier 2020.

1. Contexte

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) qualifie des prestataires de services de confiance au titre du règlement cité en première référence.

Le chapitre II.3.6 du référentiel cité en deuxième référence exige que les algorithmes et mécanismes cryptographiques mis en œuvre par les prestataires de services de confiance qualifiés soient conformes au document cité en troisième référence qui dispose que la date limite pour l'utilisation d'une clé RSA dont la taille du module est supérieure à 1900 bits et inférieure à 3000 bits est fixée au 31 décembre 2025[1].

[1] *Note 27-LegacyRSA. The acceptability deadline for the legacy use of modulus of size above 1900 bits, but less that 3000 bits, is set to December 31, 2025*

Certains prestataires de services de confiance qualifiés par l'ANSSI qui délivrent des certificats de signature, de cachet et d'horodatage électronique délivrent encore à ce jour des certificats électroniques dont la taille du module de la clé RSA est de 2048 bits et dont la date de fin de validité est postérieure au 31 décembre 2025.

Cette note clarifie les conditions d'émission, au-delà du 31 décembre 2025, de certificats de signature, de cachet et d'horodatage électronique dont la taille du module est comprise entre 1900 et 3000 bits par les prestataires de services qualifiés par l'ANSSI.

2 Clarification et recommandation

La date du 31 décembre 2025 doit être considérée comme une date limite d'acceptabilité dans le cadre d'une évaluation de sécurité. Ainsi, les prestataires de services de confiance qualifiés par l'ANSSI qui délivrent des certificats de signature, de cachet et d'horodatage électronique :

PEUVENT jusqu'au 31 décembre 2025 émettre des certificats mettant en œuvre l'algorithme RSA dont la taille du module de la clé est comprise entre 1900 et 3000 bits à condition que ces certificats aient une durée de validité de trois ans maximum ;

DOIVENT à partir du 1er janvier 2026, s'ils émettent des certificats mettant en œuvre l'algorithme RSA, n'émettre que des certificats dont la taille du module de la clé est supérieure ou égale à 3000 bits.

En conséquence, il est recommandé que les prestataires de services de confiance qualifiés par l'ANSSI mettent en œuvre dans les meilleurs délais, et dans tous les cas le 31 décembre 2025 au plus tard, les mesures leur permettant de respecter les échéances énoncées ci-dessus. Le non-respect de ces échéances par un prestataire de services de confiance qualifié entraînera le retrait par l'ANSSI de sa qualification.

Les dispositions énoncées ci-dessus sont conformes aux exigences de l'ANSSI en matière de choix et de dimensionnement des mécanismes cryptographiques définies dans le document cité en quatrième référence.

Renaud LABELLE
Sous-directeur Expertise

Diffusion interne (par messagerie)

ANSSI DG – SDE/PSS – SDE/DIT – SDE/PSS/BQA – SDS/MSN/ICARE – SDE/DST/LCR
SDE/SEC - Mathieu JORRY- chrono informatique