



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SC-12(03)

Clés asymétriques

Juill. 2026



Sécurité des communications et des systèmes

System and Communications Protection

SC-12(03) – Clés asymétriques (PaF-)

Énoncés :

Produire, contrôler et distribuer les clés cryptographiques asymétriques en faisant appel à [Sélection (un choix) : des processus de gestion des clés approuvés par le Centre pour la cybersécurité; du matériel de chiffrement préplacé; des certificats d'ICAP à assurance moyenne approuvés ou émis par le Centre pour la cybersécurité; des certificats d'ICP et des jetons de sécurité matériels qui protègent la clé privée de l'utilisatrice ou utilisateur; des certificats émis conformément aux exigences définies par l'organisation].

Responsable : Aucun

Discussion :

L'ITSP.40.111 fournit des recommandations pour les spécifications approuvées de la cryptographie asymétrique et recommande que les mises en œuvre, y compris la génération de clés, soient effectuées dans des modules cryptographiques validés selon le PVMC. L'ITSP.40.062 offre des conseils sur la gestion des clés asymétriques dans une ICP.