IDmachines et INCERT s'attaquent aux clés cryptographiques vulnérables des systèmes de sécurité physique



Le partenariat cible les clés et certificats cryptographiques faibles, partagés ou oubliés présents dans plus de 100 millions d’équipements de sécurité physique en Amérique du Nord et plus d’un milliard dans le monde.

Rien qu’en Amérique du Nord, bien plus de 100 millions d’équipements de sécurité physique n’utilisent pas de cryptographie ou l’utilisent de manière inappropriée. Il s’agit notamment des lecteurs de badges, des contrôleurs de portes et des caméras qui protègent les immeubles de bureaux, les hôtels, les habitations, les personnes et les infrastructures critiques. IDmachines et INCERT annoncent aujourd’hui une nouvelle étape de leur partenariat pour combler cette lacune. Les deux partenaires apporteront des services de gestion de clés et de certificats cryptographiques à haut niveau d’assurance au contrôle d’accès, à la vidéosurveillance et à l’ensemble du marché de la sécurité physique.

Chaque équipement de sécurité physique repose, ou devrait reposer, sur des clés et des certificats cryptographiques. Ces identifiants permettent à un équipement de prouver son identité et de

protéger les données en transit ou stockées. Dans l'ensemble du secteur, ils sont trop souvent partagés entre plusieurs équipements, oubliés après l'installation ou autosignés sans contrôle adéquat. Le cloud, l'intelligence artificielle et les technologies post-quantiques transforment aujourd'hui le secteur de la sécurité physique. Pourtant, de nombreux équipements installés restent vulnérables.

La gestion de ces identifiants n'a jamais été simple pour les propriétaires de systèmes, les intégrateurs et les fabricants. IDmachines et INCERT entendent changer la donne.

L'offre associe deux ensembles de compétences complémentaires. IDmachines apporte sa plateforme Eidola, qui découvre, évalue, surveille et gère les équipements de sécurité physique. INCERT fournit l'infrastructure de confiance sur laquelle repose Eidola, avec QORI, sa plateforme PKI (infrastructure à clés publiques), et Keys&More, son système de gestion de clés, tous deux conçus pour des opérations cryptographiques à haut niveau d'assurance. Les organisations disposent ainsi d'un moyen unifié et sécurisé de gérer leurs clés et certificats, adapté aux réalités opérationnelles et techniques du secteur de la sécurité physique. L'infrastructure de confiance peut être déployée en mode service, sur site ou selon un modèle hybride. Elle prend également en charge les standards cryptographiques les plus répandus (PKCS, JOSE et COSE) pour les clés et certificats cryptographiques d'aujourd'hui et de demain.

L'offre se déploie en trois étapes :

- **Identifier les points faibles**. Eidola analyse les équipements de sécurité physique à l'aide de protocoles standardisés. La plateforme dresse un inventaire de la cryptographie utilisée et signale les clés et certificats autosignés, partagés ou arrivant à expiration. Cette évaluation fournit aux organisations un rapport fondé sur les normes ISO, qui facilite la conformité en matière de transparence, de cybersécurité et de protection de la vie privée.
- **Émettre des identifiants de confiance**. Le Front Layer de la plateforme fournit des notifications au niveau de l'organisation et de chaque équipement. Chaque équipement est enregistré avec son contrôleur dans l'IDmachines Controller Registry. Les clés et certificats sont ensuite émis par l'autorité de certification propre au client et rattachés à l'organisation propriétaire des équipements.
- **Assurer leur sécurité dans la durée**. IDmachines gère le cycle de vie des clés et des certificats avec QORI et Keys&More d'INCERT, en tant que service géré, sur site ou selon un modèle hybride. Chaque certificat est déployé, validé, renouvelé et révoqué en temps voulu.

L'offre s'adapte ainsi à chaque client, à chaque canal de distribution et à chaque environnement technologique fournisseur. Les clients peuvent gérer leur propre hiérarchie de certificats, faire appel à IDmachines comme autorité racine ou travailler avec un prestataire tiers.

IDmachines et INCERT collaborent depuis plus de dix ans. Parmi les jalons de cette collaboration figurent la validation de certificats X.509 en 2014, des applications anti-contrefaçon de la cryptographie en 2017, la validation des signatures numériques de nouvelle génération des ePassports en 2019 et la gestion de clés pour les équipements de sécurité physique en 2022.

En juin 2026, les dirigeants des deux organisations ont officialisé un accord de partenariat qui pose les bases de cette nouvelle étape.

La première offre cible les contrôleurs Mercury MP dans le cadre du Mercury Embedded Application Program. Elle sera ensuite étendue aux caméras, aux contrôleurs et aux autres équipements du parc installé. Les sites pilotes sont les bienvenus. IDmachines et INCERT ont présenté l'offre lors de MercTech 2026, en octobre, à San Diego.

« Chacun sait protéger ses clés physiques. Les clés cryptographiques présentes dans chaque lecteur, contrôleur et caméra méritent le même soin », déclare Salvatore D'Agostino, PDG d'IDmachines. *« En associant les solutions cryptographiques d'INCERT à notre expérience de la gestion des équipements de sécurité physique, nous rendons une protection à haut niveau d'assurance plus accessible et plus rentable pour les organisations de l'ensemble du marché. »*

« Les équipements de sécurité physique méritent le même niveau de confiance que les systèmes utilisés pour protéger l'identité de chaque citoyen. Nous mettons les services de PKI et de gestion de clés qu'INCERT opère pour les services publics nationaux au service des équipements qui protègent les personnes, les bâtiments et les infrastructures critiques », déclare Clément Gorlt, directeur PKI chez INCERT.