wolfCrypt DO-178C DAL A認証キット

製品組み込み向けに最適化されたwolfCryptライブラリは、航空機搭載システム/機器のソフトウェア設計ガイドライン DO-178C DAL Aをサポートします。特に、セキュアブートおよび安全なファームウェア更新にフォーカスしています。

DO-178C認証

wolfSSL社のDO-178C認証製品およびサービスは、インターネット接続された民間航空機および軍用航空機に、軍事グレードの信頼できるセキュリティを提供します。これは、DO-178C認証に向け、安全な通信システム実現を目指すアビオニクス開発者にとって、柔軟、コンパクト、経済的かつ高性能な商用オフザシェルフ（commercial off-the-shelf、COTS）ソリューションです。

wolfCrypt DO-178C認証キット

DO-178C認証キットは民間航空機および軍用航空機に搭載される電子機器用に**セキュアブート**および安全な**ファームウェア更新**のための最適な暗号基盤を提供することにフォーカスしたRTCA DO-78CレベルA認証をサポートしています。

DO-178C認証キットは次の暗号アルゴリズムのトレース可能なアーティファクトを提供しています。

- メッセージダイジェスト用の SHA-256
- 暗号化と復号化のための AES
- メッセージ署名、検証用の RSA
- 認証された暗号/復号用の chacha20_poly1305

最適化サポート

航空機向けシステムの安全な再起動には、厳しい性能要件があります。暗号化パフォーマンスの最適化は、専門エンジニアによるコンサルティングサービスを用意しています。

FIPS認証

wolfCrypt暗号ライブラリは、NISTによる連邦政府、行政機関向けのセキュリティ機器の調達規格FIPS 認証の取得もサポートし、多数の取得実績があります。FIPS140認証が必要な場合は、検証済みのwolfCryptの暗号アルゴリズムをDO 178モードで使用し、FIPS認証の取得プロセスを加速させることができます。

サポートプラットフォーム

DO-178C認証キットはDeosをはじめ、多くの組み込み向けRTOS、あるいはベアメタル (非RTOS) での動作をサポートします。また、Intel x86、ARM をはじめとする多くのMCUアーキテクチャ上での動作をサポートします。

開発予定

DO-178C認証キットは、現在サポート範囲を広げるための開発を続けています。

wolfSSL社について

wolfSSL は2004年創立。米国ワシントン州に本社を置く製品組込み向けセキュリティの専門ベンダーです。TLS、DTLS、SSH他、インターネットの標準プロトコル、基盤となる暗号アルゴリズムなどのライブラリソフトウェア製品を提供しています。

ご質問、お問い合わせは info@wolfssl.jp までお気軽にご連絡ください。

wolfSSL Japan 合同会社 (ウルフエスエスエル)
〒108-6028 東京都港区港南 2-15-1 品川インターシティ A 棟 28 階
E メール: info@wolfssl.jp　ウェブサイト: wolfssl.jp