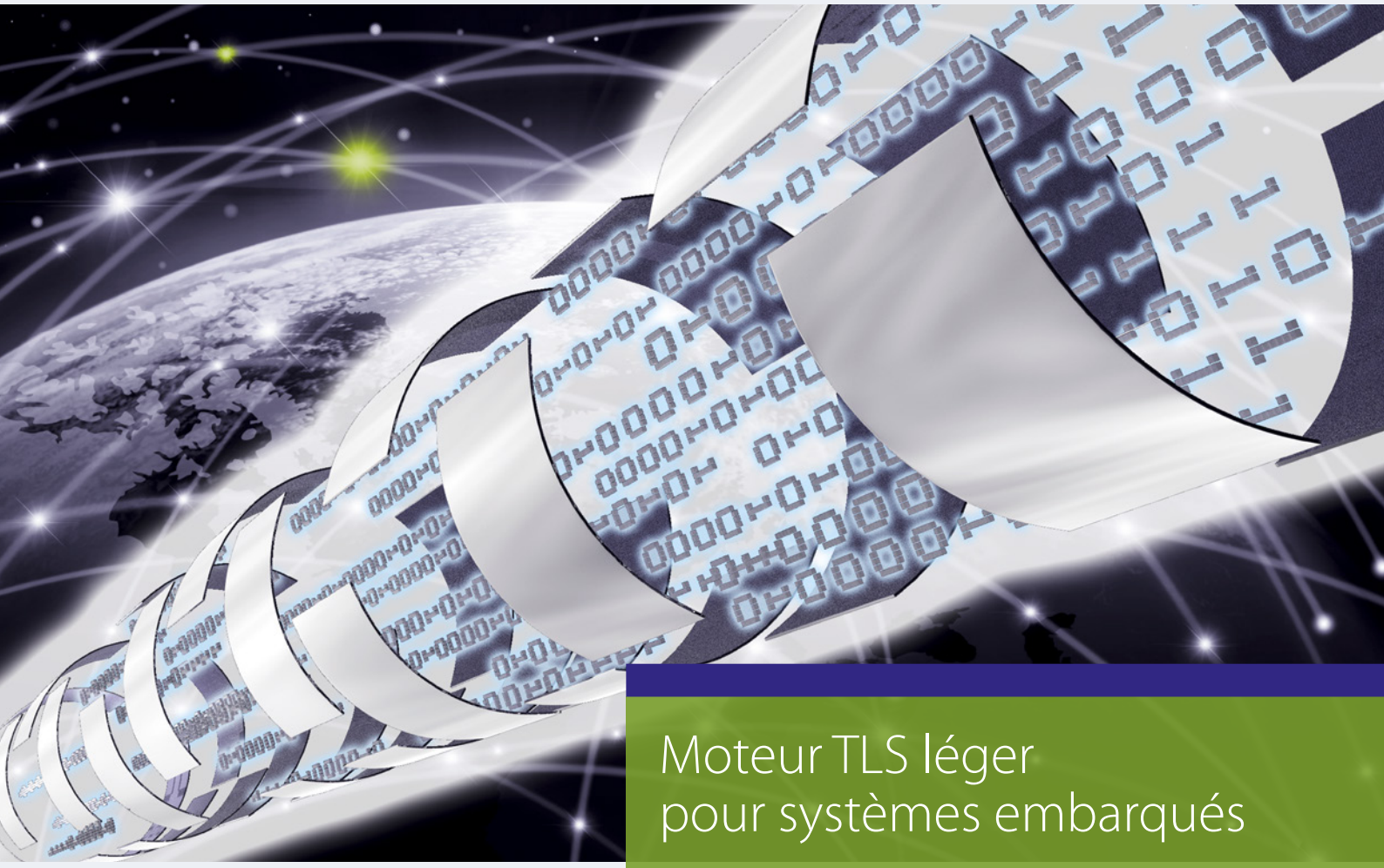
escrypt
SECURITY. TRUST. SUCCESS.

CycurTLS



Moteur TLS léger pour systèmes embarqués

Présentation

A l'heure où les réseaux ne cessent de se développer, la transmission de données confidentielles est de plus en plus cruciale. Une solution bien établie pour sécuriser une connexion est le protocole TLS (Transport Layer Security, anciennement connu sous le nom de SSL) qui assure l'authentification, l'intégrité et la confidentialité. Bien qu'il soit largement utilisé pour protéger les connexions Web via HTTPS, le protocole TLS est de plus en plus présent dans l'univers des systèmes embarqués.

CycurTLS est une mise en œuvre efficace des protocoles TLS et DTLS. Il est conçu plus particulièrement pour être utilisé dans des systèmes embarqués qui ne disposent généralement que d'une faible quantité de mémoire disponible.

CycurTLS est basé sur la bibliothèque cryptographique performante d'ESCRYPT, CycurLIB, qui permet à CycurTLS d'être très rapide et peu volumineux. La mise en œuvre du protocole est très légère et ne fournit pas de fonctionnalités facultatives inutiles comme la compression.

CycurTLS est entièrement conforme aux normes TLS 1.2 et DTLS 1.2 et satisfait à toutes les exigences de sécurité de l'IETF.

CycurTLS est très flexible et offre un support pour tout type de mode de transport. De cette manière, CycurTLS ne se limite pas au TCP et à l'UDP, mais peut également être utilisé avec d'autres couches de transport.

CycurTLS est compatible avec d'autres implémentations TLS, ce qui lui assure une flexibilité pour une utilisation polyvalente.

CycurTLS se configure facilement selon les besoins du client. Seuls les algorithmes nécessaires sont donc utilisés, tout en assurant la sécurité exigée de votre produit.

ESCRYPT 2019/09

escrypt
SECURITY. TRUST. SUCCESS.

CycurTLS

Détails

Généralités

- Mise en œuvre selon les normes IETF et ANSI-C
- Conforme à MISRA-C:2012
- Optimisé pour la taille de code, tout en respectant des contraintes de performances strictes
- Côté client et serveur
- Facile à intégrer dans votre produit
- API intuitive
- Modulaire
- Bien documenté

Cipher Suites disponibles

- Courbe elliptique Diffie-Hellman :
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_ CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Transport clé RSA :
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CCM_8
  - TLS_RSA_WITH_AES_256_CCM_8
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_NULL_SHA256
- Clés pré-partagées :
  - TLS_PSK_WITH_AES_128_CBC_SHA
  - TLS_PSK_WITH_AES_256_CBC_SHA
  - TLS_PSK_WITH_AES_128_CBC_SHA256
  - TLS_PSK_WITH_AES_128_CCM_8
  - TLS_PSK_WITH_AES_256_CCM_8
  - TLS_PSK_WITH_AES_128_GCM_SHA256
  - TLS_PSK_WITH_AES_256_GCM_SHA384
  - TLS_PSK_WITH_CHACHA20_POLY1305_SHA256
  - TLS_PSK_WITH_NULL_SHA256
  - TLS_PSK_WITH_NULL_SHA384
- Clés pré-partagées avec Diffie-Hellman :
  - TLS_DHE_PSK_WITH_AES_128_CBC_SHA
  - TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
  - TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- Fonctions de rappel :
  - pour externaliser les calculs PSK
  - pour externaliser les opérations RSA/ECDSA à clé privée

Protocoles pris en charge

- TLS 1.2
- DTLS 1.2

Extensions prises en charge

- Server Name Indication (SNI)

Plateformes prises en charge

- Toute plateforme fournissant un compilateur conforme à la norme ANSI-C - de 8 à 64 bits

Caractéristiques et avantages

- Intégration facile dans les produits existants
- Mis en œuvre pour répondre aux normes de qualité les plus élevées
- Faible encombrement
- Modularité
- Fonctionne sur toutes les plateformes
- Différents modèles de licence disponibles