M-TRUST

Objets connectés Opérateurs mobiles

Sécurisation de l'identité des objets et des communications pour les périphériques IoT

Le secteur IoT devrait atteindre 20,4 milliards d’appareils d’ici 2020, connectés à des réseaux cellulaires ou non et échangeant des tonnes de données. De nouvelles préoccupations de sécurité émergent concernant la confidentialité, l'intégrité et le contrôle des informations partagées. M-TRUST est la solution d’IDEMIA pour assurer une sécurité de bout en bout du périphérique connecté au cloud.

Aujourd'hui, la grande majorité des objets connectés ne sont pas correctement sécurisés. Les cyberattaques représentent un risque pour la réputation de la marque et les revenus d’une entreprise, mais peuvent également menacer la sécurité des personnes. Pour assurer le niveau de sécurité approprié, les principaux acteurs du secteur de l'Internet des objets doivent relever plusieurs défis: authentification de l'expéditeur et du destinataire, protection de l'intégrité des dispositifs et des données, confidentialité des informations et confidentialité.

Notre offre :

M-TRUST est une plate-forme de serveur en nuage qui permet la gestion sécurisée des objets connectés. Cela garantit que les données échangées ne seront ni falsifiées ni lues par des tiers non autorisés.
Cette solution indépendante du réseau s’adresse aux réseaux cellulaires (3G / 4G / 5G / Cat M1 / NB-IoT) et non cellulaires (LoRa / Sigfox / à courte portée). Quel que soit le réseau de communication utilisé, M-TRUST identifie de manière sécurisée les périphériques et les serveurs et assure un cryptage authentifié pour des échanges sécurisés de données et de commandes. Il empêche les atteintes à la sécurité, telles que le clonage de périphérique, qui fournit un point d’entrée pour le code malveillant ou l’exploration de données.
Combiné aux services de surveillance à distance, M-TRUST fournit des fonctionnalités avancées pour garantir l’intégrité des données, des fonctions et des périphériques, telles que le démarrage sécurisé pour la mise à jour logicielle et mettre en œuvre l'évolution des normes de sécurité.

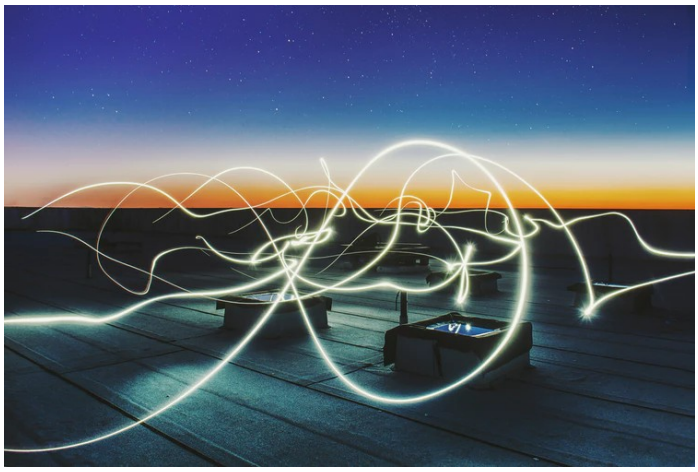
Reconnu comme un acteur majeur de la sécurité, IDEMIA tire parti de son expertise en gestion de la connectivité à distance et en signature logicielle numérique pour l'étendre à la gestion de la sécurité à distance des périphériques connectés. En tant que principal acteur de l'écosystème de l'Internet des objets, IDEMIA a noué de solides partenariats stratégiques pour traiter l'ensemble du marché.

Avantages :

Hautement sécurisé
Géré dans nos centres de données certifiés en tant que service (SaaS) ou déployé en tant que plate-forme externalisée, M-TRUST apporte une sécurité de haut niveau de bout en bout.

Pratique
M-TRUST permet l'administration de périphériques à distance avec un provisionnement simplifié au stade de la fabrication pour les OEM / ODM et une gestion optimisée du cycle de vie des périphériques pour les applications, les opérateurs de réseau et les fournisseurs de services.

Guichet unique
IDEMIA fournit des solutions de sécurité de l'objet connecté au cloud. Il n'est plus nécessaire de rassembler différents produits de plusieurs fournisseurs.



Comment ça fonctionne ?

Avec une offre complète d'éléments sécurisés (par exemple, SIM / eUICC / eSE / etc ...), TEE (Trusted Execution Environment) et le middleware associé, protégeant les données et les clés stockées dans les appareils terminaux, M-TRUST propose un ensemble complet des services de sécurité, y compris la création et la gestion des identités numériques des objets connectés (clés, certificats numériques).
L'intégration et l'activation de périphériques peuvent être facilement réalisées via le provisionnement initial à distance. Les commandes sécurisées, la configuration des périphériques et la rotation des clés sont également disponibles via les services d'administration à distance.
Ces services sont accompagnés de nombreuses notifications attestant de la bonne exécution du périphérique.