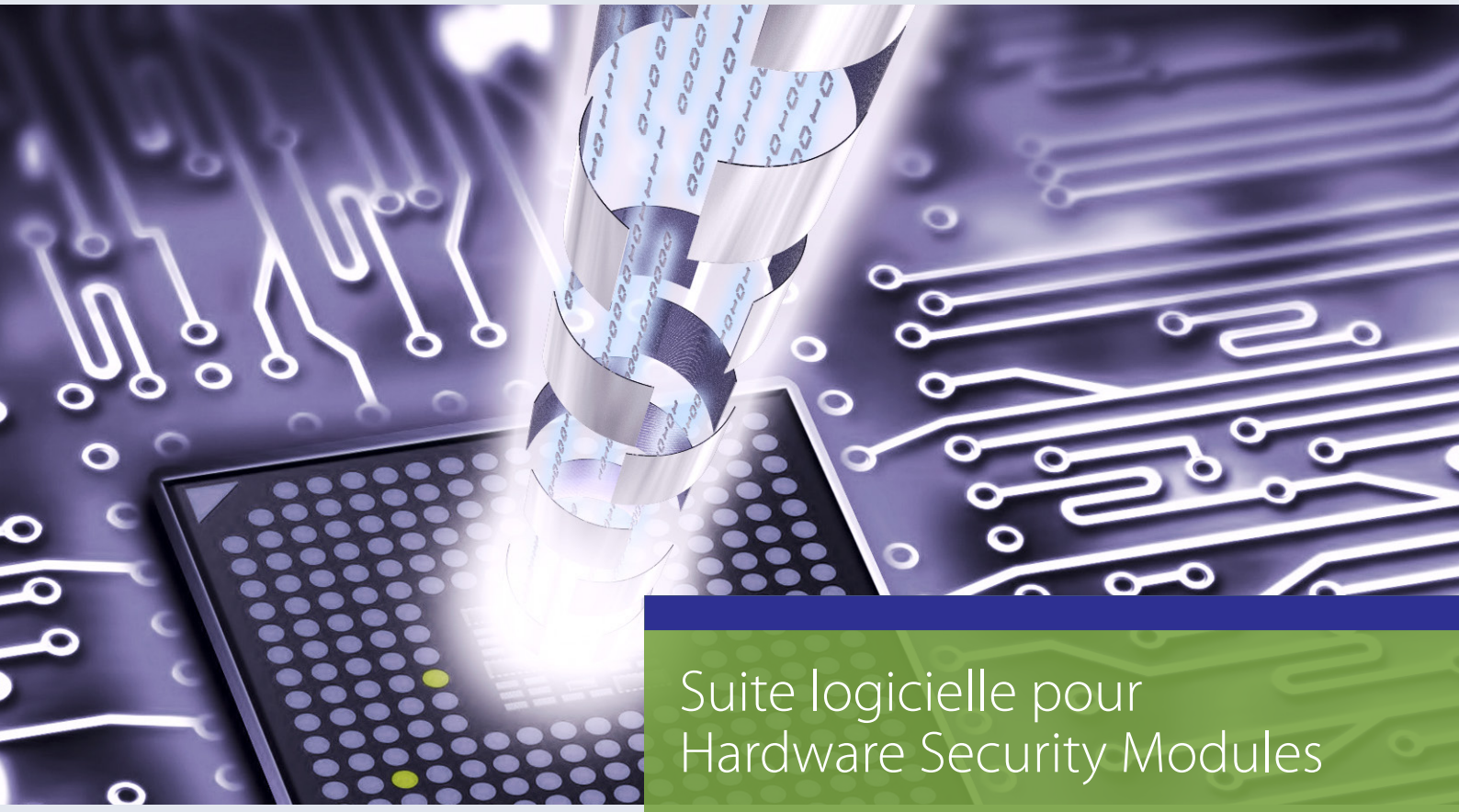
escrypt
SECURITY. TRUST. SUCCESS.

CycurHSM



Suite logicielle pour Hardware Security Modules

Présentation

Au niveau ECU, les solutions de sécurité simples implémentées dans les logiciels ne protègent pas suffisamment l'intégrité d'un système sécurisé. Les HSM sont les prérequis nécessaires au durcissement des systèmes embarqués contre les attaques, permettant d'assurer la protection de l'intégrité du logiciel.

CycurHSM est une suite logicielle complète adaptée aux implémentations disponibles du HSM Bosch par différents fabricants de silicium. CycurHSM offre la technologie permettant de répondre aux exigences d'un firmware HSM flexible fournissant des interfaces ouvertes et standardisées (ex. : CSM AUTOSAR) aux applications de sécurité renforcées avec HSM.

ESCRYPT possède une vaste expérience de la mise en œuvre des HSM à travers une longue histoire de projets industriels et de recherche. CycurHSM fournit un logiciel HSM hautement optimisé qui assure le plus haut niveau de sécurité des calculateurs.

ESCRYPT 2019/09

escrypt
SECURITY. TRUST. SUCCESS.

CycurHSM

Détails

Généralités

Prend en charge toutes les implémentations disponibles du HSM Bosch :

- Fournit une API standardisée pour accéder au HSM
- Utilisation de tous les accélérateurs matériels disponibles (TRNG, moteur AES-128 bits)
- Débogage sécurisé sous contrôle du HSM
- Prise en charge des applications de sécurité (boot sécurisé, flashage sécurisé, débogage sécurisé, etc.)
- Architecture logicielle en couches basée sur un système d'exploitation temps réel certifié ISO 26262
- Intégration de CycurLIB d'ESCRYPT pour fournir des primitives cryptographiques supplémentaires (Hashing, MAC, RSA, ECC)
- Structure modulaire pour adapter directement le logiciel au besoin du client
- Encapsulation de tous les mécanismes de sécurité pour utiliser pleinement la fonctionnalité principale du HSM
- Mise à disposition d'un environnement d'exécution sécurisé et protégé par le matériel
- Prise en charge complète des technologies HSM
- Entièrement programmables, des applications client supplémentaires peuvent être facilement intégrées dans le HSM

Composant RTA-OS

- RTA-OS est un système d'exploitation temps réel spécialement conçu pour répondre à toutes les exigences des calculateurs automobiles
- Aujourd'hui, les solutions RTA alimentent plus de 1 milliard de calculateurs sur les routes

Conforme à AUTOSAR

- Intégration facile dans AUTOSAR en tant que gestionnaire de services cryptographiques (CSM), y compris les pilotes de dispositifs HSM côté hôtes (couche CRY) et une interface PKCS#11 pour les applications hors AUTOSAR

Caractéristiques et avantages

- La conception est basée sur un système d'exploitation temps réel pour assurer les caractéristiques temps réel du HSM
- Stockage protégé blindé pour clés cryptographiques ou journalisation sécurisée
- Encapsulation de toutes les fonctions de sécurité requises pour satisfaire un large éventail d'exigences de sécurité automobile
- Mis en œuvre pour répondre aux normes de qualité les plus élevées
- Plateforme de co-conception matérielle/logicielle puissante pour des applications client spécifiques aux exigences cryptographiques haute performance
- Configuration spécifique client possible