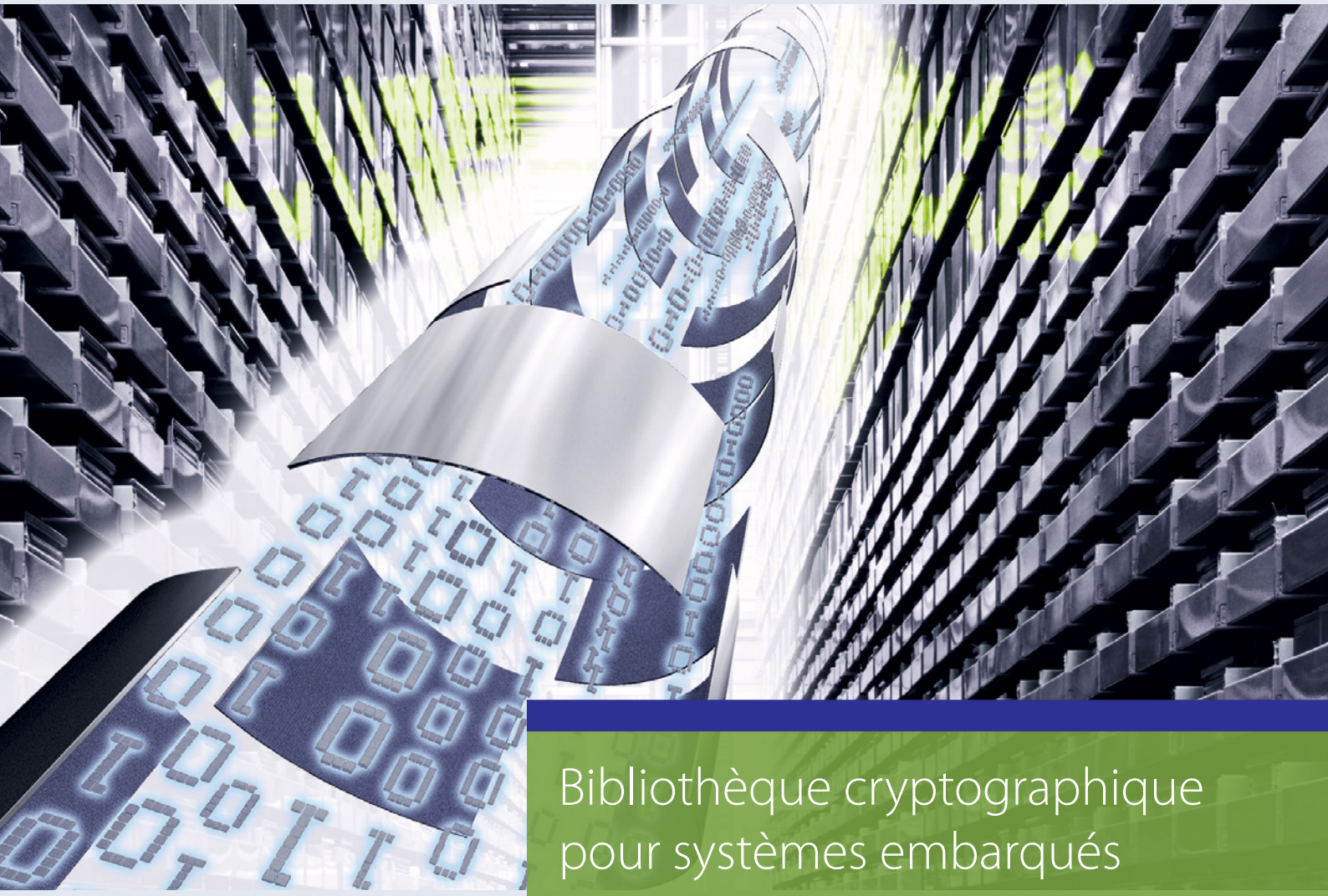
escrypt
SECURITY. TRUST. SUCCESS.

CycurLIB



Bibliothèque cryptographique pour systèmes embarqués

Présentation

Les protocoles et algorithmes cryptographiques constituent la base fondamentale de la plupart des applications de sécurité informatique. Par exemple, des algorithmes cryptographiques tels que la vérification de la signature numérique sont nécessaires pour les solutions flash sécurisées, l'activation des fonctions et le boot sécurisé. La bibliothèque cryptographique est utilisée comme base pour toutes les solutions de sécurité embarquées.

CycurLIB intègre des implémentations très efficaces des fonctions cryptographiques courantes. De plus, CycurLIB est développé par des processus conformes à la norme ASPICE et est conforme aux normes MISRA et ANSI.

CycurLIB est couramment utilisé dans de nombreux produits à grands volumes de production, par exemple dans l'industrie automobile, les équipements médicaux et la construction de machines.

CycurLIB fournit des algorithmes cryptographiques pertinents optimisés pour la taille de code tout en respectant des contraintes de performance strictes.

CycurLIB peut facilement être utilisé pour sécuriser vos produits, par exemple en vérifiant les signatures pour déterminer l'authenticité et l'intégrité des données. CycurLIB est hautement configurable selon les besoins du client (avec un outil de configuration conforme à AUTOSAR).

ESCRYPT 2019/09

escrypt
SECURITY. TRUST. SUCCESS.

Détails

Généralités

- Mise en œuvre selon les normes MISRA-C:2012 et ANSI-C
- Optimisé pour la taille de code tout en respectant des contraintes de performances strictes
- Composants conformes à HIS Source Code Metrics
- Processus de développement conformes à la norme ASPICE
- Conformité AUTOSAR
  - Outil de configuration conforme AUTOSAR
  - Mapping mémoire conforme AUTOSAR
- Facile à intégrer dans votre produit
- API intuitive
- Structure modulaire pour adapter directement le logiciel
- Bien documenté

Algorithmes cryptographiques disponibles

- AES
  - Taille des clés prises en charge : 128 bits, 192 bits, 256 bits
  - Modes de fonctionnement pris en charge : CBC, GCM
- Algorithmes de hachage
  - SHA-224, SHA-256, SHA-384, SHA-512
- MAC
  - HMAC-SHA2
  - CMAC-AES
  - Siphash
- ECC avec Curve25519
  - Accord de clé Diffie-Hellman
  - Génération de paire de clés
- RSA
  - Moduli : 1024 bits, 2048 bits, 3072 bits, 4096 bits
  - Programmes de signature RSA pris en charge : PKCS#1 RSASSA-PSS, PKCS#1 RSASSA-V1_5

Plateformes prises en charge

- Toute plate-forme fournissant un compilateur conforme à ANSI-C – de 8 à 64 bits

Caractéristiques et avantages

- Intégration fluide dans les produits existants
- Prend en charge tous les algorithmes cryptographiques communs et les normes de certificat
- Mis en œuvre pour répondre aux normes de qualité les plus élevées
- Faible encombrement
- Modularité
- Fonctionne sur toutes les plateformes

Amélioration et adaptation continues

- Extensions/Modifications : enrichissement en fonction des tendances du marché et des besoins clients
- Adaptions aux HSM/Microcontrôleurs sécurisés : adapter la mise en œuvre pour utiliser l'accélération matérielle

Personnalisation

- Veuillez nous contacter pour toute question concernant les extensions et les modifications