OPENTRUST™

L'ANSII remet son premier certificat Critères Communs à OpenTrust pour sa solution OpenTrust-PKI qui répond désormais aux critères de certification internationale les plus stricts

Opentrust PKi est la seule solution de PKI française certifiée Critère Communs

Paris, le 16 juillet : OpenTrust, fournisseur mondial de logiciels d'écosystèmes informatiques ouverts et sécurisés annonce aujourd'hui que la solution OpenTrust PKI a reçu la certification Critères Communs niveau EAL 3+.

Depuis un an, OpenTrust a travaillé à l'obtention de la certification critères communs dont l'évaluation a été confiée à OPPIDA, l'organe d'évaluation pour la certification Critères Communs. Cette certification, remise par la toute récente ANSSI (Agence Nationale pour la Sécurité des Services Informatiques), démontre bien la volonté d'OpenTrust de répondre aux standards internationaux de sécurité les plus stricts.

Les Critères Communs sont reconnus dans le monde entier en matière d'évaluation des fonctionnalités et des capacités de sécurité des solutions informatiques. Aujourd'hui, grâce au CCRA (Common Criteria Recognition Agreement), les certificats des critères communs sont reconnus dans plus de 25 pays, dont les Etats-Unis. Les certifications EAL, ne s'appliquant qu'aux produits, ont été créées dans le but de valider que l'architecture et la conception des produits est bien conforme aux règles de sécurité visant à protéger les systèmes informatiques contre les menaces.

La certification Critères Communs vient concrétiser, pour les clients, la fiabilité et la sureté de l'Ecosystème de confiance OpenTrust. La solution certifiée est officiellement conforme aux critères stricts de sécurité tout en restant en phase avec la vision d'OpenTrust : des transactions de confiance, pour tous, sur tous les supports et tous les réseaux.

Les entreprises désireuses de protéger leurs données sensibles et les agences gouvernementale du monde entier sont de plus en plus nombreuses à baser leur décision d'achats sur la certification des Critères Communs.

« OpenTrust continue à mettre en priorité absolue le respects des normes de sécurité les plus exigeantes dans ses produits clients. Cette certification Critères Communs vient récompenser des années d'efforts de nos équipes de R&D.», explique Sherley Brothier, VP R&D chez OpenTrust.

Selon Patrick Pailloux, directeur général de l'ANSSI, « la reconnaissance accordée à la solution PKI d'OpenTrust via la certification Critères Communs est non seulement une belle réussite mais également un excellent indicateur du niveau de sécurité que délivre le produit. »

A propos d'OpenTrust : OpenTrust, fondé en 2001, est un leader mondial émergeant qui conçoit et développe des solutions de mise en place d'écosystèmes informatiques de confiance. La suite logicielle d'OpenTrust fait de la gestion d'identité le cœur de l'infrastructure informatique, couplant ainsi sécurité, fiabilité, évolutivité et productivité aux nouveaux standards.

Les solutions d’OpenTrust sont faciles à mettre en place et permettent aux entreprises de rentabiliser leurs investissements dans les technologies IAM. OpenTrust compte parmi ses clients quelques unes des 500 plus grandes entreprises européennes, des organes gouvernementaux traitant des données extrêmement sensibles (sécurité nationale, énergie nucléaire, transactions financières, lignes aériennes etc.) et des entreprises recherchant tout simplement à renforcer la protection de leurs données.

A propos de l’ANSII : l’agence nationale de la sécurité des systèmes d’information (ANSSI) se substitue à la direction centrale de la sécurité des systèmes d’information (DCSSI) du secrétariat général de la défense nationale (SGDN) et ses attributions sont élargies.
Désormais, outre les missions assurées auparavant par la DCSSI, l’ANSSI assure la mission d’autorité nationale en matière de sécurité des systèmes d’information. A ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d’information de l’État et de vérifier l’application des mesures adoptées.
Dans le domaine de la défense informatique, elle assure un service de veille, de détection, d’alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l’État.