IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 December 2022, accepted 18 January 2023, date of publication 23 January 2023, date of current version 31 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3239043

PERSPECTIVE

On the Development of a Protection Profile Module for Encryption Key Management Components

NAN SUN[1,2], CHANG-TSUN LI[3], (Senior Member, IEEE), HIN CHAN[4], MD ZAHIDUL ISLAM[5], MD RAFIQUL ISLAM[6], (Senior Member, IEEE), AND WARREN ARMSTRONG[7]

[1]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2612, Australia
[2]Cyber Security Cooperative Research Centre, Joondalup, WA 6027, Australia
[3]School of Information Technology, Deakin University, Waurn Ponds, VIC 3216, Australia
[4]Australian Cyber Security Centre, Kingston, ACT 2604, Australia
[5]School of Computing, Mathematics and Engineering, Charles Sturt University, Bathurst, NSW 2795, Australia
[6]School of Computing, Mathematics and Engineering, Charles Sturt University, Albury, NSW 2640, Australia
[7]QuintessenceLabs Pty Ltd., Canberra, ACT 2609, Australia

Corresponding author: Nan Sun (nan.sun@adfa.edu.au)

This work was supported in part by the Cyber Security Research Centre Ltd., and in part by the Australian Government's Cooperative Research Centres Programme.

ABSTRACT The ability of a cryptographic system to protect information from attacks depends on many factors, including the secrecy of the encryption key. A crucial aspect of any cryptosystem is how it manages the encryption keys. Encryption Key Management (EKM) spans the entire life cycle of the key, including the key's generation, usage, distribution, renewal, and destruction. Given the security sensitivity, it is desirable to adopt a widely accepted standard when developing an encryption key management system. Through rigorous development of security requirements and following standardized validation, evaluation, and certification, the consumers' confidence in the security of the EKM system will be enhanced. The Protection Profile (PP), defined in the Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC), specifies the security functional and assurance requirements for a specific technology. In this work, we propose a PP Module that is the new evolution of the PP covering trusted security features for EKM, which is based on its compliance with the Network Device collaborative Protection Profile (NDcPP). In particular, by analyzing threats and vulnerabilities of EKM systems, corresponding security objectives and requirements are proposed in the PP, along with the specification of evaluation activities. The quantum-safe aspect of key distribution protocols is further investigated to support EKM products with quantum-resistant algorithms and quantum key distribution features. In addition to presenting the development methodology and implementation process for the PP Module of EKM, we distill lessons learned from developing and validating the PP Module to inspire future research efforts on defining security requirements with the CC.

INDEX TERMS Cyber security, common criteria, protection profile, encryption key management, quantum safe.

I. INTRODUCTION

The consideration of dependable and secure computing brings about constant concerns for confidentiality, integrity, and availability of information security systems [1]. Trust is the crucial factor for the successful introduction of new products, including Information and Communications Technology (ICT) [2]. With a trusted and secure computing environment, ICT systems and products will consistently behave in expected ways and protect the users against

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

different security threats [3]. Those behaviors are usually enforced by hardware, software, and the security function of the products.

Confidence and trust from consumers and markets of a product can be established with the certified outcomes of independent evaluations on ICT products' conformance to a common set of security functional and assurance requirements under a specific security standard [4]. The Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for specifying security requirements and evaluation criteria [5]. In particular, a Protection Profile (PP) is a document used as part of the certification process according to the CC [6]. A PP, which is intended to be reusable, defines the security requirements and objectives for a category of ICT security products, supports the definition of functional standards, and guides product development or procurement specifications [4].

Encryption keys undoubtedly play an essential role in the context of cryptography technology and broader cyber security [7]. If eavesdroppers can obtain the key used for decryption, the confidentiality of users' data cannot be guaranteed. If attackers get hold of the private key used for digital signatures, they can launch impersonation attacks. Hence, effective management of the keys is of paramount importance in ensuring security. Security requirements for cryptographic modules (e.g., NIST Special Publication 800-57 part 1 [8] and FIPS 140-3 [9]) include a set of standards published by the US government to provide guidelines for vendors to design, develop, evaluate, and certify cryptographic modules used in ICT products or systems [10]. For example, FIPS 140-3 provides four increasing qualitative levels of security to cover areas of cryptographic module specification, cryptographic module ports and interfaces, roles, services, authentication, finite state model, physical security, operational environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility, self-tests, design assurance, and mitigation of other attacks. It is followed mostly by the US and Canadian vendors [11]. Compared with security requirements for cryptographic modules, the CC covers all ICT security related technologies and a more comprehensive range of evaluation aspects in terms of security functionalities (e.g., auditing, cryptographic support, communication, user data protection, identification and authentication, privacy, resource utilization, trusted path/channels etc.), and security assurance (e.g., configuration management, guidance document, vulnerability assessment, tests, etc.) [5]. As of 31st August 2021, there are 31 signatory countries to the Common Criteria Recognition Arrangement (CCRA) [12].

In this paper, we formulate and justify the product-specific security and implementation-independent requirements based on the analysis of the vulnerabilities and threats of Encryption Key Management and its operational environments. A PP is developed for Encryption Key Management components in collaboration with the Australian Certification Authority of the Australian Cyber Security Centre, QuintessenceLabs and cyber security researchers in academia through the recent *Development of Australian Cyber Criteria Assessment (DACCA)* project.[1] The developed PP contributes to increasing the consumers' trust on the reliability and the security of the ICT products that require Encryption Key Management components. In addition, we share the methodology and lessons learned from the PP development and validation, which can serve as a useful reference and valuable guidance for further PP development and research.

The rest of the paper is organized as follows. Section 2 briefly describes the PP according to the CC, the Encryption Key Management as the Target of Evaluation (TOE), and the essential security requirements for Encryption Key Management. In Section 3, we propose a Protection Profile Module (PP Module) and the corresponding Supporting Document (SD) for the TOE. The methodology adopted in our PP Module development is also summarized. In Section 4, we further investigate the quantum-safe aspect and include a set of optional Security Requirements in the developed PP Module to make it future-proof. Future research directions are also discussed. Finally, we conclude this work in Section 5.

II. PRELIMINARY

A. COMMON CRITERIA AND PROTECTION PROFILE

In this subsection, we discussed the Common Criteria and explained how the Protection Profile evolved with the development of Common Criteria. The Common Criteria (CC) is an international standard (ISO/IEC 15408) for cyber security certification. ICT security assurance is derived through a rigorous verification process, conducted on a case-by-case basis [5]. With a strict, standardized and repeatable methodology, the CC assures implementing, evaluating and operating a security product suitable to resist the threats in the operational environments. After an ICT security product is successfully evaluated by an independent laboratory (e.g., an Australian Information Security Evaluation Facility) licensed by a certification authority of a CCRA signatory country, the product can be certified by the certification authority and listed on the Certified Products List at the Common Criteria Portal [13]. The certified results may help consumers decide whether the products fit their security requirements, which also boosts the competitiveness of the certified products when compared against similar products in the market.

Under the CC, a traditional PP is a document, usually developed by a user or user group, which defines an implementation-independent set of security requirements for a category of ICT products, systems or technology that fulfils the consumers' particular need and serves as a guide for formulating product development [14]. The PP document stipulates the security functionalities that must be included in the CC evaluation in order to address a range of defined security problems. PPs are particularly helpful for comparing different IT products since they specify a minimum set of security requirements that must be satisfied [15]. If an ICT product is intended to be evaluated and certified under the CC standards, the vendor must complete a Security Target

[1] https://cybersecuritycrc.org.au/development-australian-cyber-criteria-assessment

(ST) description. The ST is the document that may comply with one or more PPs to implement the security features of the TOE [5]. In addition, the ST provided by the vendor should include the evaluation of any potential security risks by defining the security functional and assurance measures that the TOE should offer to meet CC requirements [4].

The new evolution of the CC supports the comparability among the results of independent cyber security evaluations through collaborative Protection Profile (cPP) [16]. Compared with the traditional standalone PP, a PP Module builds on a cPP, and the conforming TOEs are obligated to implement the functionalities specified in the cPP along with the additional functionalities defined in the PP Module. Building a PP Module upon a cPP rather than developing a traditional PP prevents redeveloping certain functionalities and ensure the additional functionalities specified in the PP Module are sufficient to enhance cyber security for the TOE. Hence, for our TOE - Encryption Key Management, we utilize the collaborative Protection Profile for Network Devices (NDcPP) [17] as the Base PP and develop a PP Module to be used in conjunction with the NDcPP. According to the NDcPP [17], a network device consists of any device that connects to a network and serves as infrastructure for that network [17]. The reason for choosing the NDcPP as the Base PP of our PP Module is because a device that requires centralized enterprise Encryption Key Management is a specific type of network device. There is nothing about implementing Encryption Key Management that would prevent any of the security capabilities defined by the Base PP from being satisfied. In our PP Module, only the security functionalities and assurance requirements specific to Encryption Key Management components that are not included in the NDcPP need to be added. Such an approach avoids repetitive efforts and redundant information, and increases the efficiency of the development process.

The Supporting Document (SD) for the PP Module describes the activities to be taken to assess the security functions of a product (i.e., TOE). As a supplementary document to the PP Module, the SD specifies the evaluation activities, including review of the TOE Summary Specification (TSS) and Operational Guidance (OG). The SD also specifies tests to be performed during the evaluation. The TSS describes the security functions required of the TOE to ensure that the TOE meets the IT Security Functional Requirements (SFRs). The OG sets standards for operating procedures to achieve the SFRs. The tests dictate what the evaluators should perform during their assessments. Given the above consideration, for the targeted Encryption Key Management technologies, we aim to develop a PP Module and the associated SD as a package based on the NDcPP.

B. OVERVIEW OF ENCRYPTION KEY MANAGEMENT

Using a centralized key management system allows a consolidated view of an organization's encryption keys and allows management of policies (e.g., access control, length and algorithm restrictions, entropy source selection) via one central interface. It also reduces the specialist knowledge required of other application developers compared to the alternative where applications manage their own keys. However, in a corporate context, collecting an organization's cryptographic keys in one place makes that place attractive to hostile actors. As listed below, it is imperative that an EKM system is designed and implemented in such a way as to resist such threats.

- **High-quality encryption keys generation:** An EKM must generate high-quality encryption keys [18], [19]. A high-quality key is one that is unpredictable and contains no structural weaknesses. The key can be generated via algorithmic means (i.e., using a pseudo-random number generator) or via measurements of a physical system (i.e., a true random number generator).
- **Unauthorized disclosure prevention:** An EKM must prevent unauthorized disclosure of key material or metadata [20], [21], [22]. It must implement authentication and authorization mechanisms to control access to key material. It must employ robust software development practices and use tooling to guard against data leaks from programming errors, including when under attack (e.g., as occurred in the well-known SSL Heartbleed vulnerability). The cryptographic implementations must be robust against side-channel attacks such as timing attacks.
- **Authorized use of key material:** An EKM must facilitate the authorized use of key material [23]. This could be done by revealing key material to authorized parties (although should key material leave the purview of the EKM, the EKM can make no guarantees about its continued secrecy) or by performing operations using the key material on behalf of the end-user without revealing the key itself.
- **Secure destruction of key material:** An EKM must facilitate secure destruction of key material when a key is no longer required [20]. This can arise in various circumstances: a key can be rotated (based on a time-based or usage-based trigger) as part of normal operations, a key can be discovered to be compromised and rotated out, or the cryptosystem as a whole could require zeroization (e.g., if it is about to fall into unfriendly hands). Note that in some use cases, destruction of key material need not require the destruction of the associated metadata.
- **Audit records maintenance:** An EKM must maintain audit records to facilitate compliance and incident response activities [24].
- **Resilience to failures:** An EKM must be resilient to failures of hardware or infrastructure [25]. As the central repository of all cryptographic keys, the data loss in an EKM is likely catastrophic. The EKM must provide mechanisms (e.g., backups, replicated geographically-dispersed deployment, and the like) to reduce the likelihood of data loss to an acceptably low level.
- **Validated software updates:** An EKM must allow for validated software updates [26]. It is an unfortunate fact of life that software vulnerabilities exist. For a large, complex system, these vulnerabilities can arise from many points: the software itself, the underlying

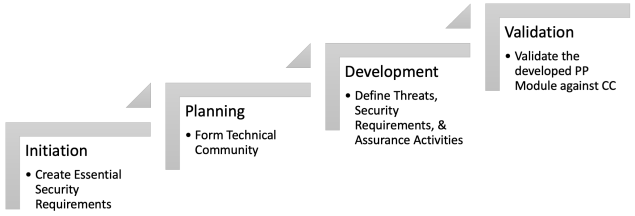


FIGURE 1. Protection profile development methodology.

libraries, the operating system, or in the host hardware itself. To keep the security of an EKM system at the cutting edge, it is important that a mechanism exists to allow it to be updated, and that this mechanism allows for validation that the updates have been issued by the vendor and have not been tampered with enroute.

III. PROTECTION PROFILE MODULE DEVELOPMENT

A. METHODOLOGY

A PP Module includes an independent set of security objectives and requirements for a specific category of products, systems, or technology, typically written by the user community, developers of the TOE, vendors, or a combination of the above. Inspired by the proposed PP development process published by National Information Assurance Partnership (NIAP) [27], we adopt four phases when we develop PP Module for the target TOE, respectively *initiation*, *planning*, *development* and *validation*, as shown in Figure 1.

In the first phase *initiation*, we create the Essential Security Requirements (ESRs) for the target TOE based on the understanding of the security features of the Encryption Key Management Components. The intent is that the ESR will allow Security Functional Requirements (SFRs) to be crafted in a manner that makes sense to the Technical Community (TC) (e.g., vendors, researchers, and policymakers).

During the *planning* stage, the members of the TC, including at least developers, government experts, and evaluators, bring together skills and backgrounds needed for developing the PP Module and the corresponding SD [28]. The TC seeks to come to a consensus on the requirements for the given TOE type. The developers of a TOE, or a group of developers of similar TOEs as the technical representatives, wish to establish a minimum baseline for the kind of TOE. In addition, the government or large corporation specifies its requirements as part of the acquisition process. The government experts primarily refer to those versed in the threats associated with the technology and governmental use cases. The evaluators are expected to contribute to the requirements and assurance activities and comment on the proposed assurance activities concerning technical feasibility as well as cost-effectiveness.

In the third phase *development*, the security problems, security objectives, security requirements, and assurance activities are defined in the PP. The definition of security problem shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two [5]. The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition [29]. Security requirements are a translation of the security objectives for the TOE [5]. Security requirements that address the security objectives are typically at a more detailed abstraction level and independent of specific technical implementation. Furthermore, security assurance components define how assurance is to be gained that the TOE meets the security requirements [13].

Once the developed PP is evaluated to obtain approval for public release, it will be posted on CC Portal [30]. In the last phase *validation* of PP, it is demonstrated that the PP is technically sound and internally consistent. If the developed PP module is based on one or more other PPs, the developed PP should be a correct instantiation of the base PP.

B. IMPLEMENTATION

1) INITIATION: ESSENTIAL SECURITY REQUIREMENTS

Encryption Key Management is a comprehensive technology [31]. It involves not only technicalities but also management factors, such as administrative management level [32]. The weakest part of the system determines the security level of the encryption system. A sound key management system aims to be immaterial to human factors.

One of the first steps prior to developing a PP is to develop and agree on an Essential Security Requirement (ESR). The ESR's purpose is to capture the high-level fundamental security requirements expected of the technology by the interested party. It is a natural language document (i.e., avoiding CC abbreviations and constructs) that scopes and bounds the security problem for PP by defining a set of use cases, assets, and threats. It then identifies both general and, when appropriate, specific requirements with which an ICT product of this type must comply in order to satisfy the end-users' procurement guidance or technical regulations. The high-level fundamental requirements as the ESR for Encryption Key Management are as follows:

- **Full audit and log traces:** The devices shall maintain a log/record of all key operations according to the date and time at which the operation was carried out.
- **Creating roles from capabilities:** The effective capabilities and domain of each role are required to be set clearly. Once the roles are designed and created, they should be tested to ensure they perform all required range of operations.
- **Secure backup:** The device shall be able to back up settings, encryption keys and associated metadata, and to restore its state based on an earlier backup. The backups shall be encrypted.
- **Secure key generation:** The devices incorporate True Random Number Generators, which generate real-time random numbers based on physical entropy sources.
- **Protection of secret:** The device shall protect keys, key material, and authentication credentials from unauthorized disclosure.
- **Secure authentication mechanism:** The device shall provide an authentication mechanism for local and remote administrators, as well as the device itself (e.g.,

the device maintains an authentication credential that can be used to authenticate it to an administrator's client).
- **Self-test:** The device shall provide self-tests to ensure the security functions it implements are operating correctly.

2) PLANNING: TARGET OF EVALUATION AND TECHNICAL COMMUNITY

To develop the PP for the Encryption Key Management components, we formed a group comprising cybersecurity researchers from Deakin University and Charles Sturt University, government experts from Australian Certification Authority (ACA) of the Australian Cyber Security Centre, vendors (e.g., QuintessenceLabs, Senetas), and evaluators from Teron Labs. ACA and evaluators place the TC on the right track early on so that we can comply with the expectation from the evaluators and certifiers' tutorial. QuintessenceLabs as the vendor representative of encryption key management products, inform the TC of the commercial relevance, previous work and existing products in need of certification.

We first define the usage and major security features of Encryption Key Management in the PP Module, to give end-users a general idea of its capabilities, usage, and whether the TOE meets their security needs [5]. The PP Module specifically addresses the cryptographic key management appliance, which is designed to centrally manage enterprise digital keys and certificates for enterprise applications, users, and devices throughout their full lifecycle, including key generation, distribution, usage, automated rotation, renewal, and destruction in line with TOE-defined policy. The TOE can be deployed as part of any cryptographic system that uses digital keys. The TOE is intended to provide a high-level assurance in protecting the digital keys, especially keys of high value, to avoid negative impacts on the system if the keys were to be compromised.

We further work with the Encryption Key Managers vendors to find out the expected security features of products. In summary, the TOE is expected to provide the following major security features:

- Secure generation, distribution, renewal, and destruction of cryptographic keys.
- On-board cryptographic functions to secure traffic sent between the TOE and external users.
- Secure storage and management of keys throughout their lifecycle.
- Role-based authentication and access control mechanisms to facilitate controlled access to cryptographic key management and TOE management functions by trusted personnel only.
- Functionality to detect errors in received traffic or replay attacks.
- Auditing of security-relevant events to provide suitable accountability.
- Protection of stored audit data to prevent modification or accidental deletion; and
- Self-test of the core cryptographic functions and algorithms of the TOE.

3) DEVELOPMENT: SECURITY PROBLEM, OBJECTIVES AND REQUIREMENTS

In line with the description of the TOE, the security problems are defined in three aspects: threats, organizational security policies, and assumptions [5]. The first part of security problems shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two [29]. A threat is composed of adverse actions on an asset by a threat agent. These adverse actions affect one or more properties of an asset from which that asset derives its value. The organizational security policies are the rules, procedures, or guidelines that are to be enforced by the TOE. Besides, assumptions are made on the operational environment to provide security functionality. Suppose the TOE that is placed in the operational environment does not meet the defined assumptions. In that case, the TOE may not be able to provide all of its security functionality anymore [29].

There are two types of threats agents for Encryption Key Management components: unauthenticated users and unauthorized users. Unauthenticated users refer to individuals who have not been granted access to the application, and they attempt to gain access to information or functions provided by the TOE. Unauthorized users refer to registered individuals who have been explicitly granted access to some parts of the application, but they may attempt to access information or functions that are not permitted. Typically, the operational environments for the TOE involve operating systems, application software, and hardware. To infer the security problem, we include the security problems that may apply to different threat agents, operational environments, and the vulnerabilities of theses for the Encryption Key Management as summarized in Table 1 that extends the security problems defined by the base PP.

Furthermore, to ensure the entire system, including TOE, is completely secure, the security objectives as summarized in Table 2 are the expected solution expressed as a concise and abstract response to the defined security problems. To address the security objectives of the TOE, we define the additional security functional requirements besides these existing in the NDcPP as a translation of the security objectives for the TOE [29]. We have taken an incremental approach by iterating five steps to mature the PP. This approach proved effective for the inter-sectoral DACCA project with partners from academia, industry, and certification authority. Here, we briefly introduce the process. The detailed information can be retrieved from our recent review work [4] on defining security requirements with CC. We begin with brainstorming *Q&A* with initial questions and answers about the target TOE, such as the common characteristics, functions, and security features of the TOE. The second step, *Draft*, aims to outline key information in the developed PP following the CC guidance [5], [13], [29]. Based on literature review, cross-reference to related PPs, and feedback from industrial partners, the third step, *Refinement*, refines the contents by adding the specifications on security requirements and

TABLE 1. Security problems defined in PP Module for encryption key management components.

Threat	Description
T.DATA_INTEGRITY	The TOE may be exposed to the attackers positioned on a communications channel or elsewhere on the network infrastructure that attempt to corrupt or modify data in transit without authorisation. Attackers may monitor and gain access to data exchanged between the interfaces in the TOE and other endpoints to compromise it. The data contained within the communications may be susceptible to a loss of data integrity.
T.DATA_CONFIDENTIALITY	The TOE may be inadvertently configured, used, and administered in an insecure manner (e.g., insecure communications channels) by either authorized or unauthorized persons.
T.DATA_ACCOUNTABILITY	The accountability of audit records for security relevant events is hard to capture if the TOE doesn't have the ability to identify and authenticate users, and to record the behaviour of these users.
T.SECURITY_FUNCTIONALITY_FAILURE	Internal malfunction of TOE functions may result in the modification or misuse of TOE services. This includes hardware failures which prevent the TOE from performing its services. Technical failure may result in an insecure operational state violating the integrity and availability of the TOE services. The correct operation of the TOE also depends on the correct operation of critical hardware and software components. Critical services include: a) cryptographic operations; and b) random number generation.
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	A user may gain unauthorized access to the TOE and residing data.
A.CLIENT	It is assumed that key management clients protect the keys and other security sensitive data that are used to communicate with the TOE.

TABLE 2. Security objectives defined in PP Module for encryption key management components.

Threat	Description
O.AUDIT_RECORD	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.AUDIT_ACCESS_AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.
O.CRYPT	The TOE implements cryptographic functions compliant to the relevant industry standards. The TOE shall be designed to support changes to cryptographic functions, parameters, or communications protocols, to address emerging threats. The changes may be applied via software upgrades.
O.DATA_TRANSIMISSION	The TOE shall utilize cryptographic functions and industry standards (TLS 1.3 (RFC 8446) or TLS 1.2 (RFC 5246) or TLS 1.1 (RFC 4346)) to ensure that data transmitted between a) a TOE and a client, or b) two TOEs, or c) a TOE and an administrator is secure and protected from tampering or modification.
O.CONTROL	The TOE shall restrict TOE security and management functions to authorised roles by a robust access control system.
O.TEST	The TOE shall perform tests to verify that its components operate correctly. This includes testing of the TOE's random number generator and cryptographic module during operation.
O.PROTECT	The TOE shall ensure that all TSF data stored within the TOE are protected sufficiently to prevent their disclosure to a malicious entity.

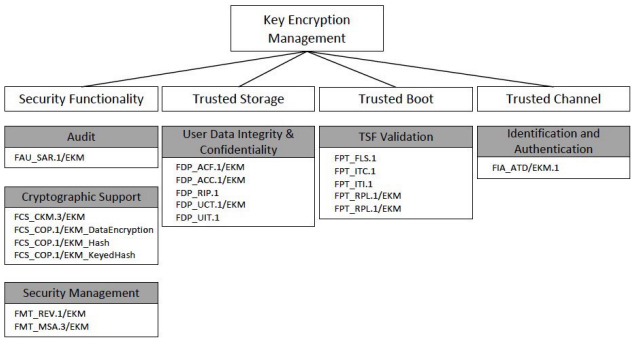


FIGURE 2. Overview of the key encryption management technologies with grouping of SFRs.

evaluation activities. And the next step, *Polishing*, ensures that the security countermeasures are precise and sufficient to respond to the considered threats. The last step *Evaluation* reviews the deliverability of the PP to improve the consistency with the CC standard. The defined SFRs are grouped into four categories, as shown in Figure 2, including security functionality, trusted storage, trusted boot, and trusted channel. The category of security functionality that refers to the security-related features, functions, mechanisms, procedures, and architecture includes the requirements on audit, cryptographic support, and security management. Trusted storage makes sure that the confidentiality and integrity of the stored data are provided and ensured by the storage features of the TOE. Trusted boot defines only valid configurations that can be loaded by the TOE security functionality (TSF) validation. By specifying the requirements on identification and authentication, the integrity and confidentiality of data transmitted between entities can be guaranteed.

In tandem with the PP Module, the SD was developed to provide Evaluation Activities (EAs) for the functionality to be provided by the Encryption Key Management PP Module. The main purpose of the SD is to define the EAs for the evaluators to follow. The operational guidance and details on the tests that guide the evaluators to conduct evaluation will be provided in the SD. In addition, the SD will also help developers to prepare for the evaluation by identifying the specific requirements for the TOE. For example, for the SFR Audit Data Generation FAU_GEN.1, besides the EA for FAU_GEN.1 as described in the NDcPP, the other auditable events and audit data with the TOE (e.g., server connection status, random number generation test results if any, backup and duplication status) should be appropriately audited by the admin for the target TOE. The specific requirements in EA in some cases clarify the meaning of SFR and may identify particular requirements for the content

of ST (especially the TOE Summary Specification (TSS)), user guidance documentation, and possibly supplementary information.

4) VALIDATION: VALIDITY PROOF BEFORE PUBLISHING

Based on the Common Criteria Recognition Arrangement (CCRA) cPP development process, once the development of the PP Module is completed, it will be evaluated and certified against the CC Protection Profile Evaluation (APE Class) [13] before publishing. The objective of PP validation is to ensure that the PP is sound and internally consistent.

The APE Class defines the assurance packages for PP evaluation, including APE_INT PP introduction, APE_CCL conformance claims, APE_SPD security problem definition, APE_OBJ security objectives, APE_ECD extended components definition, and APE_REQ security requirements. These properties are necessary for the PP to be suitable for use as the basis for developing a Security Target (ST) and product evaluation. AP_INT requires that the PP describes the TOE in a narrative way. APE_CCL determines the validity of the conformance claims with other PPs or CC documents. APE_SPD demonstrates that the security problem intended to be addressed by the TOE and its operational environment is clearly defined. APE_OBJ shows that the security objectives completely and adequately address the security problem with the presentation of evidence. APE_ECD requires that any extended security requirements defined by the PP are clear, unambiguous and necessary. Lastly, APE_REQ ensures that the security requirements are well defined, clear, internally consistent, and precise.

After validation, the evaluation can be done either before the first use of the PP in a TOE evaluation or carried out during the first use of the PP for a PP intended to be listed on the PP Portal [30]. Usually, before the first use of the PP Module with the base PP, the accompanying SD is reviewed and approved for initial evaluation use. Given our developed PP Module will be using the NDcPP [17] as its base, the engagement with the network device international Technical Community (iTC) to approve a PP configuration document we developed is needed. The PP configuration is typically prepared and developed by the Network Device iTC with representatives from industry, government agencies, CC test laboratories, and members of academia. The PP Configuration aims to describe that the security functionality of the Encryption Key management complies with the NDcPP [17]. Once the PP Module specified in the approved PP configuration together with the product have all been evaluated and certified successfully at first use, the product with the PP, its SD and PP configuration can be listed on the CC portal's Certified Products List (CPL) as the baseline of same types for this type of security product.

IV. DISCUSSION

In light of the quantum computing prospects [33], [34], [35], [36], we further study the quantum-safe aspect of key distribution protocols to ensure the Encryption Key Management vendors continue to obtain CC certifications in the future.

Quantum-resistant, quantum-safe, and post-quantum cryptography are terms adopted to describe cryptographic algorithms running on the standard encryption/decryption devices and widely recognized by experts to be resistant to cryptanalytic attacks from both classical and quantum computers [37]. Although the subject of cryptography using classical computing has been studied for many decades, the art and science of cryptanalysis that requires a potential quantum computer is relatively new. Considering the functionality and security of Encryption Key Management, we further include the optional requirements in terms of Quantum Key Distribution (QKD) and Quantum Resistant Algorithms (QRAs).

A QKD system typically requires specialized optics and electronics hardware and specialized signal processing/error correction software, which is entirely separate from the capabilities that can reasonably be expected of the general Encryption Key Management software. Current efforts on PP development for preparing and measuring Quantum Key Distribution Modules demonstrates the increasing need for QKD capable and trustworthy equipment [38]. Under the consideration of promoting widespread adoption of the PP Module for Encryption Key Management, we include the SFRs related to QKD and QRAs as optional requirements that can be used for ST authors to evaluate the product with QKD features against the QKD related security requirements in the PP Module. The optional requirements can be included in the ST but do not have to be for a TOE to claim conformance to the Encryption Key Management PP Module.

Firstly, to support QKD systems, a key manager must provide an interface to an universal hashing function, suitable for use as a one-time authenticator (e.g., Poly1305). The key manager interface must allow the QKD system to supply its own key material for use by the hashing function. Secondly, the output of a QKD system is a stream of bits, which can be passed into a key manager where they can be sliced into keys and assigned to end-user applications. There are emerging standards around an output interface for QKD systems. Supports for standards defining the QKD output interface are added as the optional extra in the PP Module. ETSI (a European Standards Organization (ESO) [39]) publishes the industry standard on QKD to contribute towards making QKD a robust deployable solution to protect next generation telecommunications [40]. ETSI GS QKD 004 for QKD application interface and ETSI GS QKD 014 for QKD REST API that define external interfaces of a QKD system as the key standards are included in our PP Module to support interfacing and data transfer between a key management and QKD systems.

To support post-quantum readiness, NIST has initated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms to establish Post-Quantum Cryptography Standardization [41]. After the Round 3 candidates, the third round finalists and candidates for QRAs are released by NIST [42]. Due to the uncertainties on the candidate algorithms, to the best of our knowledge, no existing PPs cover the specification on QRAs. The potential availability of suitable implementations

for Encryption Key Management vendors to use to include the QRAs in the current stage is unclear. Hence, in our developed PP Module, the security requirements on QRAs are added as the optional requirement and request that the selection and usage of QRAs should be consistent with the overall strength of the algorithm used for QRAs recommendations [42]. The future direction on embedding the QRAs into PPs will be studied on how universal each candidate QRA is and whether different QRAs will be needed for different use cases (e.g., embedded processors, over bandwidth-constrained links).

V. CONCLUSION

Common Criteria for Information Technology Security Evaluation, as an international standard for cyber security certification, facilitates mutual recognition of secure ICT products. Under the CC, a Protection Profile defines a set of security objectives and requirements for a specific category of products or systems, which can serve as a benchmark in terms of product security. In this paper, we proposed a PP Module for Encryption Key Management with the demonstration on the development methodology and implementation process. With the collaboration among academic, government and product vendors, the proposed PP Module targets the increasing reliability of Encryption Key Management and the trust of consumers. The vendors can evaluate their products against the security requirements defined in the PP Module, where the security assurance process is to be guided. Besides the mandatory SFRs for the target TOE, we further investigate and embed the quantum-safe algorithms in the PP Module as optional security requirements to support products with quantum-resistant algorithms and quantum key distribution features.

REFERENCES

[1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004.

[2] L. J. Hoffman, K. Lawson-Jenkins, and J. J. Blum, "Trust beyond security: An expanded trust model," *Commun. ACM*, vol. 49, no. 7, pp. 94–101, 2006.

[3] N. Sun, C.-T. Li, H. Chan, M. Z. Islam, M. R. Islam, and W. Armstrong, "How do organizations seek cyber assurance? Investigations on the adoption of the common criteria and beyond," *IEEE Access*, vol. 10, pp. 71749–71763, 2022.

[4] N. Sun, C.-T. Li, H. Chan, B. D. Le, M. Z. Islam, L. Y. Zhang, M. R. Islam, and W. Armstrong, "Defining security requirements with the common criteria: Applications, adoptions, and challenges," *IEEE Access*, vol. 10, pp. 44756–44777, 2022.

[5] Common Criteria. (Apr. 2017). *Common Criteria for Information Technology Security Evaluation—Part 1: Introduction and General Model*. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf

[6] Common Criteria. (2021). *Protection Profiles*. [Online]. Available: https://www.commoncriteriaportal.org/pps/

[7] W. Stallings, *Cryptography and Network Security*, 4th ed. New Delhi, India: Pearson, 2006.

[8] E. Barker and Q. Dang, "NIST special publication 800–57 part 1, revision 4," NIST, Gaithersburg, MD, USA, Tech. Rep. 16, 2016.

[9] *Security Requirements for Cryptographic Modules*, Standard FIPS 140-3, NIST, 2019.

[10] R. Snouffer, A. Lee, and A. Oldenhoeft, "A comparison of the security requirements for cryptographic modules in FIPS 140–1 and FIPS 140–2," Booz-Allen Hamilton, McLean, VA, USA, Tech. Rep. NIST Special Publication 800-29 0704-0188, 2001.

[11] D. L. Evans, P. Bond, and A. Bement, *Security Requirements for Cryptographic Modules*, Standard FIPS Pub 140-2, Federal Information Processing Standards Publication, Gaithersburg, MD, USA, 2002, vol. 12.

[12] Common Criteria. (May 2021). *About the Common Criteria*. [Online]. Available: https://www.commoncriteriaportal.org/ccra/

[13] Common Criteria. (2021). *Certified Products*. [Online]. Available: https://www.commoncriteriaportal.org/products/

[14] D. S. Herrmann, *Using the Common Criteria for IT Security Evaluation*. Boca Raton, FL, USA: CRC Press, 2002.

[15] H. Löhr, A.-R. Sadeghi, C. Stüble, M. Weber, and M. Winandy, "Modeling trusted computing support in a protection profile for high assurance security kernels," in *Proc. Int. Conf. Trusted Comput.* Berlin, Germany: Springer, 2009, pp. 45–62.

[16] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "A survey of cybersecurity certification for the Internet of Things," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–36, Nov. 2021.

[17] Networking International Technical Community. (Mar. 2020). *Collaborative Protection Profile for Network Devices*. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf

[18] H. Corrigan-Gibbs, W. Mu, D. Boneh, and B. Ford, "Ensuring high-quality randomness in cryptographic key generation," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 685–696.

[19] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Phys. Rev. X*, vol. 4, no. 3, Sep. 2014, Art. no. 031056.

[20] I. Kuzminykh, M. Yevdokymenko, and D. Ageyev, "Analysis of encryption key management systems: Strengths, weaknesses, opportunities, threats," in *Proc. IEEE Int. Conf. Problems Infocommun. Sci. Technol. (PIC ST)*, Oct. 2020, pp. 515–520.

[21] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," *Futur. Gener. Comput. Syst.*, vol. 57, pp. 24–41, Apr. 2016.

[22] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "SELAMAT: A new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems," *Sensors*, vol. 21, no. 4, p. 1428, Feb. 2021.

[23] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 6, pp. 1615–1625, Jun. 2014.

[24] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1421–1432, Jul. 2021.

[25] A. M. Caulfield, E. S. Chung, A. Putnam, H. Angepat, J. Fowers, M. Haselman, S. Heil, M. Humphrey, P. Kaur, J.-Y. Kim, D. Lo, T. Massengill, K. Ovtcharov, M. Papamichael, L. Woods, S. Lanka, D. Chiou, and D. Burger, "A cloud-scale acceleration architecture," in *Proc. 49th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO)*, Oct. 2016, pp. 1–13.

[26] D. K. Nilsson, T. Roosta, U. Lindqvist, and A. Valdes, "Key management and secure software updates in wireless process control environments," in *Proc. 1st ACM Conf. Wireless Netw. Secur.*, Mar. 2008, pp. 100–108.

[27] National Information Assurance Partnership. *Protection Profiles in Development*. [Online]. Available: https://www.niap-ccevs.org/Profile/InDraft.cfm

[28] Common Criteria. (2021). *International Technical Communities and Collaborative Protection Profiles*. [Online]. Available: https://www.commoncriteriaportal.org/communities/technical_communities.cfm

[29] Common Criteria. (2021). *Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security*. [Online]. Available: https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

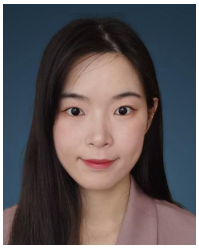
[30] Common Criteria. (2021). *The Common Criteria Portal*. [Online]. Available: https://www.commoncriteriaportal.org/

[31] M. Barbosa, G. Barthe, K. Bhargavan, B. Blanchet, C. Cremers, K. Liao, and B. Parno, "SoK: Computer-aided cryptography," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 777–795.

[32] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2020.

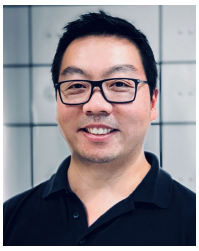
[33] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Trans. Depend. Sec. Comput.*, vol. 19, no. 3, pp. 1885–1899, May 2022.

[34] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir, "A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 681–690, Jan. 2020.
[35] R. Kuang, D. Lou, A. He, and A. Conlon, "Quantum safe lightweight cryptography with quantum permutation pad," in *Proc. IEEE 6th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2021, pp. 790–795.
[36] C. Elliott, "Quantum cryptography," *IEEE Security Privacy*, vol. 2, no. 4, pp. 57–61, Jul. 2004.
[37] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[38] L. Hanke. (Oct. 2021). *Support for QKD Device Evaluations: The Common Criteria Protection Profile for Prepare and Measure Quantum Key Distribution Modules (L12C)*. [Online]. Available: https://iccconference.org/?session=support-for-qkd-device-evaluations-the-common-criteria-protection-profile-for-prepare-and-measure-quantum-key-distribution-modules-l12c
[39] European Telecommunications Standards Institute. (2021). *About ETSI*. [Online]. Available: https://www.etsi.org/about
[40] European Telecommunications Standards Institute. (2021). *Industry Specification Group (ISG) on Quantum Key Distribution (QKD) for Users*. [Online]. Available: https://www.etsi.org/committee/qkd
[41] National Institute of Standards and Technology. (Jun. 2021). *Post-Quantum Cryptography*. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
[42] National Institute of Standards and Technology. (Jun. 2021). *Post-Quantum Cryptography—Round 3 Submissions*. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions



NAN SUN received the B.S. (Hons.) and Ph.D. degrees in information technology from Deakin University. She is currently a Lecturer with the School of Engineering and Information Technology, University of New South Wales (UNSW), Canberra, Australia. Before joining UNSW, she was a Postdoctoral Research Fellow at Deakin University. Her current research interests include cybersecurity and social network security.

CHANG-TSUN LI (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from National Defence University (NDU), Taiwan, in 1987, the M.Sc. degree in computer science from U.S. Naval Postgraduate School, USA, in 1992, and the Ph.D. degree in computer science from the University of Warwick, U.K., in 1998. He was an Associate Professor at the Department of Electrical Engineering, NDU, from 1998 to 2002, and a Visiting Professor at the Department of Computer Science, U.S. Naval Postgraduate School, in the second half of 2001. He was a Professor of the Department of Computer Science, University of Warwick, until January 2017, and a Professor of Charles Sturt University, Australia, from January 2017 to February 2019. He is currently a Professor with the School of Information Technology, Deakin University, Australia. His research interests include multimedia forensics and security, biometrics, data mining, machine learning, data analytics, computer vision, image processing, pattern recognition, bioinformatics, and content-based image retrieval. The outcomes of his multimedia forensics research have been translated into award-winning commercial products protected by a series of international patents and used by a number of police forces and courts of law around the world. He is currently the Chair of IAPR Computational Forensics Technical Committee. He is an Associate Editor of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, *EURASIP Journal on Image and Video Processing (JIVP)*, and *IET Biometrics*.



HIN CHAN is currently the Manager of the Australian Information Security Evaluation Program (AISEP) that resides within the Australian Cyber Security Centre (ACSC). The AISEP performs Common Criteria (CC) evaluation and certification of ICT security products for Australian Organizations use as well as to set standards to improve the security in ICT products. Within this role, he is the Australian Government Advisor on all matters related to product assurance and leads the Strategic Direction of Australia's International Common Criteria Effort. He is also an Australian representative at various international CC committees, at ISO JTC1/SC27 working groups. He is a member of the Accreditation Advisory Committee (AAC) within Australia's national accreditation body for testing laboratories, the National Association of Testing and Accreditation (NATA).

MD ZAHIDUL ISLAM is currently a Professor of computer science with the School of Computing, Mathematics, and Engineering, Charles Sturt University, Australia. His main research interests include data mining/machine learning, privacy preserving data mining, and applications of data mining/machine learning in real life including cyber security.

MD RAFIQUL ISLAM (Senior Member, IEEE) is currently working as an Associate Professor with the School of Computing, Mathematics and Engineering, Charles Sturt University, Australia. His main research interests include cybersecurity focuses on malware analysis and classification, security in the cloud, privacy in social media, and the dark web.

WARREN ARMSTRONG received the Ph.D. degree from Australian National University, in 2011. He is currently the Director of the Engineering at QuintessenceLabs, building cyber security products.