FIPS 認証の準備

wolfSSL Japan 合同会社

この資料では、wolfSSL の FIPS 認証取得サービスのためにお客様に準備いただく事項について説明します。

□ 概要

認証テストは弊社にてソースコードベースのテスト対象(wolfCrypt)をテストベクターとテストハーネスとともにコンパイル、リンクして御社プラットフォームにてテストすることになります。従って、認証テストのためには、認証対象の CPU ボードとともに御社でご使用のプログラミング環境一式を貸与いただくことになります。

認証取得のためのテスト範囲はすべて弊社の wolfCrypt(wolfSSL) に含まれています。御社側のアプリケーションなどは対象となりませんので、ご提供いただく必要はありません。

□ 準備いただく作業

お客様側では、認証テストまでに以下をご確認いただき必要な情報をお知らせください。

１）対象ボードへの wolfSSL のインストール確認
対象ボードと OS の上で wolfSSL 一式をインストールして、製品に含まれる一連のテストが動作することを確認してください。このインストール、テストは FIPS 認証テストではありませんので、プラットフォーム上で wolfCrypt が通常程度に安定して動作することをご確認ください。

wolfSSL ライブラリーは、共有ライブラリー、スタティックライブラリー、または、カーネル組み込みライブラリーとして使用することができます。認証はそれらの形態ご

とに異なる認証となりますので、あらかじめいずれかの形態を選択して動作確認してください。

２）CMVP 取得の場合は FIPS-Ready 版で確認

CMVP 取得の場合は、1)の確認の際、FIPS-Ready 版を使用して selftest の起動が正常に行われることを確認してください。詳細手順は FIPS-Ready ユーザマニュアルを参照ください。

３）上記、１)、２）の際にご使用のコンフィグレーションオプションと同じオプション設定にて弊社にてライブラリーのビルド、認証テストを行います。コンフィグレーションオプション情報一式を弊社にお知らせください。

４）C プログラムコンパイル環境

弊社側で、テストラボからのテストベクターと弊社のテストハーネスをコンパイル実行し、実行結果をテストラボにて検証します。その際、上記１)、２）で使用している御社と同じコンパイラーなどプログラミングツールを使用する必要があります (いわゆる Hello World のような) C 言語の簡単なプログラムがコンパイルできる環境一式が必要となります。

GCC などパブリックに入手できるものであれば、入手先、バージョン番号などの情報をお知らせください。

有償ライセンスなどでパブリックに入手できない場合は、お客様から貸与いただきます。必要時期までにご準備お願いします。

５）テスト結果の収集方法

弊社側で行う上記のテストでは、テスト結果をテスト対象のボードから USB, シリアルラインなどで接続されたコンソール出力を収集します。お客様のボード、プラットフォームの事情で特別なテスト結果の収集方法を必要とする場合は事前にご相談ください。

６）環境一式の受け入れ

認証テストに際しては、ボードとプログラミング環境一式の貸与をお願いします。ボードにはあらかじめ OS など弊社テストプログラムが動作するのに必要なプラットフォームのインストールをお願いします。

３）から５）の内容をお客様から受け取り、弊社にて Hello World プログラムのコンパイル、実行、メッセージの収集までができることを確認したのち、弊社側の FIPS 認証作業に入ります。

□ 認証済ライブラリの使用

FIPS 認証済バージョンも通常製品版と同じ形式(CMVP の場合は FIPS-Ready 版と同じ形式)でソースコードとしてご提供します。準備いただく作業：１） ２）で確認いただいた手順にてビルド、インストールして御社アプリケーションとともにご使用ください。

以上、