



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-17(07)

Structure relative au droit d'accès minimal

Juill. 2026



Acquisition sécurisée des systèmes/services

System and Services

SA-17(07) – Structure relative au droit d'accès minimal (PbMM)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte structure le matériel, les logiciels et les micrologiciels servant à la sécurité de manière à faciliter le contrôle de l'accès avec le droit d'accès minimal.

Responsable : Aucun

Discussion :

Le principe de droit d'accès minimal repose sur le fait que l'on doit affecter suffisamment de privilèges à chaque composant pour lui permettre d'accomplir ses fonctions, mais sans plus (voir le contrôle SA-08(14)). L'application du principe de droit d'accès minimal limite la portée des actions du composant, ce qui a deux effets désirables. Dans un premier temps, l'incidence sur la sécurité advenant la défaillance, la corruption ou une mauvaise utilisation du composant du système est limitée. Dans un second temps, l'analyse de la sécurité du composant est simplifiée. Le principe de droit d'accès minimal est un principe omniprésent qui se reflète dans tous les aspects de la conception d'un système sécurisé. Les interfaces utilisées pour appeler les capacités du composant ne sont accessibles que par certains sous-ensembles de la population d'utilisatrices et utilisateurs, et la conception du composant prend en charge un degré de granularité suffisamment précis pour assurer la décomposition des privilèges. Par exemple, dans le cas d'un mécanisme de vérification, on pourrait retrouver une interface pour la ou le gestionnaire des vérifications qui configure les paramètres des vérifications, une interface pour l'exploitante ou exploitant des vérifications qui s'assure que les données de vérification sont collectées et stockées en toute sécurité et, pour finir, une autre interface pour la vérificatrice ou le vérificateur des vérifications qui doit afficher les données de vérification collectées sans toutefois effectuer d'opérations à partir de ces données. En plus de ses manifestations dans l'interface du système, le principe de droit d'accès minimal peut être utilisé comme principe directeur pour la structure interne du système en tant que tel. Un aspect du droit d'accès minimal interne est de construire des modules de manière à ce que seules les fonctions d'un module puissent effectuer des opérations directes sur les éléments encapsulés par ce module. Il est possible d'accéder indirectement aux éléments externes à un module susceptibles d'être touchés par l'exploitation de ce module dans le cadre d'une interaction (par exemple, lors d'un appel de fonction) avec le module qui contient ces éléments. Un autre aspect du droit d'accès minimal interne veut que la portée d'un module ou d'un composant donné comprenne uniquement les éléments du système qui sont nécessaires pour son fonctionnement et que les modes d'accès des éléments (par exemple, lecture, écriture) soient minimaux.