



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

IA-05(02)

Authentification basée sur clé publique

Juill. 2026



Contrôle de l'identité et de l'authentification

Identification and Authentication

IA-05(02) – Authentification basée sur clé publique (PbM-)

Énoncés :

- a. Pour une authentification basée sur clé publique :
 - 1. appliquer la procédure d'accès autorisé à la clé privée correspondante
 - 2. associer l'identité authentifiée au compte d'une personne ou d'un groupe
- b. Lorsque l'infrastructure à clé publique (ICP) est utilisée :
 - 1. valider les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé, y compris la vérification de l'information d'état des certificats
 - 2. utiliser une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins

Responsable : Aucun

Discussion :

La cryptographie à clé publique est un mécanisme d'authentification valide pour les personnes, les machines et les dispositifs. Pour ce qui est des solutions d'ICP, l'information d'état pour les chemins de certification comprend les listes de certificats révoqués ou les réponses du protocole d'état de certificat. Utiliser une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins soutient également la disponibilité du système dans des situations où les organisations ne sont pas en mesure d'avoir accès à l'information révoquée par le réseau.