

FIPS 140-2 Compliance for Android Data Storage V1.0

(FCADS)

Overview

Version 1.0

6/4/2014

Prepared by  


[www.inforeliance.com](http://www.inforeliance.com)

Approval Page

Background

This document has been prepared for T2 – National Center for Telehealth and Technology

Point of Contact

The Point of Contact for questions about this document is:

Scott Coleman

InfoReliance Corporation

[Street address]

[City, State, zip]

Phone: ([xxx]) [xxx-xxxx]

Email: scott.coleman@tee2.org

Submitted By:

|  |  |
| --- | --- |
| This document is prepared by: | This document is endorsed by: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature Date | Signature Date |
|  | [name], [title] |

Approved By:

|  |
| --- |
| This document was approved by: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature Date |
| [customer\_name], [customer\_title] |

Document History

Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Action |
| 1.0 | 6/4/2014 | Scott Coleman | Created Document |
|  |  |  |  |

Table of Contents

[1.0 Introduction 1](#_Toc389803216)

[1.1 Purpose 1](#_Toc389803217)

[1.2 Definitions Nomenclature and Restrictions 1](#_Toc389803218)

[2.0 Components 1](#_Toc389803219)

[3.0 File Integrity Chain 3](#_Toc389803220)

[4.0 FIPS Capable OpenSSL Build Process 4](#_Toc389803221)

[4.1 FIPS Object Module Build 4](#_Toc389803222)

[4.2 OpenSSL Library Build 4](#_Toc389803223)

[5.0 SQLCipher build process 4](#_Toc389803224)

[6.0 Documentation and Record-keeping 5](#_Toc389803225)

[Appendix A: References 6](#_Toc389803226)

[Appendix B: Acronyms 7](#_Toc389803227)

[Appendix C: A note about the “Heartbleed” Vulnerability 8](#_Toc389803228)

Table of Figures

[Figure 1 Data Storage Components 2](#_Toc389803229)

List of Tables

[Table 1 T2 Process Sources 3](#_Toc389803230)

[Table 2 T2 Process Artifacts 3](#_Toc389803231)

[Table 3: References 6](#_Toc389803232)

[Table 4: T2 Supporting documents 6](#_Toc389803233)

[Table 5: Acronyms 7](#_Toc389803234)

# Introduction

## Purpose

The purpose of this document is to outline T2’s solution to FIPS 140-2 compliance for data storage on the Android platform. Procedures in this document are based on recommendations and requirements outlined in the “User Guide for the OpenSSL FIPS” (OpenSSL FIPS Users Guide), and “OpenSSL FIPS 140-2 Security Policy” (Security Policy) documents.

## Definitions Nomenclature and Restrictions

From the OpenSSL FIPS Users Guide:

* “OpenSSL itself is not validated,and never will be. Instead a carefully defined software component called the OpenSSL FIPS Object Module has been created. The Module was designed for compatibility with the OpenSSL library so products using the OpenSSL library and API can be converted to use FIPS 140-2 validated cryptography with minimal effort.”
* “A version of the OpenSSL product that is suitable for use with the FIPS Object Module is a FIPSCompatible OpenSSL.”
* “When the FIPS Object Module and a FIPS compatible OpenSSL are separately built and installed on a system, with the FIPS Object Module embedded within the OpenSSL library as part of theOpenSSL build process, the combination is referred to as a FIPS capable OpenSSL.”
* “The monolithic FIPS Object Module must be used in its entirely and cannot be edited to accommodate size constraints.”
* The FIPS 140-2 Approved Mode of Operation is the operation of the FIPS Object Module when all requirements of the Security Policy have been met and the software has successfully performed the power-up and self test operation (invocation of the FIPS\_mode\_set() function call). In this document this Approved Mode is referred to simply as FIPS mode.”

FIPS\_mode\_set() is a routine that performs power up and self test functions.

# Components

The main components of T2’s FIPS solution are all open source. A FIPS Object Module, and an FIPS compatible OpenSSL library are compiled per the “User Guide for the OpenSSL FIPS Object Module” to form a FIPS capable OpenSSL. The OpenSSL FIPS 140-2 Security Policy refers to the FIPS Object Module as the “validated module”.

The FIPS 140-2 Compliance for Android Data Storage solution uses this FIPS capable OpenSSL in addition to SQLCipher, another open source module which sits in-between the Android application and it’s SQLite database. SQLCipher uses the FIS capable OpenSSL to provide FIPS 140-2 validated encryption.



Figure Data Storage Components

# File Integrity Chain

The “Trusted Path” Requirement of the CMVP FIPS 140-2 process is satisfied by obtaining the sources for the FIPS Object Module, and the FIPS compatible OpenSSL library from physical media (CD) obtained directly from the OpenSSL foundation.

|  |  |  |
| --- | --- | --- |
| Component | File(s) | Source |
| FIPS Object Module | openssl-fips-ecp-2.0.tar.gz | OpenSSL Foundation Physical Media CD |
| FIPS compatible OpenSSL | openssl-1.0.1c.tar.gz | OpenSSL Foundation Physical Media CD |
| SqlCipher | Various Source files | GitHub |

Table T2 Process Sources

|  |  |
| --- | --- |
| Component | File(s) |
| FIPS Object Module | /usr/local/ssl/fips-2.0/bin/fips\_standalone\_sha1  /usr/local/ssl/fips-2.0/bin/fipsld  /usr/local/ssl/fips-2.0/include/openssl/\*.h  /usr/local/ssl/fips-2.0/lib/fips\_premain.c  /usr/local/ssl/fips-2.0/lib/fips\_premain.c.sha1  /usr/local/ssl/fips-2.0/lib/fipscanister.o  /usr/local/ssl/fips-2.0/lib/fipscanister.o.sha1 |
| OpenSSL Cryptographic Routines | openssl-1.0.1f/libcrypto.a |
| SQLCipher | armeabi/libdatabase\_sqlcipher.so  armeabi/libsqlcipher\_android.so  armeabi/libstlport.so  commons-codec.jar  guava-r09.jar  sqlcipher.jar |

Table T2 Process Artifacts

The CMVP validates source code, and not binaries. So to ensure compliance, "A chain of

checks beginning with the source code and extending through each step in the transformation of the

source code into a running process was established to provide a check equivalent to that used by

more traditional object based validations."

T2’s solution to FIPS 140-2 compliance for the Android platform asserts this compliance by strictly adhering to the process outlined by the CMVP and the Security Policy.

# FIPS Capable OpenSSL Build Process

By strictly following the procedures outlines in the User Guide for the OpenSSL FIPS Object Module, and the Security Policy we ensure our end product is based on FIPS Validated sources.

## FIPS Object Module Build

From the User Guide for the OpenSSL FIPS Object Module:

“The build process described in the Security Policy results in the creation of an object module,

fipscanister.o, and a matching digest file, fipscanister.o.sha1. This FIPS Object

Module contains the object code corresponding to the sequestered source files (object code for

FIPS specific functions such as FIPS\_mode\_set() and for the algorithm implementations).”

The source code used to generate the FIPS object module is referred to as “sequestered source code” , meaning is cannot be modified (nor can the process of building it). – “If the original distribution is modified, or if anything other than those three specified commands are used, or if any intermediate files are modified, the result is not FIPS validated.”

Those three commands are :

./config

make

make install

These are the commands that the T2 process uses. See Table 2 T2 Process Artifacts, for a specific lists of artifacts produced at this stage.

## OpenSSL Library Build

The OpenSSL distribution is built in accordance with the User Guide for the OpenSSL FIPS Object Module v2.0 using the following commands:

./config fips no-ec2m --with-fipslibdir=/usr/local/ssl/fips-2.0/lib/

make depend

make

See Table 2 T2 Process Artifacts, for a specific lists of artifacts produced at this stage.

# SQLCipher build process

The T2 FIPS 140-2 Compliance for Android Data Storage process links the components built in the previous steps with the SQLCipher open source code to produce its final solution. First, SQLCipher is built according to its original specifications. Then to ensure FIPS 140-2 compliance additional compilation/link steps are performed to link in the validated OpenSSL/FIPS Module code. Note that the utility ***FIPSLD*** is used as described in the User Guide for the OpenSSL FIPS Object Module is used in compilation/links steps to preserve the validation integrity.

See , for a specific lists of artifacts produced at this stage. These artifacts are directly used by an Android project. The initialization of the application MUST call FIPS\_mode\_set() and confirm and a success was returned. Once this happens the application can claim the following (According to CMVP)

***Product XXXX uses an embedded FIPS 140-2-validated cryptographic module (Certificate#1747) running on a Android 4.0 platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.***

Where XXXX is the product name.

**See template document: FIPS140-2ApplicationComplianceStatement.txt**

“This statement asserts "user affirmation" of the validation per Section G.5 of the *Implementation Guidance* document”

# Documentation and Record-keeping

In accordance with section 5 of User Guide for the OpenSSL FIPS Object Module, the following is documentation compliance with the Security Policy:

For the FIPS object module generation:

1. The openssl-fips-ecp-2.02.tar.gz file distribution file which was used as the basis for the production of the FIPS object module was obtained from the FIPS compatible OpenSSL library from physical media (CD) obtained directly from the OpenSSL foundation.
2. The host platform on which the fipscanister.o, fipscanister.o.sha1,fips\_premain.c, and fips\_premain.c.sha1 files were generated is OS-X. The compiler used was gcc version 4.6.
3. The fipscanister.o module was generated with exactly the three commands:

./config

make

make install

No other build-time options were specified.

1. The HMAC SHA-1 digest of the produced fipscanister.o is: HMAC-SHA1(fipscanister.o)= f129aeb6f91736bde36e8b0d4c11a15bd454d2d1
2. The contents of the distribution file used to create fipscanister.o was not manually modified in any way at any time during the build process.

**See document: FIPS140-2ObjectModuleRecordV1.0.txt**

For the application in which the FIPS Object Module is embedded, a document with the following information should be updated and attached:

1. A record of the HMAC SHA-1 digest of the fipscanister.o that was embedded in the application.
2. An assertion that the application does not utilize any cryptographic implementations other that those provided by the FIPS Object Module or contained in the FIPS capable OpenSSL 1.0.1 libraries (where non-FIPS algorithms are disabled in FIPS mode).
3. A description of how the application clearly indicates when FIPS mode is enabled

(assuming that FIPS mode is a runtime selectable option). Note that the application must call FIPS\_mode\_set(), whether that call is triggered by runtime options or not.

**See template document: FIPS140-2ApplicationComplianceRecord.txt**

# Appendix A: References

|  |
| --- |
|  |
| OpenSSL FIPS 140-2 Security Policy Version 2.0.4 |
| User Guide for the OpenSSL FIPS Object Module v2.0 |

Table : References

|  |  |
| --- | --- |
|  |  |
| FIPS140-2ApplicationComplianceStatement.txt | Application compliance statement to be completed by developer after integrating FCADS into application.  (template) |
| FIPS140-2ApplicationComplianceRecord.txt | Application record keeping statement to be completed by developer after integrating FCADS into application.  (template) |
| FIPS140-2ObjectModuleRecordVx.y.txt | FIPS object model record keeping statement to be completed by developer after building the The FIPS 140-2 Compliance for Android Data Storage solution. |
| BuildInstructionsV1.0.txt | Specific instructions used to build the The FIPS 140-2 Compliance for Android Data Storage solution. |

Table : T2 Supporting documents

# Appendix B: Acronyms

All of the acronyms used in this document appear in Table 5: Acronyms. All acronyms are also fully defined the first time they appear in the document.

|  |  |
| --- | --- |
| Acronym | Definition |
| API | Application Programming Interface |
| CMVP | Cryptographic Module Validation Program |
| FIPS | Federal Information Processing Standards, see  <http://www.itl.nist.gov/fipspubs/> |
| FIPS 140-2 | See <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf> |

Table : Acronyms

# Appendix C: A note about the “Heartbleed” Vulnerability

The “Heartbleed” vulnerability does not affect T2’s solution to FIPS 140-2 compliance for the Android platform since SQLCipher does only uses the Cryptographic routines of OpenSSL and not it’s SSL implementation where the vulnerability exists.