Addressing the Encryption Requirements of the Common Criteria Protection Profiles for Mobility

---

A White Paper from SafeLogic

SafeLogic Inc.

530 Lytton Ave, Suite 200

Palo Alto, CA 94301

www.SafeLogic.com

Executive Summary

In October 2013, the US Government's Common Criteria Evaluation and Validation Scheme (CCEVS) announced Protection Profiles for Mobile Devices (MD) and Mobile Device Management (MDM) systems. The Common Criteria is an international standard for the evaluation of security features within IT products. It is also widely recognized as a crucial certification needed for products seeking addition to the Unified Capabilities Approved Products List (UC APL), administered by the U.S. Defense Information Systems Agency (DISA). Products that successfully earn addition to the UC APL become eligible for procurement and deployment by the various agencies of the United States Department of Defense.

These new Protection Profiles embody the requirements that are to be met by a specific technology type in Common Criteria evaluations. The Mobile Device Protection Profile (MDPP) contains the security functional requirements for mobile devices such as smart phones and tablets. The Mobile Device Management Protection Profile (MDMPP) includes the security functions to be evaluated including key protection, protected communications, mobile device configuration, and administration.

Cryptographic support functions are critical requirements in these new Protection Profiles, as anticipated. It is important to note that while many vendors pursue both Common Criteria certification and FIPS 140-2 validation, the latter does not automatically satisfy the former. The encryption requirements in these new Protection Profiles reflect certain standards imposed by NIST for FIPS 140-2, but they are not interchangeable.

SafeLogic has addressed the necessary cryptographic support functions required by the MDPP and MDMPP and streamlined implementation with the CryptoComply drop-in module. Integrating CryptoComply eliminates the several engineer-years it would take to design and implement these functions. This white paper presents information on how CryptoComply meets the encryption requirements in each of the new Protection Profiles for Common Criteria and discusses the benefits of integrating the drop-in module.

Table of Contents

1 Introduction

The Common Criteria is an international standard for the evaluation of security features within IT products (see www.commoncriteriaportal.org and www.niap-ccevs.org for more information). Certifications using this methodology are recognized by 27 nations around the globe. Protection Profiles define the security requirements for a specific technology type in Common Criteria evaluations.

In the United States, the Common Criteria Evaluation and Validation Service (CCEVS) ensures that protection profiles align with corresponding National Security Systems guidance documents, including Security Requirements Guides/Security Technical Implementation Guides (SRGs/STIGs). Enforcing the use of Common Criteria for security evaluations comes from the following policies:

- National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems"
- CNSS Policy (CNSSP) 11 "National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products"
- CNSS Directive (CNSSD) 502, "National Directive on Security of National Security Systems"
- Department of Defense Directive DoDD 5100.2, "National Security Agency/ Central Security Service"
- Department of Defense Directive DoDD 8500.01E, "Information Assurance"
- Department of Defense Directive DoDI 8500.02, "Information Assurance Implementation"

Moreover, the U.S. Defense Information Systems Agency (DISA) hosts the Department of Defense Unified Capabilities Approved Products List, typically called the DoD UC APL. It was established by the UC Requirements (UCR 2013) document to maintain a single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) certification. By limiting their usage to products on the UC APL, agencies may purchase and operate UC systems over all DoD network infrastructures without requiring further testing or certification. In addition, DoD components are required to fulfill their system needs by only purchasing products listed on the APL, provided one of the listed products meets their needs. This means the APL must be consulted prior to purchasing a system or product, and competitive products are routinely removed from consideration because they have not yet been added to the UC APL. A Common Criteria evaluation and FIPS 140-2 validation certificates are required to submit products for consideration for the APL, with few exceptions.

On October 23, 2013, the Common Criteria Evaluation and Validation Service (CCEVS) announced the publication of Protection Profiles for Mobile Devices (MD) and Mobile Device Management (MDM) systems. By doing so, the CCEVS acknowledged the growing need for specific attention to these technology types. In the past, as no protection profile was available for these technologies, vendors and

evaluators were forced to a build certification cases around generalized security standards. Now, the establishment of the protection profiles clarified the exact requirements for certification. The Mobile Device Protection Profile (MDPP) contains the security feature requirements for mobile devices such as smart phones and tablets, while the Mobile Device Management Protection Profile (MDMPP) includes key protection, protected communications, mobile device configuration, and administration.

Cryptographic support functions are critical requirements in these new protection profiles, as anticipated. It is important to note that while many vendors pursue both Common Criteria certification and FIPS 140-2 validation, the latter does not automatically satisfy the former. The encryption requirements in these new Protection Profiles reflect certain standards imposed by NIST for FIPS 140-2, but they are not interchangeable.

SafeLogic has addressed the necessary cryptographic support functions required by the MDPP and MDMPP and streamlined implementation with the CryptoComply drop-in module. Integrating CryptoComply eliminates the engineer-years it would take to design and implement these functions. Instead, refer to the tables below for more information on how CryptoComply meets the encryption requirements in each of the new protection profiles for Common Criteria.

2 Mobile Device Protection Profile – Protected Communications and Storage

The Mobile Device Protection Profile cryptographic support functions are focused around securing communications to and from the mobile device as well as providing secure data storage. These requirements are described in Common Criteria language and notation in the MDPP. The cryptographic requirements are represented by the FCS_XXX.N notation. This shorthand is merely the designation used to classify the requirements. Functional class Cryptographic Support is shortened to FCS while XXX are placeholders for the type of cryptographic functions and N denotes the sub-functions.

The table below shows how CryptoComply directly meets the Security Functional Requirements (SFR) in the Mobile Device Protection Profile (MDPP).

SECURITY FUNCTIONAL REQUIREMENT	HOW CRYPTOCOMPLY MEETS THE REQUIREMENT
FCS_CKM.1	• Generates asymmetric cryptographic keys used for key establishment in accordance with NIST Special Publication 800-56A or 56B for Key Establishment. • Generates asymmetric cryptographic keys used for authentication in accordance with NIST FIPS PUB 186-4 or ANSI X9.31-1998. • Generates symmetric cryptographic using PRF-384 to support IEEE 802.11-2012.
FCS_COP.1	• Performs encryption and decryption in accordance with AES GCM, CCM, XTS, or CBC mode. • Performs cryptographic hashing in accordance with SHA. • Performs cryptographic signature services in accordance with RSA or DSA. • Performs Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC SHA.
FCS_RBG_EXT.1	• Performs all deterministic random bit generation services and entropy justifications in accordance with NIST Special Publication 800-90A.

Table 2-1 - Cryptographic Requirements in the MDPP

CryptoComply's cryptographic functions also provide underlying data protection support for Security Functional Requirements (SFR) in the Mobile Device Protection Profile (MDPP). Some of the supported security functions come from functional classes outside of the cryptographic support functional class and thus have different class designations as shown in the following table.

SECURITY FUNCTIONAL REQUIREMENT	HOW CRYPTOCOMPLY SUPPORTS THE REQUIREMENT
FCS_CKM.2	• Decrypts Group Temporal Key (GTK) in accordance with AES Key Wrap in an EAPOL-Key frame that meets NIST SP 800-38F and IEEE 802.11-2012 for the packet format and timing considerations.
FCS_CKM_EXT.1	• Supports a hardware-protected REK with an AES key.
FCS_CKM_EXT.2	• Generates random DEKs with entropy corresponding to the security strength of AES key sizes.
FCS_CKM_EXT.3	• Generates all KEKs with 128-bit or 256-bit keys corresponding to at least the security strength of the keys encrypted by the KEK.
FCS_CKM_EXT.6	• Generates all salts using a RBG.
FCS_DTLS_EXT.1	• Implements the DTLS protocol in accordance with either DTLS 1.0 (RFC 4347), or DTLS 1.2 (RFC 6347).
FCS_HTTPS_EXT.1	• Implements HTTPS using TLS.
FCS_IV_EXT.1	• Generates initialization vectors for each AES mode.
FCS_SRV_EXT.1	• Provides cryptographic services to applications.
FCS_STG_EXT.1	• Provides secure key storage and management.
FCS_STG_EXT.2	• Encrypts all DEKs and KEKs using KEKs using AES in either Key Wrap (KW) mode, Key Wrap with Padding (KWP) mode, GCM, CCM, or CBC mode.
FCS_STG_EXT.3	• Protects the integrity of any encrypted KEK.
FCS_TLS_EXT.1	• Implements EAP TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), and/or TLS 1.2 (RFC 5246).
FDP_DAR_EXT.1	• Protects all data using DEKs with AES in the XTS, CBC, or GCM mode.

FIA_X509_EXT.1	• Validates certificates in accordance with RFC 5280 certificate validation.
FIA_X509_EXT.2	• Uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, TLS, HTTPS, and/or DTLS.
FIA_X509_EXT.3	• Provides a certificate validation service to applications.
FPT_KST_EXT.1	• Does not store any plaintext key material in readable non-volatile memory.
FPT_KST_EXT.2	• Does not transmit any plaintext key material from the cryptographic module.
FPT_KST_EXT.3	• Ensures that it is not possible for the TOE user(s) to export plaintext keys.
FPT_TST_EXT.1	• Runs a suite of self-tests [during initial start-up (on power on)] to demonstrate the correct operation of [all cryptographic functionality].
FTP_ITC_EXT.1	• Uses 802.11-2012, 802.1X, and EAP-TLS and at least one of: IPsec, TLS, DTLS, HTTPS protocol to provide a communication channel between itself and another trusted IT product.

Table 2-2 - Data Protection Requirements in the MDPP

3 Mobile Device Management Protection Profile – Protected Communications

The Mobile Device Management Protection Profile defines security requirements for managing mobile devices and reflects the requirements for capabilities that run on both the mobile device as well as management servers. CryptoComply is available for server platforms as well as mobile, and is able to meet requirements for both. The focus of cryptographic support functions in the MDMPP is on protected communications.

The table below shows how CryptoComply directly meets the cryptographic requirements in the Mobile Device Management Protection Profile (MDMPP).

SECURITY FUNCTIONAL REQUIREMENT	HOW CRYPTOCOMPLY MEETS THE REQUIREMENT
FCS_CKM.1	• Generates asymmetric cryptographic keys used for key establishment in accordance with NIST Special Publication 800-56A or 56B for Key Establishment. • Generates asymmetric cryptographic keys used for authentication in accordance with NIST FIPS PUB 186-4 or ANSI X9.31-1998.
FCS_COP.1	• Performs cryptographic signature services in accordance with RSA or DSA. • Performs keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC SHA. • Performs encryption and decryption in accordance with AES with GCM, CCM, or CBC mode. • Performs cryptographic hashing in accordance with SHA.
FCS_RBG_EXT.1	• Performs all deterministic random bit generation services and entropy justifications in accordance with NIST Special Publication 800-90A.

Table 3-1 - Cryptographic Requirements in the MDMPP

CryptoComply also provides the underlying cryptographic functions to support protected communications Security Functional Requirements (SFR) in the MDMPP.

SECURITY FUNCTIONAL REQUIREMENT	HOW CRYPTOCOMPLY SUPPORTS THE REQUIREMENT
FCS_DTLS_EXT.1	• Implements the DTLS protocol in accordance with either DTLS 1.0 (RFC 4347), or DTLS 1.2 (RFC 6347).
FCS_HTTPS_EXT.1	• Implements HTTPS using TLS.

FCS_IPSEC_EXT.1	• Implements the IPsec architecture.
FCS_IV_EXT.1	• Provides Initialization vectors for each AES mode.
FCS_SSH_EXT.1	• Implements the SSH protocol.
FCS_STG_EXT.1	• Encrypts all keys using AES in either Key Wrap (KW) mode, Key Wrap with Padding (KWP) mode, GCM, CCM, or CBC mode.
FCS_TLS_EXT.1	• Implements TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), and/or TLS 1.2 (RFC 5246).
FIA_X509_EXT.1	• Validates certificates in accordance with RFC 5280 certificate validation.
FIA_X509_EXT.2	• Uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, TLS, HTTPS, and/or DTLS.
FPT_ITT.1	• Protects all data from disclosure and modification through use of IPsec, TLS, or DTLS when it is transferred between the MDM Agent and MDM Server.
FPT_TST_EXT.1	• Provides the capability to verify the integrity of stored MDM Server executable code when it is loaded for execution through the use of cryptographic services.
FTP_TRP.1	• Uses IPsec, TLS, or TLS/HTTPS to provide a trusted communication path between itself and remote administrators.
FTP_TRP.2	• Uses TLS or TLS/HTTPS] to provide a trusted communication path between itself and MD users.

Table 3-2 - Protected Communications Requirements in the MDMPP

4 Conclusion

CryptoComply by SafeLogic can minimize the engineering teams' burden in meeting Common Criteria encryption requirements, and specifically the new Mobile Device and Mobile Device Management Protection Profiles. The establishment of the new Protection Profiles has clarified exactly what will be required of these technology types, and the stakes are extremely high.

SafeLogic's CryptoComply meets the encryption requirements set forth by the Common Criteria Evaluation and Validation Scheme (CCEVS). By leveraging a 'Drop-In Compliance' approach, SafeLogic accelerates the timeline for integration, reduces the overall development time and eliminates compliance risks. Common Criteria is a challenging and time-consuming process and can be a major distraction to engineering teams. While traditional methods require significant commitment of time and resources, developers can integrate CryptoComply quickly and return to their core tasks. The net result is that developers are able to maintain focus on the product while compliance is achieved immediately.

The barrier to entry for the UC APL is high for good reason. Common Criteria, along with FIPS 140-2, has traditionally posed significant roadblocks but now offers an opportunity for competitive advantage. The solutions that integrate CryptoComply will enjoy instant compliance, faster release cycles, and the ability to sell the current product as FIPS 140-2 compliant. Waiting 12 months or longer to be added to the UC APL will quite simply render a product irrelevant, no matter the quality of engineering. The Department of Defense needs solutions that are compliant *now*.

For a real life scenario, please refer to SafeLogic's Case Study with API Technologies, available in the Exclusive Content area of the SafeLogic website. API Technologies was seeking an updated listing on the UC APL, and they were able to accelerate the process by integrating CryptoComply. In tandem with SafeLogic's RapidCert, API Technologies satisfied all requirements and proceeded directly to the JITC testing phase.

In conclusion, be aware of the demanding processes of UC APL, Common Criteria, and FIPS 140-2, but don't forget the rewards that are waiting. Begin planning a strategy as soon as possible, and please reach out with any questions regarding CryptoComply, CryptoComply Professional Services for more extensive needs, or these encryption requirements.

© SafeLogic

4.1 About SafeLogic

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in Cloud, mobile, wearable, IoT, server, workstation, and appliance environments. These modules have been fully validated to FIPS 140-2 standards and offer drop-in OpenSSL and Bouncy Castle compatibility, a variety of connectors to accommodate unique product architecture, and instant compliance for federal deployments to SafeLogic customers.

Even better, SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost.

SafeLogic's customers are among the most influential and innovative companies in technology today, from startups to the Fortune 100.

SafeLogic was established in 2012, is privately held and is headquartered in Palo Alto, California.

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301

(844) 4-ENCRYPTION

www.SafeLogic.com

www.Twitter.com/SafeLogic