

健保資料與資訊安全

王柏堯 中央研究院資訊科學研究所

資訊安全涵蓋技術、管理、教育等不同面向，本文將從技術面解釋與健保資料相關之資訊安全知識，以供參考。

I. 背景

為達到隱私保障之目的，健保資料庫中可識別個人之資料（姓名、身份證字號、住址、出生日期、醫事人員代碼等），以加密方式處理後才釋出。對敏感資料進行加密，便是資訊安全中常用之手段。而加密之過程及方式種類眾多，大眾不易瞭解，常對加密所提供之安全保障產生誤解。筆者對密碼程式之安全性進行數年之研究，與密碼學家和密碼程式設計師共同合作，期望建立可靠的密碼程式供大眾使用。除此外，筆者曾受健康保險署委託，進入健康保險資料加值中心，共同參與身份證號碼加密亂度之研究。雖然健康保險署與衛生福利部資料庫不同，但運作邏輯相似。而衛生福利部資料庫資料種類眾多，應以更高標準考量其安全性。本文以筆者過去研究及健康保險資料庫使用經驗，分析健保資料庫加密程序之安全性。

II. 加密、解密、密碼系統

「加密」意指對不欲洩露之資料改寫，使他人無法獲得有關原始資料之資訊，而「解密」意指還原改寫後之資料，使原始資料得以重現。在密碼學中，加密與解密是互補的操作。「密碼系統」會提供加密及解密兩個操作。不同的密碼系統，加密及解密操作互不相容，無法將密碼系統甲之解密操作，還原密碼系統乙之加密操作所改寫的資料。過去數十年，密碼學家為了不同的需要，提出各種不同的密碼系統。

密碼學家多半以發表論文的方式，提出新的密碼系統。論文中會仔細敘述密碼系統，並以演算法的形式明確地說明加密與解密的操作，甚至提供程式碼以避免誤解。除此外，密碼學家利用數學說明論文中密碼系統的安全性。而解密專家，則試圖找出論文中密碼系統的漏洞，以實際的行動說明密碼系統的（不）安全性。在密碼學家與解密專家測試密碼系統的安全性後，密碼程式設計師才會為密碼系統編寫

最有效率的程式，並公開程式碼供大眾檢視及使用。在資料加密的過程中，密碼系統提供加密和解密演算法，並不改寫資料。只有密碼程式需要讀取資料，並對資料進行加密和解密等操作。

前述密碼程式建構之過程中，公開檢視是不可缺少之要件。自提出密碼系統的論文開始，加解密演算法就被密碼學家及解密專家檢視。其目的在於避免任何數學推論中有意或是無意的疏失，造成資訊安全上的漏洞。而在加解密演算法經過檢視後，密碼程式設計師所編寫的密碼程式也要經過檢視，以避免程式撰寫中有意或無意之過失，造成資訊系統安全上的破口。

筆者關於資訊安全上之研究，在於提供形式化技術以檢視密碼程式中之錯誤。過去的研究中，曾經檢視多個廣為使用的密碼程式庫，也曾經找出程式庫中密碼程式的錯誤¹。去年底亦受美國國家標準局人員邀請，以虛擬會談的方式，分享形式化技術在密碼系統上之應用²。對於密碼程式之安全性略知一二，也看到國際專家（密碼學家、解密專家、密碼程式設計師）開發密碼系統及程式之過程。即便是舉世公認的密碼專家，也必須將其開發的密碼系統公開以供檢視，否則無法令人分析其密碼系統之安全性，更遑論被廣泛使用。

另以美國國家標準局舉辦之後量子密碼系統標準制定徵選為例，說明公開檢視之普遍性³。為了因應未來量子電腦的出現，美國國家標準局2017年向全世界廣徵足以抵禦量子計算攻擊之密碼系統。所有參加之後量子密碼系統，必須提出詳細文件，說明其演算法，並提供程式碼，置於網頁接受公開檢視。在徵選之過程中，亦有解密專家提出各式攻擊，導致一些後量子密碼系統放棄徵選。美國國家標準局自最初

¹ Fu, Y.-F. F., Liu, J., Shi, X., Tsai, M.-H., Wang, B.-Y. W., & Yang, B.-Y. (2019). Signed Cryptographic Program Verification with Typed Cryptoline. *ACM SIGSAC Conference on Computer and Communications Security* (pp. 1591-1606). London, UK: ACM.

Liu, J., Shi, X., Tsai, M.-H., Wang, B.-Y., & Yang, B.-Y. (2019). Verifying Arithmetic in Cryptographic C Programs. *IEEE/ACM International Conference on Automated Software Engineering* (pp. 552-564). San Diego, USA: IEEE/ACM.

² Mouha, N., & Hailane, A. (2021, January). The Application of Formal Methods to Real-World Cryptographic Algorithms, Protocols, and Systems. *IEEE Computer*, 54, pp. 29-38. doi:10.1109/MC.2020.3033613

³ National Institute of Standards and Technology. (2021). *Post-Quantum Cryptography*. Retrieved from <https://csrc.nist.gov/projects/post-quantum-cryptography>

69 個收件之系統中，經過三輪的評選，於 2020 年七月公佈最後七個進入決選的後量子密碼系統。所有進入決選的系統，其歷史技術資料（包含所有版本之規格文件、演算法、程式碼）一律公開於網頁，以供大眾檢視密碼系統設計及開發過程，以期達到資訊安全之目的。

III. 健康保險資料庫中之加密

健康保險資料庫中對可識別個人之欄位（姓名、住址、醫事人員代碼等），進行多次加密之操作，改寫可識別個人之欄位，以期保障當事人隱私。然而對健康保險資料庫之加密操作，健康保險署僅公開密碼系統之名稱（DES 和 blowfish），而不公開加密操作之演算法及加密程式；而衛生福利部之說明中，甚至連密碼系統名稱都不公開。在健康保險署之研究案中，筆者曾詢問密碼系統之名稱、加密演算法、加密程式等資訊而一無所獲。相關人員一致認為公開任何密碼系統之資訊，將使密碼系統失去安全性，無法達到加密之目的。這無疑與筆者之認知和國際實務操作截然不同。

密碼系統必須經過密碼學家理論上的數學分析，加上解密專家實務上的具體攻擊，才具有初步的安全性。當密碼程式設計師編寫密碼程式時，也必須精準地實現論文中的加解密演算法，些許的差異便可能導致密碼程式失真。若程式與經過理論分析之密碼系統不同，則失去理論分析中之安全保障。這是密碼學界與美國國家標準局要求公開檢視之原因。衛生福利部與健康保險署以資訊安全為由，拒絕公開健康保險資料庫之加密方式，與學術界主流意見相左，筆者沒有足夠資訊得以評估健康保險資料庫加密操作之安全性。

而依據筆者過去之分析密碼程式之經驗，即便專業之密碼學家或密碼程式設計師，也無法保證密碼程式正確性，故樂意公開程式碼以供檢視。筆者也曾在研究中找到程式錯誤，足見開發密碼程式之困難。在衛生福利部與健康保險署密碼程式未經檢視之現況下，筆者很難相信健康保險資料庫加密程式沒有錯誤。不公開密碼系統及程式，往往造成安全的假象，易造成資訊安全之漏洞。

IV. 安全認證

「安全認證」一詞常出現於資訊安全的相關討論中，如健康保險資料庫、數位身份證等，論者多以具備安全認證代表具備實質資訊安全。這是對「安全認證」常見之誤解，故在此加以說明。在管理上，「認證」是以形式的手段，期望達到實質之目的。申請者欲獲得認證，只需準備文件並經過形式上之審查，便可以得到認證。而形式審查是否足以達到實質上之目的，從來不是認證所能提供之保證。

英飛凌是德國知名半導體供應商，其安全晶片經愛沙尼亞政府採用，置於該國數位身份證中。2017 年，英飛凌提供的密碼程式庫被捷克的研究團隊發現漏洞，微軟發佈安全更新，約 75 萬愛沙尼亞數位身份證受影響，也使得愛沙尼亞政府停用該晶片⁴。英飛凌網頁中，指出該密碼程式庫獲得德國聯邦資訊安全機構認證。在過去不知有數學上的弱點，而在認證過程中，亦無弱點被發現。即使知名廠商的密碼程式庫獲得德國安全認證，也不代表該程式庫具備實質安全性。

另一與認證相關之例子是波音 737 MAX 客機。波音 737 MAX 客機在 2016 年一月完成處女航，並在 2017 年三月獲得美國聯邦航空署認證，2017 年五月第一次營運⁵。然而波音 737 MAX 客機在 2019 年三月，由於一連串事故被美國聯邦航空署禁飛，直到 2020 年十一月才解禁。航空器必須獲得美國聯邦航空署安全認證，才能在美國飛行。波音 737 MAX 客機獲得認證後，還是因安全問題而被禁飛，足見即使是美國聯邦航空署之認證，亦無法保證飛行安全無虞。

具體而言，國家安全標準 CNS 27001 對密碼系統之要求如下（詳附件一第 14 頁附錄 A 參考控制目標及控制措施之表 A.1 控制目標及控制措施）：

- A. 10 密碼學
- A. 10.1 密碼式控制措施

⁴ Bernstein, D. J., & Lange, T. (2017). *The cr.yp.to blog*. Retrieved from <https://blog.cr.yp.to/20171105-infineon.html> ROCA vulnerability. (2021). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/ROCA_vulnerability

⁵ Boeing 737 MAX. (2021). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Boeing_737_MAX

目標：確保適當及有效使用密碼學，以保護資訊之機密性、鑑別性及/或完整性。

- A. 10.1.1 使用密碼式控制措施之政策
 控制措施
 應發展及實作政策，關於資訊保護之密碼式控制措施
- A. 10.1.2 金鑰管理
 控制措施
 應發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

其中雖指出對密碼學之控制目標，但是其控制措施卻不明確，筆者也無法從不明確的措施中，推論出所欲之目標。

另一方面，美國國家標準局為密碼模組所訂立之安全要求 FIPS 140-2 中⁶，概論明確指出（詳附件二第一頁第一節第三段）：

“While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure.”

附錄 A 中更明列了 37 份文件要求。密碼模組開發要求中（4.10.3 節），安全層級一有三點要求（附件二第 37 頁，底線為筆者所加）：

- Documentation shall specify the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (see Section 4.1).
- If a cryptographic module contains software or firmware components, documentation shall specify the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module.
- If a cryptographic module contains hardware components, documentation shall specify the schematics and/or Hardware Description Language (HDL) listings for the hardware components.

6

Information Technology Laboratory, National Institute of Standards and Technology. (2001, May 25). Security Requirements for Cryptographic Modules. *FIPS PUB 140-2*. United States of America: Federal Information Processing Standards Publication.

安全層級二有一點要求（附件二第37頁，底線為筆者所加）：

- Documentation shall specify a functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces.

安全層級三列有兩點要求（附件二第38頁，底線為筆者所加）：

- All software and firmware components within a cryptographic module shall be implemented using a high-level language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available.
- If HDL is used, all hardware components within a cryptographic module shall be implemented using a high-level specification language.

其中high-level language和high-level specification language意指撰寫密碼模組時所使用之程式語言必須是較易讀的高階語言。

而最安全層級四列有五點要求（附件二第38頁，底線為筆者所加）：

- Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module security policy. The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.
- Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy.
- Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.
- For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. The preconditions and postconditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure.
- Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification.

在關於密碼模組開發的過程中，最高安全層級的認證共計有 8 份文件 2 項程式語言及 1 項程式註解之要求，而沒有任何實質的安全檢驗或保證。實質的資訊安全隨著技術的發展而不斷改變，現在安全的密碼模組在新的科技下（如速度更快、容量更大的電腦），可能不再安全。以健康保險署所採用的 DES 密碼系統為例，該系統在上世紀末，普遍認為是安全的密碼系統，當時也獲得美國國家標準局之認可。但是現在的科技足以在合理的時間內破解 DES 密碼系統，美國國家標準局也於 2001 年訂立了 AES 密碼系統以取代 DES 密碼系統。足見實質之安全標準沒有永恆的定義，安全認證便無法檢驗實質的資訊安全，更遑論保證資訊安全，而只能以文件之格式，形式上檢視資訊安全。

資訊安全認證如同其他認證，一向是管理手段，無法保證實質資訊安全。在資訊安全的論述中，試圖以「安全認證」所提供之形式上的安全，混淆真實世界中所需之實質的安全，不是正確的作法。

V. 結論

本文自密碼系統設計開始，至密碼程式完成為止，簡述密碼系統及程式如何以公開檢視之方式，達到資訊安全之目的。並比較健康保險資料庫加密以不透明之方式進行，與國際學術、產業界完全公開密碼程式並接受檢視方式之不同。最後釐清關於安全認證中，所得到形式上的安全與實質上的資訊安全之不同。目前健康保險資料加密方式不公開，無以檢視其安全性，實非保障資訊安全，反而易造成安全風險。資訊安全是一場與駭客永不停止的競賽，實質的資訊安全絕非一紙形式上的認證即可獲得。健康保險資料庫中包含大量的個人資料，而將可識別個人之欄位加密，其密碼系統及程式之安全性，直接影響大眾隱私，不可不謹慎評估。

中華民國國家標準

CNS**資訊技術－安全技術－資訊安全
管理系統－要求事項**

總號

2 7 0 0 1

類號

X 6 0 4 9

勘誤表(1)

104 年 8 月 6 日

頁次	位置	原文	更正
12	A.7.1 聘用前	目標：確保員工及 <u>承包者</u> 瞭解其將承擔之責任，且適任其角色。	目標：確保員工及 <u>約用人員</u> 瞭解其將承擔之責任，且適任其角色。
12	A.7.1.2 聘用條款及條件	控制措施 組織與員工及 <u>承包者</u> 簽訂之契約化協議書，應敘明雙方對資訊安全的責任。	控制措施 組織與員工及 <u>約用人員</u> 簽訂之契約化協議書，應敘明雙方對資訊安全的責任。
12	A.7.2 聘用期間	目標：確保員工及 <u>承包者</u> 認知並履行其資訊安全責任。	目標：確保員工及 <u>約用人員</u> 認知並履行其資訊安全責任。
12	A.7.2.1 管理階層責任	控制措施 管理階層應要求所有員工及 <u>承包者</u> ，依組織所建立政策及程序施行資訊安全事宜。	控制措施 管理階層應要求所有員工及 <u>約用人員</u> ，依組織所建立政策及程序施行資訊安全事宜。
12	A.7.2.2 資訊安全認知、教育及訓練	控制措施 組織所有員工及相關之 <u>承包者</u> ，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。	控制措施 組織所有員工及相關之 <u>約用人員</u> ，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。
12	A.7.3.1 聘用責任之終止或變更	控制措施 應對員工及 <u>承包者</u> 定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。	控制措施 應對員工及 <u>約用人員</u> 定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。
20	A.16.1.3 通報資訊安全弱點	控制措施 應要求使用資訊系統及服務之員工及 <u>承包者</u> ，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。	控制措施 應要求使用資訊系統及服務之員工及 <u>約用人員</u> ，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。

(共 1 頁)

公 布 日 期
95 年 6 月 16 日

經濟部標準檢驗局印行

修訂公布日期
103 年 4 月 24 日

印行年月 104 年 8 月

本標準非經本局同意不得翻印

中華民國國家標準

CNS**資訊技術－安全技術－資訊安全
管理系統－要求事項**

總號 2 7 0 0 1

類號 X 6 0 4 9

Information technology – Security techniques – Information security
management systems – Requirements

目錄

節次	頁次
前言	3
0. 簡介	3
0.1 一般	3
0.2 與其他管理系統標準之相容性	3
1. 適用範圍	4
2. 引用標準	4
3. 用語及定義	4
4. 組織全景	4
4.1 瞭解組織及其全景	4
4.2 瞭解關注方之需要及期望	4
4.3 決定資訊安全管理系統之範圍	4
4.4 資訊安全管理系統	4
5. 領導作為	4
5.1 領導及承諾	4
5.2 政策	5
5.3 組織角色、責任及權限	5
6. 規劃	5
6.1 因應風險及機會之行動	5
6.2 資訊安全目標及其達成之規劃	6
7. 支援	7
7.1 資源	7
7.2 能力	7
7.3 認知	7
7.4 溝通或傳達	7
7.5 文件化資訊	7
8. 運作	8
8.1 運作之規劃及控制	8
8.2 資訊安全風險評鑑	8

(共 26 頁)

公 布 日 期
95 年 6 月 16 日

經濟部標準檢驗局印行

修訂公布日期
103 年 4 月 24 日

印行年月 103 年 4 月

本標準非經本局同意不得翻印

8.3 資訊安全風險處理	8
9. 績效評估	9
9.1 監督、量測、分析及評估	9
9.2 內部稽核	9
9.3 管理審查	9
10. 改善	10
10.1 不符合項目及矯正措施	10
10.2 持續改善	10
附錄 A(規定)參考控制目標及控制措施	11
名詞對照	23
參考資料	26

前言

本標準係依據 2013 年發行之第 2 版 ISO/IEC 27001，不變更技術內容，修訂成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。CNS 27001:2007 已修訂並由本標準取代。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

0. 簡介

0.1 一般

本標準之制定旨在提供用以建立、實作、維持及持續改善資訊安全管理系統 (information security management system, ISMS) 之要求事項。採用資訊安全管理系統為組織之策略性決策 (strategic decision)。組織之資訊安全管理系統的建立及實作受組織之需要及目標、安全要求事項、所使用之組織過程與組織之規模及結構所影響。預期所有此等影響因素將隨時間改變。

資訊安全管理系統藉由應用風險管理過程，保持資訊之機密性、完整性及可用性，並就已適切管理風險，賦予關注方信心。

資訊安全管理系統須為組織各項過程及整體管理結構之一部分並與之整合，且須於過程、資訊系統及控制措施之設計中考量資訊安全。預期資訊安全管理系統之實作將依組織需要調整。

本標準可由內部及外部各方使用，以評鑑組織符合組織自身資訊安全要求事項之能力。

本標準各項要求事項呈現之順序，並不反映其重要性或隱含其實作順序。列舉條目編號僅供參引之用。

CNS 27000 引用資訊安全管理系統系列標準 (包括 CNS 27003[2]、CNS 27004[3] 及 CNS 27005[4])，描述資訊安全管理系統之概觀及詞彙，與相關用語及定義。

0.2 與其他管理系統標準之相容性

本標準適用 ISO/IEC Directives, Part 1, Consolidated ISO Supplement 之附錄 SL 所定義之高階結構，相同節次標題、相同文字、共同用語及核心定義，因此得以與其他已採用該附錄之管理系統標準維持相容性。

此定義於該附錄之共同作法，對選擇運作單一管理系統，以滿足 2 或多個管理系統標準要求事項之組織將是有用的。

1. 適用範圍

本標準規定於組織全景內建立、實作、維持及持續改善資訊安全管理系統之要求事項。本標準亦包括依組織需要而裁適之安全風險評鑑及處理的要求事項。本標準敘述之要求事項為通用的，旨在適用於所有組織，不論其型式、規模或性質。當組織宣稱符合本標準時，不得排除本標準第 4 節至第 10 節所規定之任何要求事項。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

CNS 27000 資訊技術－安全技術－資訊安全管理系統－概觀及詞彙

3. 用語及定義

CNS 27000 所規定之用語及定義適用於本標準。

4. 組織全景

4.1 瞭解組織及其全景

組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力者之內部及外部議題。

備考：決定此等議題，係指建立於 CNS 31000[5]5.3 中所考量之組織內部及外部全景。

4.2 瞭解關注方之需要及期望

組織應決定下列事項。

(a) 與資訊安全管理系統有關之關注各方。

(b) 此等關注方對資訊安全之要求事項。

備考：關注方之要求事項可能包括法律及法規要求，以及契約義務。

4.3 決定資訊安全管理系統之範圍

組織應決定資訊安全管理系統之邊界及適用性，以建立其範圍。

於決定範圍時，組織應考量下列事項。

(a) 4.1 中所提及之內部及外部議題。

(b) 4.2 中所提及之要求事項。

(c) 組織履行之活動與其他組織履行之活動間的介面及相依性。

範圍應以文件化資訊提供。

4.4 資訊安全管理系統

組織應依本標準之要求事項，建立、實作、維持及持續改善資訊安全管理系統。

5. 領導作為

5.1 領導及承諾

最高管理階層應藉由下列事項，展現對資訊安全管理系統之領導及承諾。

(a) 確保已建立資訊安全政策及資訊安全目標，並與組織之策略方向相容。

(b) 確保資訊安全管理系統要求事項整合入組織之各項過程。

(c) 確保資訊安全管理系統所需之資源可取得。

(d) 傳達有效之資訊安全管理的重要性，以及符合資訊安全管理系統要求事項之重

要性。

- (e) 確保資訊安全管理系統達成其預期成果。
- (f) 指導及支援人員，以促進資訊安全管理系統之有效性。
- (g) 宣導持續改善。
- (h) 當適用其他相關管理角色之責任範圍時，加以支持以展現其領導權。

5.2 政策

最高管理階層應建立包含下列事項之資訊安全政策。

- (a) 適合於組織之目的。
- (b) 包括資訊安全目標(參照 6.2)或提供設定資訊安全目標使用之框架。
- (c) 包括對滿足相關於資訊安全之適用要求事項的承諾。
- (d) 包括對持續改善資訊安全管理系統之承諾。

資訊安全政策應符合下列項目。

- (e) 以文件化資訊提供。
- (f) 於組織內傳達。
- (g) 適用時，提供給關注方。

5.3 組織角色、責任及權限

最高管理階層應確保資訊安全相關角色之責任及權限已指派並傳達。

最高管理階層應指派下列責任及權限。

- (a) 確保資訊安全管理系統符合本標準之要求事項。
- (b) 向最高管理階層報告資訊安全管理系統之績效。

備考：最高管理階層亦可指派報告組織內資訊安全管理系統績效之責任及權限。

6. 規劃

6.1 因應風險及機會之行動

6.1.1 一般要求

於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及之要求事項，並決定需因應之風險及機會，以達成下列事項。

- (a) 確保資訊安全管理系統達成其預期成果。
- (b) 預防或減少非所欲之影響。
- (c) 達成持續改善。

組織應規劃下列事項。

- (d) 因應此等風險及機會之行動。
- (e) 執行下列事項之方法。
 - (1) 將各項行動整合及實作於其資訊安全管理系統過程之中。
 - (2) 評估此等行動之有效性。

6.1.2 資訊安全風險評鑑

組織應定義及應用資訊安全風險評鑑過程於下列事項中。

- (a) 建立及維持包括下列準則之資訊安全風險準則。
 - (1) 風險接受準則。

(2) 履行資訊安全風險評鑑之準則。

(b) 確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果。

(c) 識別資訊安全風險。

(1) 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險。

(2) 識別風險擁有者。

(d) 分析資訊安全風險。

(1) 評鑑若 6.1.2(c)(1)中所識別之風險實現時，可能導致之潛在後果。

(2) 評鑑 6.1.2(c)(1)中所識別之風險發生的實際可能性。

(3) 決定風險等級。

(e) 評估資訊安全風險。

(1) 以 6.1.2(a)中所建立之風險準則，比較風險分析結果。

(2) 訂定已分析風險之風險處理優先序。

組織應保存關於資訊安全風險評鑑過程之文件化資訊。

6.1.3 資訊安全風險處理

組織應定義並應用資訊安全風險處理過程，以達成下列事項。

(a) 考量風險評鑑結果，選擇適切之資訊安全風險處理選項。

(b) 對所選定資訊安全風險處理選項，決定所有必須實作之控制措施。

備考：組織可依要求設計控制措施，或由任何來源識別之。

(c) 比較上述 6.1.3(b)中所決定之控制措施與附錄 A 中者，並確認未忽略必要之控制措施。

備考 1. 附錄 A 包括控制目標及控制措施之詳細清單。本標準之使用者參照附錄 A 以確保未忽略必要之控制措施。

備考 2. 控制目標隱含於所選定之控制措施中。附錄 A 中所列之各項控制目標及控制措施並未盡列，故可能需要額外之控制目標及控制措施。

(d) 產生適用性聲明，包括必要之控制措施(參照 6.1.3(b)及(c))，且不論是否實作，提供納入之理由，以及由附錄 A 排除之理由。

(e) 制訂資訊安全風險處理計畫。

(f) 取得風險擁有者對資訊安全風險處理計畫之核准，以及對剩餘資訊安全風險之接受。

組織應保存關於資訊安全風險處理過程之文件化資訊。

備考：本標準中之資訊安全風險評鑑與處理過程與 CNS 31000[5]內提供之原則及通用指導綱要調和。

6.2 資訊安全目標及其達成之規劃

組織應於各相關部門及層級建立資訊安全目標。

資訊安全目標應滿足下列事項。

(a) 與資訊安全政策一致。

(b) 可量測(若可行時)。

(c) 考量適用之資訊安全要求事項，以及風險評鑑及風險處理之結果。

(d) 被傳達。

(e) 於適當時，更新之。

組織應保存關於資訊安全目標之文件化資訊。

於規劃如何達成資訊安全目標時，組織應決定下列事項。

(f) 待辦事項。

(g) 所需資源。

(h) 負責人員。

(i) 完成時間。

(j) 結果之評估方式。

7. 支援

7.1 資源

組織應決定並提供建立、實作、維持及持續改善資訊安全管理系統所需之資源。

7.2 能力

組織宜採取下列措施。

(a) 決定於組織控制下執行工作，影響其資訊安全績效人員之必要能力。

(b) 確保此等人員於適當教育、訓練或經驗之基礎上能勝任。

(c) 於適當時，採取取得必要能力之行動，並評估所採取行動之有效性。

(d) 保存適切之文件化資訊，作為勝任之證據。

備考：適用之行動可能包括，例：對現有員工提供訓練、指導或重新指派，或是雇用或委外勝任人員。

7.3 認知

於組織控制下執行工作之人員，應認知下列事項。

(a) 資訊安全政策。

(b) 其對資訊安全管理系統有效性之貢獻，包括改善之資訊安全績效的益處。

(c) 未遵循資訊安全管理系統要求事項之可能後果。

7.4 溝通或傳達

組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項。

(a) 溝通或傳達事項。

(b) 溝通或傳達時間。

(c) 溝通或傳達對象。

(d) 溝通或傳達人員。

(e) 進行有效溝通或傳達所採用過程。

7.5 文件化資訊

7.5.1 一般要求

組織之資訊安全管理系統應包括下列內容。

(a) 本標準要求之文件化資訊。

(b) 由組織所決定對資訊安全管理系統有效性，必要之文件化資訊。

備考：各組織之資訊安全管理系統文件化資訊內容，可能因下列因素而異。

(a) 組織規模，以及其活動之型式、過程、產品及服務。

(b) 各過程及其互動之複雜度。

(c) 人員之能力。

7.5.2 制訂及更新

於制訂及更新文件化資訊時，組織應確保適切之下列項目。

(a) 識別及描述(例：標題、日期、作者或參引號碼)。

(b) 格式(例：語言、軟體版本、圖形)及媒體(例：紙本、電子)。

(c) 合宜性及適切性之審查及核准。

7.5.3 文件化資訊之控制

應控制資訊安全管理系統及本標準要求之文件化資訊，以確保下列事項。

(a) 其於需要處及需要時為可用及適用。

(b) 其受適切保護(例：防止漏失機密性、不當使用或漏失完整性)。

為控制文件化資訊，組織應於適當時，闡明下列活動。

(c) 派送、存取、檢索及使用。

(d) 儲存及保存，包括可讀性之保存。

(e) 變更之控制(例：版本控制)。

(f) 留存及屆期處置(retention and disposition)。

於適當時，應識別及控制由組織所決定對資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊。

備考：存取意謂關於文件化資訊僅可檢視之許可、或檢視及變更文件化資訊之許可及權限的決策等。

8. 運作

8.1 運作之規劃及控制

組織應規劃、實作及控制達成資訊安全要求事項所需之過程，並實作 6.1 中所決定之行動。組織亦應實作各項計畫，以達成 6.2 中所決定之資訊安全目標。

組織應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。組織應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何負面效果。

組織應確保委外過程經確定並受控制。

8.2 資訊安全風險評鑑

組織應依規劃之期間，或當提議或發生重大變更時，考量 6.1.2(a)所建立之準則，執行資訊安全風險評鑑。

組織應保存資訊安全風險評鑑結果之文件化資訊。

8.3 資訊安全風險處理

組織應實作資訊安全風險處理計畫。

組織應保存資訊安全風險處理結果之文件化資訊。

9. 績效評估

9.1 監督、量測、分析及評估

組織應評估資訊安全績效及資訊安全管理系統之有效性。

組織應決定下列事項。

- (a) 需要監督及量測之事項，包括資訊安全過程及控制措施。
- (b) 監督、量測、分析及評估之適用方法，以確保有效的結果。

備考：所選擇之方法宜產生適於比較及可重製視為有效之結果。

- (c) 執行監督及量測之時間。
- (d) 監督及量測之人員。
- (e) 監督及量測結果應分析及評估之時間。
- (f) 分析及評估上述結果之人員。

組織應保存適切之文件化資訊，作為監督及量測結果的證據。

9.2 內部稽核

組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統之下列資訊。

- (a) 是否遵循下列事項。
 - (1) 組織本身對其資訊安全管理系統之要求事項。
 - (2) 本標準之要求事項。

- (b) 是否有效實作及維持。

組織應採取下列作為。

- (c) 規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及報告。該稽核計畫應將所關注之重要過程及前次稽核之結果納入考量。
- (d) 定義各稽核之準則及稽核之範圍。
- (e) 選擇稽核員及施行稽核，以確保稽核過程之客觀性及公平性。
- (f) 確保稽核之結果對相關管理階層報告。
- (g) 保存文件化資訊作為稽核計畫及稽核結果之證據。

9.3 管理審查

最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。

管理審查應包括對下列事項之考量。

- (a) 過往管理審查之議案的處理狀態。
- (b) 與資訊安全管理系統有關之內部及外部議題的變更。
- (c) 資訊安全績效之回饋，包括下列之趨勢。
 - (1) 不符合項目及矯正措施。
 - (2) 監督及量測結果。
 - (3) 稽核結果。
 - (4) 資訊安全目標之達成。
- (d) 關注方之回饋。
- (e) 風險評鑑結果及風險處理計畫之狀態。

(f) 持續改善之機會。

管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。

組織應保存文件化資訊，以作為管理審查結果之證據。

10. 改善

10.1 不符合項目及矯正措施

不符合項目發生時，組織應有下列作為。

(a) 對不符合項目反應，並於適當時採取下列作為。

(1) 採取行動以控制並矯正之。

(2) 處理其後果。

(b) 藉由下列作為，評估對消除不符合項目之原因的行動之需要，使其不再發生且不於他處發生。

(1) 審查不符合項目。

(2) 決定不符合項目之原因。

(3) 決定是否有類似之不符合項目存在，或可能發生。

(c) 實作所有所需行動。

(d) 審查所有所採取矯正措施之有效性。

(e) 若必要時，則對資訊安全管理系統進行變更。

矯正措施應切合所遇到之不符合項目。

組織應保存文件化資訊，以作為下列事項之證據。

(f) 不符合項目之本質及後續採取之所有行動。

(g) 所有矯正措施之結果。

10.2 持續改善

組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。

附錄 A

(規定)

參考控制目標及控制措施

表 A.1 所列之各項控制目標及控制措施，乃直接取自 CNS 27002[1]之第 5 至 18 節，並與之調和，且於內文中與 6.1.3 一起使用。

表 A.1 控制目標及控制措施

A.5 資訊安全政策		
A.5.1 資訊安全之管理指導方針		
目標：依營運要求及相關法律與法規，提供資訊安全之管理指導方針及支持。		
A.5.1.1	資訊安全政策	控制措施 資訊安全政策應由管理階層定義並核准，且對所有員工及相關外部各方公布及傳達。
A.5.1.2	資訊安全政策之審查	控制措施 資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。
A.6 資訊安全之組織		
A.6.1 內部組織		
目標：建立管理框架，以於組織內啟動及控制資訊安全之實作及運作。		
A.6.1.1	資訊安全之角色及責任	控制措施 應定義及配置所有資訊安全責任。
A.6.1.2	職務區隔	控制措施 衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。
A.6.1.3	與權責機關之連繫	控制措施 應維持與相關權責機關之適切聯繫。
A.6.1.4	與特殊關注方之連繫	控制措施 應維持與各特殊關注方或其他各專家安全論壇及專業協會之適切聯繫。
A.6.1.5	專案管理之資訊安全	控制措施 不論專案之型式，應在專案管理中因應資訊安全。
A.6.2 行動裝置及遠距工作		
目標：確保遠距工作及使用行動裝置之安全。		
A.6.2.1	行動裝置政策	控制措施 應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。
A.6.2.2	遠距工作	控制措施 應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。

表 A.1 控制目標及控制措施(續)

A.7 人力資源安全		
A.7.1 聘用前		
目標：確保員工及承包者瞭解其將承擔之責任，且適任其角色。		
A.7.1.1	篩選	控制措施 對所有可能被聘用者所進行之背景調查，應依相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊的保密等級及組織所察覺之風險聘用。
A.7.1.2	聘用條款及條件	控制措施 組織與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。
A.7.2 聘用期間		
目標：確保員工及承包者認知並履行其資訊安全責任。		
A.7.2.1	管理階層責任	控制措施 管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。
A.7.2.2	資訊安全認知、教育及訓練	控制措施 組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。
A.7.2.3	懲處過程	控制措施 應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。
A.7.3 聘用之終止及變更		
目標：將保護組織利益納入聘用變更或終止聘用過程之一部分。		
A.7.3.1	聘用責任之終止或變更	控制措施 應對員工及承包者定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。
A.8 資產管理		
A.8.1 資產責任		
目標：識別組織之資產並定義適切之保護責任。		
A.8.1.1	資產清冊	控制措施 應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。
A.8.1.2	資產擁有權	控制措施 清冊中所維持之資產應具擁有者。
A.8.1.3	資產之可被接受使用	控制措施 對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

表 A.1 控制目標及控制措施(續)

A.8.1.4	資產之歸還	控制措施 所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。
A.8.2 資訊分級		
目標：確保資訊依其對組織之重要性，受到適切等級的保護。		
A.8.2.1	資訊之分級	控制措施 資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。
A.8.2.2	資訊之標示	控制措施 應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。
A.8.2.3	資產之處置	控制措施 應依組織所採用之資訊分級方案，發展及實作處置資產之程序。
A.8.3 媒體處置		
目標：防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。		
A.8.3.1	可移除式媒體之管理	控制措施 應依組織所採用之資訊分級方案，實作管理可移除式媒體之程序。
A.8.3.2	媒體之汰除	控制措施 當不再需要媒體時，應使用正式程序加以安全汰除。
A.8.3.3	實體媒體傳送	控制措施 應保護含有資訊之媒體於傳送時，不受未經授權的存取、誤用或毀損。
A.9 存取控制		
A.9.1 存取控制之營運要求事項		
目標：限制對資訊及資訊處理設施之存取。		
A.9.1.1	存取控制政策	控制措施 存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。
A.9.1.2	對網路及網路服務之存取	控制措施 應僅提供予使用者存取其已被特定授權使用之網路及網路服務。
A.9.2 使用者存取管理		
目標：確保經授權使用者對系統及服務之存取，並防止未經授權之存取。		
A.9.2.1	使用者註冊及註銷	控制措施 應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

表 A.1 控制目標及控制措施(續)

A.9.2.2	使用者存取權限之配置	控制措施 應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。
A.9.2.3	具特殊存取權限之管理	控制措施 應限制及控制具特殊存取權限之配置及使用。
A.9.2.4	使用者之秘密鑑別資訊的管理	控制措施 應以正式之管理過程控制秘密鑑別資訊的配置。
A.9.2.5	使用者存取權限之審查	控制措施 資產擁有者應定期審查使用者之存取權限。
A.9.2.6	存取權限之移除或調整	控制措施 所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。
A.9.3 使用者責任		
目標：令使用者對保全其鑑別資訊負責。		
A.9.3.1	秘密鑑別資訊之使用	控制措施 於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。
A.9.4 系統及應用存取控制		
目標：防止系統及應用遭未經授權之存取。		
A.9.4.1	資訊存取限制	控制措施 應依存取控制政策，限制對資訊及應用系統功能之存取。
A.9.4.2	保全登入程序	控制措施 當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。
A.9.4.3	通行碼管理系統	控制措施 通行碼管理系統應為互動式，並應確保嚴謹通行碼。
A.9.4.4	具特殊權限公用程式之使用	控制措施 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。
A.9.4.5	對程式源碼之存取控制	控制措施 應限制對程式源碼之存取。
A.10 密碼學		
A.10.1 密碼式控制措施		
目標：確保適當及有效使用密碼學，以保護資訊之機密性、鑑別性及/或完整性。		
A.10.1.1	使用密碼式控制措施之政策	控制措施 應發展及實作政策，關於資訊保護之密碼式控制措施的使用。

表 A.1 控制目標及控制措施(續)

A.10.1.2	金鑰管理	控制措施 應發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。
A.11 實體及環境安全		
A.11.1 保全區域		
目標：防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。		
A.11.1.1	實體安全周界	控制措施 應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。
A.11.1.2	實體進入控制措施	控制措施 保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。
A.11.1.3	保全之辦公室、房間及設施	控制措施 應設計辦公室、房間及設施之實體安全並施行之。
A.11.1.4	防範外部及環境威脅	控制措施 應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。
A.11.1.5	於保全區域內工作	控制措施 應設計並施行於保全區域內工作之程序。
A.11.1.6	交付及裝卸區	控制措施 對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。
A.11.2 設備		
目標：防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。		
A.11.2.1	設備安置及保護	控制措施 應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。
A.11.2.2	支援之公用服務事業	控制措施 應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。
A.11.2.3	佈纜安全	控制措施 應保護傳送資料或支援資訊服務之電源及電信佈纜，以防範竊聽、干擾或損害。
A.11.2.4	設備維護	控制措施 應正確維護設備，以確保其持續之可用性及完整性。
A.11.2.5	資產之攜出	控制措施 未經事前授權，不得將設備、資訊或軟體帶出場域外。

表 A.1 控制目標及控制措施(續)

A.11.2.6	場所外設備及資產之安全	控制措施 安全應適用於場域外資產，並將於組織場所外工作之不同風險納入考量。
A.11.2.7	設備汰除或再使用之保全	控制措施 含有儲存媒體之所有設備組件，於汰除或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。
A.11.2.8	無人看管之使用者設備	控制措施 使用者應確保無人看管之設備具適切保護。
A.11.2.9	桌面淨空及螢幕淨空政策	控制措施 對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。
A.12 運作安全		
A.12.1 運作程序及責任		
目標：確保資訊處理設施之正確及安全操作。		
A.12.1.1	文件化運作程序	控制措施 運作程序應加以文件化，並使所有有需要之使用者均可取得。
A.12.1.2	變更管理	控制措施 應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。
A.12.1.3	容量管理	控制措施 各項資源之使用應受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。
A.12.1.4	開發、測試及運作環境之區隔	控制措施 應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。
A.12.2 防範惡意軟體		
目標：確保資訊及資訊處理設施，以防範惡意軟體。		
A.12.2.1	防範惡意軟體之控制措施	控制措施 應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。
A.12.3 備份		
目標：防範資料漏失。		
A.12.3.1	資訊備份	控制措施 應依議定之備份政策，定期取得資訊、軟體及系統的影像備份複本，並測試之。

表 A.1 控制目標及控制措施(續)

A.12.4 存錄及監視		
目標：記錄事件並產生證據。		
A.12.4.1	事件存錄	控制措施 應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。
A.12.4.2	日誌資訊之保護	控制措施 應防範存錄設施及日誌資訊遭竄改及未經授權存取。
A.12.4.3	管理者及操作者日誌	控制措施 應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。
A.12.4.4	鐘訊同步	控制措施 組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。
A.12.5 運作中軟體之控制		
目標：確保運作中系統之完整性。		
A.12.5.1	對運作中系統之軟體安裝	控制措施 應實作各項程序，以控制對運作中系統之軟體安裝。
A.12.6 技術脆弱性管理		
目標：防範對技術脆弱性之利用。		
A.12.6.1	技術脆弱性管理	控制措施 應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。
A.12.6.2	對軟體安裝之限制	控制措施 應建立並實作使用者安裝軟體之管控規則。
A.12.7 資訊系統稽核考量		
目標：使稽核活動對運作中系統之衝擊降至最低。		
A.12.7.1	資訊系統稽核控制措施	控制措施 應仔細規劃並議定，涉及查證運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。
A.13 通訊安全		
A.13.1 網路安全管理		
目標：確保對網路及其支援之資訊處理設施中資訊之保護。		
A.13.1.1	網路控制措施	控制措施 應管理及控制網路，以保護資訊系統及應用。

表 A.1 控制目標及控制措施(續)

A.13.1.2	網路服務之安全	控制措施 應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外提供。
A.13.1.3	網路之區隔	控制措施 應區隔各群組之資訊服務、使用者及資訊系統使用的網路。
A.13.2 資訊傳送		
目標：維護組織內及與任何外部個體所傳送資訊之安全。		
A.13.2.1	資訊傳送政策及程序	控制措施 應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。
A.13.2.2	資訊傳送協議	控制措施 協議應闡明組織與外部各方間營運資訊之安全傳送。
A.13.2.3	電子傳訊	控制措施 應適切保護電子傳訊時所涉及之資訊。
A.13.2.4	機密性或保密協議	控制措施 宜識別、定期審查及文件化，以反映組織對資訊保護之需要的機密性或保密協議之要求事項。
A.14 系統獲取、開發及維護		
A.14.1 資訊系統之安全要求事項		
目標：確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。		
A.14.1.1	資訊安全要求事項分析及規格	控制措施 資訊安全相關要求事項，應納入新資訊系統或既有資訊系統之強化的要求事項中。
A.14.1.2	保全公共網路之應用服務	控制措施 應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。
A.14.1.3	保護應用服務交易	控制措施 應保護應用服務交易中涉及之資訊，以防止不完整傳輸、誤選路(mis-routing)、未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。
A.14.2 於開發及支援過程中之安全		
目標：確保於資訊系統之開發生命週期內，設計及實作資訊安全。		
A.14.2.1	保全開發政策	控制措施 應建立軟體及系統開發之規則，並應用至組織內之開發。

表 A.1 控制目標及控制措施(續)

A.14.2.2	系統變更控制程序	控制措施 應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。
A.14.2.3	運作平台變更後，應用之技術審查	控制措施 當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。
A.14.2.4	軟體套件變更之限制	控制措施 應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。
A.14.2.5	保全系統工程原則	控制措施 保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。
A.14.2.6	保全開發環境	控制措施 對涵蓋整個系統開發生命週期之系統開發及整合工作，組織應建立並適切保護安全開發環境。
A.14.2.7	委外開發	控制措施 組織應監督及監視委外系統開發活動。
A.14.2.8	系統安全測試	控制措施 於開發中，應實施安全功能性之測試。
A.14.2.9	系統驗收測試	控制措施 應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。
A.14.3 測試資料		
目標：確保測試用資料之保護。		
A.14.3.1	測試資料之保護	控制措施 應小心選擇、保護及控制測試資料。
A.15 供應者關係		
A.15.1 供應者關係中之資訊安全		
目標：確保對供應者可存取之組織資產的保護。		
A.15.1.1	供應者關係之資訊安全政策	控制措施 應與供應者議定並文件化，降低與供應者存取組織資產關聯之風險的資訊安全要求事項。
A.15.1.2	於供應者協議中闡明安全性	控制措施 應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。
A.15.1.3	資訊及通訊技術供應鏈	控制措施 與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。

表 A.1 控制目標及控制措施(續)

A.15.2 供應者服務交付管理		
目標：維持資訊安全及服務交付之議定等級與供應者協議一致。		
A.15.2.1	供應者服務之監視及審查	控制措施 組織應定期監視、審查及稽核供應者服務交付。
A.15.2.2	管理供應者服務之變更	控制措施 應管理供應者所提供服務之變更，包括維持及改善既有的資訊安全政策、程序及控制措施，並考量所涉及之營運資訊、系統及過程的關鍵性，以及風險之重新評鑑。
A.16 資訊安全事故管理		
A.16.1 資訊安全事故及改善之管理		
目標：確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。		
A.16.1.1	責任及程序	控制措施 應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。
A.16.1.2	通報資訊安全事件	控制措施 應循適切之管理管道，儘速通報資訊安全事件。
A.16.1.3	通報資訊安全弱點	控制措施 應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。
A.16.1.4	對資訊安全事件之評鑑及決策	控制措施 應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。
A.16.1.5	對資訊安全事故之回應	控制措施 應依文件化程序，回應資訊安全事故。
A.16.1.6	由資訊安全事故中學習	控制措施 應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性或衝擊。
A.16.1.7	證據之收集	控制措施 組織應定義及應用程序，以識別、收集、獲取及保存可用作證據之資訊。
A.17 營運持續管理之資訊安全層面		
A.17.1 資訊安全持續		
目標：資訊安全持續應嵌入組織之營運持續管理系統中。		
A.17.1.1	規劃資訊安全持續	控制措施 組織應決定其對資訊安全之要求事項，以及於不利情況下(例：危機或災難期間)，對資訊安全管理之持續性要求事項。

表 A.1 控制目標及控制措施(續)

A.17.1.2	實作資訊安全持續	控制措施 組織應建立、文件化、實作及維持過程、程序及控制措施，以確保不利情況期間所要求之資訊安全持續等級。
A.17.1.3	查證、審查並評估資訊安全持續	控制措施 組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。
A.17.2 多重備援		
目標：確保資訊處理設施之可用性。		
A.17.2.1	資訊處理設施之可用性	控制措施 應對資訊處理設施實作充分之多重備援，以符合可用性要求。
A.18 遵循性		
A.18.1 對法律及契約要求事項之遵循		
目標：避免違反有關資訊安全之法律、法令、法規或契約義務，以及任何安全要求事項。		
A.18.1.1	適用之法規及契約的要求事項之識別	控制措施 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。
A.18.1.2	智慧財產權	控制措施 應實作適切程序，以確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。
A.18.1.3	紀錄之保護	控制措施 應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。
A.18.1.4	個人可識別資訊之隱私及保護	控制措施 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。
A.18.1.5	密碼式控制措施之監管	控制措施 應使用密碼式控制措施，以遵循所有相關協議、法律及法規。
A.18.2 資訊安全審查		
目標：確保依組織政策及程序，實作及運作資訊安全。		
A.18.2.1	資訊安全之獨立審查	控制措施 應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作(亦即資訊安全之各項控制目標、控制措施、政策、過程及程序)。

表 A.1 控制目標及控制措施(續)

A.18.2.2	安全政策及標準之遵循性	控制措施 管理人員應以適切之安全政策、標準及所有其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。
A.18.2.3	技術遵循性審查	控制措施 應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。

名詞對照

—A—

acceptance	驗收；接受
access control	存取控制
adequacy	適切性
application system	應用系統
approach	導向；作法
aspect	層面
assessment	評鑑
asset	資產
audit	稽核
authentication	鑑別
authorization	授權
availability	可用性
awareness	認知

—B—

business continuity management	營運持續管理
--------------------------------	--------

—C—

classification	分級；保密等級
communication	溝通或傳達
compliance	遵循性；遵循
confidentiality	機密性
competence	能力
cryptographic	密碼

—D—

development	發展；開發
disaster	災難
disciplinary	懲處
disposal	汰除；作廢

—E—

equipment	設備
evaluation	評估
event	事件
evidence	證據

—F—

facility	設施
forum	論壇
framework	框架

fraud	詐欺
-H-	
handling	處置
hazard	危害
-I-	
identification	識別
impact	衝擊
implementation	實作
incident	事故
information security	資訊安全
integrity	完整性
interested parties	關注方
intellectual property right, IPR	智慧財產權
information security management system, ISMS	資訊安全管理系統
-K-	
key management	金鑰管理
-L-	
label	標籤；標示
log	日誌；存錄
-M-	
maintenance	維持；維護
malware	惡意軟體
media	媒體
misuse	誤用
mobile device	行動裝置
monitor	監視
-N-	
non-disclosure agreement	保密協議
-O-	
objective	目標
operation	運作；作業；操作
outsource	委外
-P-	
password	通行碼
policy	政策
privilege	特權
procedure	程序
-R-	
registration	註冊

requirement	要求；要求事項
responsibility	責任
review	審查
risk	風險
risk acceptance	風險接受
risk analysis	風險分析
risk assessment	風險評鑑
risk evaluation	風險評估
risk management	風險管理
risk treatment	風險處理
routing	選路
-S-	
scope	範圍
screening	篩選
segregation	區隔
statement of applicability	適用性聲明
suitability	合宜性
synchronization	同步
-T-	
teleworking	遠距工作
threat	威脅
-U-	
unattended user equipment	無人看管之使用者設備
-V-	
vulnerability	脆弱性
-W-	
weakness	弱點

參考資料

- [1] CNS 27002 資訊技術－安全技術－資訊安全管理之作業規範
- [2] CNS 27003 資訊技術－安全技術－資訊安全管理系統實作指引
- [3] CNS 27004 資訊技術－安全技術－資訊安全管理－量測
- [4] CNS 27005 資訊技術－安全技術－資訊安全風險管理
- [5] CNS 31000 風險管理－原則與指導綱要
- [6] ISO/IEC Directives – Part 1 Consolidated ISO Supplement – Procedures specific to ISO 2012

相對應國際標準

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

修訂日期

第一次修訂：96年10月24日

FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY

SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Issued May 25, 2001



U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

William Mehuron, Director
Information Technology Laboratory

Abstract

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Key words: computer security, telecommunication security, cryptography, cryptographic modules, Federal Information Processing Standard (FIPS).

National Institute of Standards
and Technology
FIPS PUB 140-2
64 pages (May 25, 2001)

U.S. Government Printing Office
Washington: 2001

For Sale by the National
Technical Information
Service
U.S. Department of Commerce

**Federal Information
Processing Standards Publication 140-2**

May 25, 2001

**Announcing the Standard for
SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES**

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. Name of Standard. Security Requirements for Cryptographic Modules (FIPS PUB 140-2).

2. Category of Standard. Computer Security Standard, Cryptography.

3. Explanation. This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. This standard supersedes FIPS 140-1, *Security Requirements for Cryptographic Modules*, in its entirety.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories perform cryptographic module compliance/conformance testing.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. Cross Index.

- a. FIPS PUB 46-3, Data Encryption Standard.
- b. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.
- c. FIPS PUB 81, DES Modes of Operation.
- d. FIPS PUB 113, Computer Data Authentication.

- e. FIPS PUB 171, Key Management Using ANSI X9.17.
- f. FIPS PUB 180-1, Secure Hash Standard.
- g. FIPS PUB 186-2, Digital Signature Standard.
- h. Special Publication 800-2, Public Key Cryptography.
- i. Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures

These documents may be found at the CMVP URL <http://www.nist.gov/cmvp>. Other NIST publications may be applicable to the implementation and use of this standard. A list (NIST Publications List 91) of currently available computer security publications, including ordering information, can be obtained from NIST.

7. Applicability. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. The adoption and use of this standard is available to private and commercial organizations.

8. Applications. Cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, and key management) provided by a cryptographic module are based on many factors that are specific to the application and environment. The security level to which a cryptographic module is validated must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module will be utilized and the security services that the module will provide. The security requirements for a particular security level include both the security requirements specific to that level and the security requirements that apply to all modules regardless of the level.

9. Specifications. Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules (affixed).

10. Implementations. This standard covers implementations of cryptographic modules including, but not limited to, hardware components or modules, software/firmware programs or modules or any combination thereof. Cryptographic modules that are validated under the CMVP will be considered as conforming to this standard. Information about the CMVP can be obtained from the

- a. National Institute of Standards and Technology, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.
- b. Communications Security Establishment, ITS Client Services, 1500 Bronson Ave., Ottawa, ON K1G 3Z4.
- c. CMVP URL <http://www.nist.gov/cmvp>.

11. Approved Security Functions. Cryptographic modules that conform to this standard shall employ Approved security functions such as cryptographic algorithms, cryptographic key management techniques, and authentication techniques that have been approved for protecting Federal government sensitive information. Approved security functions include those that are either:

- a. specified in a Federal Information Processing Standard (FIPS),
- b. adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS, or
- c. specified in the list of Approved security functions.

12. Interpretation. Questions concerning the content and specifications of this standard should be addressed to: Director, Information Technology Laboratory, ATTN: FIPS 140-2 Interpretation, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900. Resolution of questions regarding this standard will be provided by the validation authorities at NIST and CSE.

13. Export Control. Certain cryptographic devices and technical data regarding them are subject to Federal export controls and exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Applicable Federal government export controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

14. Implementation Schedule. This standard becomes effective six months after approval by the Secretary of Commerce. A transition period from November 25, 2001 until six months after the effective date is provided to enable all agencies to develop plans for the acquisition of products that are compliant with FIPS 140-2. Agencies may retain and use FIPS 140-1 validated products that have been purchased before the end of the transition period. After the transition period, modules will no longer be tested against the FIPS 140-1 requirements. After the transition period, all previous validations against FIPS 140-1 will still be recognized. Figure 1 summarizes the FIPS 140-2 implementation schedule.

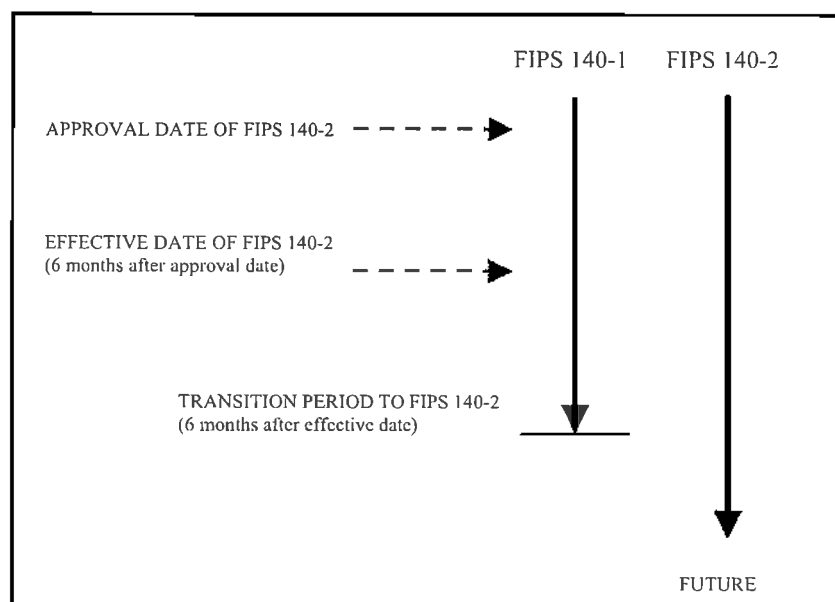


Figure 1. *FIPS 140-2 Implementation Schedule*

15. Qualifications. The security requirements specified in this standard are based upon information provided by many sources within the Federal government and private industry. The requirements are designed to protect against adversaries mounting cost-effective attacks on sensitive government or commercial data (e.g., hackers, organized crime, and economic competitors). The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff.

While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure. The operator of a cryptographic module is responsible for ensuring that the security provided by a module is sufficient and acceptable to the owner of the information that is being protected and that any residual risk is acknowledged and accepted.

Similarly, the use of a validated cryptographic module in a computer or telecommunications system does not guarantee the security of the overall system. The responsible authority in each agency shall ensure that the security of the system is sufficient and acceptable.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, this standard will be reviewed every five years in order to consider new or revised requirements that may be needed to meet technological and economic changes.

16. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal agencies, or their delegates, may approve waivers to Federal Information Processing Standards (FIPS), for their agency. The heads of such agencies may redelegate such authority only to a senior official designated pursuant to Section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when compliance with a standard would

- a. adversely affect the accomplishment of the mission of an operator of Federal computer system or
- b. cause a major adverse financial impact on the operator that is not offset by government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine which conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision that explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decision, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the **Federal Register**.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the **Commerce Business Daily** as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under Section 552(b) of Title 5, U.S. Code, shall be part of the procurement documentation and retained by the agency.

17. Where to obtain copies. Copies of this publication are available from the URL: <http://csrc.nist.gov/publications>. Copies are available for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 140-2 (FIPSPUB1402) and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account, or charged to a credit card accepted by NTIS.

18. CHANGE NOTICE. See important change notice at the end of this document.

TABLE OF CONTENTS

1. OVERVIEW.....	1
1.1 Security Level 1.....	1
1.2 Security Level 2.....	2
1.3 Security Level 3.....	2
1.4 Security Level 4.....	3
2. GLOSSARY OF TERMS AND ACRONYMS.....	4
2.1 Glossary of Terms	4
2.2 Acronyms	8
3. FUNCTIONAL SECURITY OBJECTIVES.....	11
4. SECURITY REQUIREMENTS.....	12
4.1 Cryptographic Module Specification.....	13
4.2 Cryptographic Module Ports and Interfaces	14
4.3 Roles, Services, and Authentication	15
4.3.1 Roles.....	16
4.3.2 Services.....	16
4.3.3 Operator Authentication	17
4.4 Finite State Model	19
4.5 Physical Security	20
4.5.1 General Physical Security Requirements.....	21
4.5.2 Single-Chip Cryptographic Modules.....	23
4.5.3 Multiple-Chip Embedded Cryptographic Modules.....	24
4.5.4 Multiple-Chip Standalone Cryptographic Modules.....	25
4.5.5 Environmental Failure Protection/Testing.....	26
4.6 Operational Environment	27
4.6.1 Operating System Requirements	28
4.7 Cryptographic Key Management.....	30
4.7.1 Random Number Generators (RNGs).....	30
4.7.2 Key Generation.....	31
4.7.3 Key Establishment.....	31
4.7.4 Key Entry and Output.....	31
4.7.5 Key Storage	33
4.7.6 Key Zeroization	33
4.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	33
4.9 Self-Tests.....	33
4.9.1 Power-Up Tests	34
4.9.2 Conditional Tests.....	35
4.10 Design Assurance.....	36
4.10.1 Configuration Management.....	36
4.10.2 Delivery and Operation.....	37
4.10.3 Development.....	37
4.10.4 Guidance Documents.....	38
4.11 Mitigation of Other Attacks.....	39
APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS	41
APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES	45
APPENDIX C: CRYPTOGRAPHIC MODULE SECURITY POLICY.....	47
APPENDIX D: SELECTED BIBLIOGRAPHY	51

APPENDIX E: APPLICABLE INTERNET UNIFORM RESOURCE LOCATORS (URL)..... 53

CHANGE NOTICE..... 54

 Change Notice 1 (Superceded by Change Notice 2) 54

 Change Notice 2 55

 Change Notice 3 60

 Change Notice 4 61

1. OVERVIEW

This standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

FIPS 140-1 was developed by a government and industry working group composed of both operators and vendors. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 11 requirement areas. Each security level offers an increase in security over the preceding level. These four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. FIPS 140-2 incorporates changes in applicable standards and technology since the development of FIPS 140-1 as well as changes that are based on comments received from the vendor, laboratory, and user communities.

While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure. The operator of a cryptographic module is responsible for ensuring that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.

Similarly, the use of a validated cryptographic module in a computer or telecommunications system is not sufficient to ensure the security of the overall system. The overall security level of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and environment.

The importance of security awareness and of making information security a management priority should be communicated to all users. Since information security requirements vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

The following sections provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive.

The location of Annexes A, B, C, and D can be found in APPENDIX D: SELECTED BIBLIOGRAPHY.

1.1 Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

1.2 Security Level 2

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified in the Common Criteria (CC) Protection Profiles (PPs) listed in Annex B and
- is evaluated at the CC evaluation assurance level EAL2 (or higher).

An equivalent evaluated trusted operating system may be used. A trusted operating system provides a level of trust so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

1.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

Security Level 3 requires the entry or output of plaintext CSPs (including the entry or output of plaintext CSPs using split knowledge procedures) be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. Plaintext CSPs may be entered into or output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified in the PPs listed in Annex B with the additional functional requirement of a Trusted Path (FTP_TRP.1) and
- is evaluated at the CC evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An equivalent evaluated trusted operating system may be used. The implementation of a trusted path protects plaintext CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

1.4 Security Level 4

Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified for Security Level 3 and
- is evaluated at the CC evaluation assurance level EAL4 (or higher).

An equivalent evaluated trusted operating system may be used.

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are tailored for use in this standard:

Approved: FIPS-Approved and/or NIST-recommended.

Approved mode of operation: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

Approved security function: for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either

- a) specified in an Approved standard,
- b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
- c) specified in the list of Approved security functions.

Authentication code: a cryptographic checksum based on an Approved security function (also known as a Message Authentication Code).

Automated key transport: the transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).

Compromise: the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Control information: information that is entered into a cryptographic module for the purposes of directing the operation of the module.

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

Cryptographic boundary: an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in an Approved security function to form a plaintext cryptographic key or perform a cryptographic function.

Cryptographic module: the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Cryptographic module security policy: a precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard and additional rules imposed by the vendor. (See Appendix C.)

Crypto officer: an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.

Data path: the physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths.

Differential power analysis (DPA): an analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.

Digital signature: the result of a cryptographic transformation of data which, when properly implemented, provides the services of:

1. origin authentication
2. data integrity, and
3. signer non-repudiation.

Electromagnetic compatibility (EMC): the ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment.

Electromagnetic interference (EMI): electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system.

Electronic key entry: the entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.)

Encrypted key: a cryptographic key that has been encrypted using an Approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

Environmental failure protection (EFP): the use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range.

Environmental failure testing (EFT): the use of testing to provide a reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

Finite state model: a mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state.

Firmware: the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Hardware: the physical equipment within the cryptographic boundary used to process programs and data.

Hash-based message authentication code (HMAC): a message authentication code that utilizes a keyed hash.

Initialization vector (IV): a vector used in defining the starting point of an encryption process within a cryptographic algorithm.

Input data: information that is entered into a cryptographic module for the purposes of transformation or computation using an Approved security function.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Interface: a logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key establishment: the process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

Key loader: a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Key transport: secure transport of cryptographic keys from one cryptographic module to another module.

Manual key transport: a non-electronic means of transporting cryptographic keys.

Manual key entry: the entry of cryptographic keys into a cryptographic module, using devices such as a keyboard.

Microcode: the elementary processor instructions that correspond to an executable program instruction.

Operator: an individual accessing a cryptographic module or a process (subject) operating on behalf of the individual, regardless of the assumed role.

Output data: information that is produced from a cryptographic module.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal identification number (PIN): an alphanumeric code or password used to authenticate an identity.

Physical protection: the safeguarding of a cryptographic module, cryptographic keys, or CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Port: a physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Private key: a cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Random Number Generator: Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.

Removable cover: a cover designed to permit physical access to the contents of a cryptographic module.

Secret key: a cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single secret key for both encryption and decryption.

Security policy: see Cryptographic module security policy.

Seed key: a secret value used to initialize a cryptographic function or operation.

Simple power analysis (SPA): a direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

Software: the programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.

Split knowledge: a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

Status information: information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.

System software: the special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.

Tamper detection: the automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.

Tamper evidence: the external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.)

Tamper response: the automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the zeroization of plaintext keys and CSPs).

Target of Evaluation (TOE): an information technology product or system and associated administrator and user guidance documentation that is the subject of an evaluation.

TEMPEST: a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.

TOE Security Functions (TSF): used in the Common Criteria, a set of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE Security Policy.

TOE Security Policy (TSP): used in the Common Criteria, a set of rules that regulate how assets are managed, protected, and distributed within a Target of Evaluation.

Trusted path: a means by which an operator and a TOE Security Function can communicate with the necessary confidence to support the TOE Security Policy.

User: an individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.

Validation authorities: NIST and CSE.

Zeroization: a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

2.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

ANSI	American National Standards Institute
API	Application Program Interface

CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment of the Government of Canada
CSP	Critical Security Parameter
DES	Data Encryption Standard
DOD	Department of Defense
DPA	Differential Power Analysis
DTR	Derived Test Requirements
EAL	Common Criteria Evaluation Assurance Level
EDC	Error Detection Code
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IG	Implementation Guidance
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector

NIST	National Institute of Standards and Technology
NTIS	National Technical Information Service
PIN	Personal Identification Number
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
SPA	Simple Power Analysis
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	Target of Evaluation Security Policy
URL	Uniform Resource Locator

3. FUNCTIONAL SECURITY OBJECTIVES

The security requirements specified in this standard relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module:

- To employ and correctly implement the Approved security functions for the protection of sensitive information.
- To protect a cryptographic module from unauthorized operation or use.
- To prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and CSPs.
- To prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and CSPs.
- To provide indications of the operational state of the cryptographic module.
- To ensure that the cryptographic module performs properly when operating in an Approved mode of operation.
- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors.

4. SECURITY REQUIREMENTS

This section specifies the security requirements that shall be satisfied by cryptographic modules conforming to this standard. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. An additional area concerned with the mitigation of other attacks is currently not tested but the vendor is required to document implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas.

	<i>Security Level 1</i>	<i>Security Level 2</i>	<i>Security Level 3</i>	<i>Security Level 4</i>
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15, Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Table 1: *Summary of security requirements*

A cryptographic module shall be tested against the requirements of each area addressed in this section. The cryptographic module shall be independently rated in each area. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic

module will receive a rating that reflects the maximum security level for which the module fulfills all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the cryptographic module will receive a rating commensurate with the overall level of security.

In addition to receiving independent ratings for each of the security areas, a cryptographic module will also receive an overall rating. The overall rating will indicate the minimum of the independent ratings received in the areas.

Many of the security requirements of this standard include specific documentation requirements that are summarized in Appendices A and C. All documentation, including copies of the user and installation manuals, shall be provided to the testing laboratory by the vendor.

4.1 Cryptographic Module Specification

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation. Non-Approved security functions may also be included for use in non-Approved modes of operation. The operator shall be able to determine when an Approved mode of operation is selected. For Security Levels 1 and 2, the cryptographic module security policy may specify when a cryptographic module is performing in an Approved mode of operation. For Security Levels 3 and 4, a cryptographic module shall indicate when an Approved mode of operation is selected. (Approved security functions are listed in Annex A to this standard.)

A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical bounds of a cryptographic module. If a cryptographic module consists of software or firmware components, the cryptographic boundary shall contain the processor(s) and other hardware components that store and protect the software and firmware components. Hardware, software, and firmware components of a cryptographic module can be excluded from the requirements of this standard if shown that these components do not affect the security of the module.

The following documentation requirements shall apply to all security-specific hardware, software, and firmware contained within a cryptographic module. These requirements do not apply to microcode or system software whose source code is not available to the vendor or to any hardware, software, or firmware components that can be shown not to affect the security of the cryptographic module.

- Documentation shall specify the hardware, software, and firmware components of a cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module (see Section 4.5).
- Documentation shall specify any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this standard and explain the rationale for the exclusion.
- Documentation shall specify the physical ports and logical interfaces and all defined input and output data paths of a cryptographic module.
- Documentation shall specify the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics.
- Documentation shall list all security functions, both Approved and non-Approved, that are employed by a cryptographic module and shall specify all modes of operation, both Approved and non-Approved.

- Documentation shall specify:
 - a block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory, and
 - the design of the hardware, software, and firmware components of a cryptographic module. High-level specification languages for software/firmware or schematics for hardware shall be used to document the design.
- Documentation shall specify all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.
- Documentation shall specify a cryptographic module security policy. The security policy shall include the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor (see Appendix C).

4.2 Cryptographic Module Ports and Interfaces

A cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. The cryptographic module interfaces shall be logically distinct from each other although they may share one physical port (e.g., input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g., input data may enter via both a serial and a parallel port). An Application Program Interface (API) of a software component of a cryptographic module may be defined as one or more logical interfaces(s).

A cryptographic module shall have the following four logical interfaces ("input" and "output" are indicated from the perspective of the module):

Data input interface. All data (except control data entered via the control input interface) that is input to and processed by a cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and status information from another module) shall enter via the "data input" interface.

Data output interface. All data (except status data output via the status output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another module) shall exit via the "data output" interface. All data output via the data output interface shall be inhibited when an error state exists and during self-tests (see Section 4.9).

Control input interface. All input commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the "control input" interface.

Status output interface. All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface.

All external electrical power that is input to a cryptographic module (including power from an external power source or batteries) shall enter via a power port. A power port is not required when all power is

provided or maintained internally to the cryptographic boundary of the cryptographic module (e.g., an internal battery).

The cryptographic module shall distinguish between data and control for input and data and status for output. All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path. All output data exiting the cryptographic module via the "data output" interface shall only pass through the output data path. The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroization. To prevent the inadvertent output of sensitive information, two independent internal actions shall be required to output data via any output interface through which plaintext cryptographic keys or CSPs or sensitive data are output (e.g., two different software flags are set, one of which may be user initiated; or two hardware gates are set serially from two separate actions).

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, the physical port(s) and logical interface(s) used for the input and output of plaintext cryptographic keys, cryptographic key components, authentication data, and CSPs may be shared physically and logically with other ports and interfaces of the cryptographic module.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4,

- the physical port(s) used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be physically separated from all other ports of the cryptographic module

or

- the logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path,

and

- plaintext cryptographic key components, authentication data, and other CSPs shall be directly entered into the cryptographic module (e.g., via a trusted path or directly attached cable). (See Section 4.7.4.)

4.3 Roles, Services, and Authentication

A cryptographic module shall support authorized roles for operators and corresponding services within each role. Multiple roles may be assumed by a single operator. If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services. An operator is not required to assume an authorized role to perform services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., *show status*, *self-tests*, or other services that do not affect the security of the module).

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module, and to verify that the operator is authorized to assume the requested role and perform the services within the role.

4.3.1 Roles

A cryptographic module shall support the following authorized roles for operators:

User Role. The role assumed to perform general security services, including cryptographic operations and other Approved security functions.

Crypto Officer Role: The role assumed to perform cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions).

If the cryptographic module allows operators to perform maintenance services, then the module shall support the following authorized role:

Maintenance Role: The role assumed to perform physical maintenance and/or logical maintenance services (e.g., hardware/software diagnostics). All plaintext secret and private keys and unprotected CSPs shall be zeroized when entering or exiting the maintenance role.

A cryptographic module may support other roles or sub-roles in addition to the roles specified above.

Documentation shall specify all authorized roles supported by the cryptographic module.

4.3.2 Services

Services shall refer to all of the services, operations, or functions that can be performed by a cryptographic module. *Service inputs* shall consist of all data or control inputs to the cryptographic module that initiate or obtain specific services, operations, or functions. *Service outputs* shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs. Each service input shall result in a service output.

A cryptographic module shall provide the following services to operators:

Show Status. Output the current status of the cryptographic module.

Perform Self-Tests. Initiate and run the self-tests as specified in Section 4.9.

Perform Approved Security Function. Perform at least one Approved security function used in an Approved mode of operation, as specified in Section 4.1.

A cryptographic module may provide other services, operations, or functions, both Approved and non-Approved, in addition to the services specified above. Specific services may be provided in more than one role (e.g., key entry services may be provided in the user role and the crypto officer role).

If a cryptographic module implements a *bypass* capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), then

- two independent internal actions shall be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error (e.g., two different software or hardware flags are set, one of which may be user-initiated), and
- the module shall show status to indicate whether

- 1) the bypass capability *is not* activated, and the module is exclusively providing services *with* cryptographic processing (e.g., plaintext data *is* encrypted),
- 2) the bypass capability *is* activated and the module is exclusively providing services *without* cryptographic processing (e.g., plaintext data *is not* encrypted), or
- 3) the bypass capability *is alternately* activated and deactivated and the module is providing some services *with* cryptographic processing and some services *without* cryptographic processing (e.g., for modules with multiple communication channels, plaintext data *is* or *is not* encrypted depending on each channel configuration).

Documentation shall specify:

- the services, operations, or functions provided by the cryptographic module, both Approved and non-Approved,
- for each service provided by the module, the service inputs, corresponding service outputs, and the authorized role(s) in which the service can be performed, and
- any services provided by the cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

4.3.3 Operator Authentication

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Depending on the security level, a cryptographic module shall support at least one of the following mechanisms to control access to the module:

Role-Based Authentication: If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator and shall authenticate the assumption of the selected role (or set of roles). The cryptographic module is not required to authenticate the individual identity of the operator. The selection of roles and the authentication of the assumption of selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated.

Identity-Based Authentication: If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually identified, shall require that one or more roles either be implicitly or explicitly selected by the operator, and shall authenticate the identity of the operator and the authorization of the operator to assume the selected role (or set of roles). The authentication of the identity of the operator, selection of roles, and the authorization of the assumption of the selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall verify the authorization of the identified operator to assume any role that was not previously authorized.

A cryptographic module may permit an authenticated operator to perform all of the services allowed within an authorized role, or may require separate authentication for each service or for different sets of services. When a cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated.

Various types of authentication data may be required by a cryptographic module to implement the supported authentication mechanisms, including (but not limited to) the knowledge or possession of a password, PIN, cryptographic key, or equivalent; possession of a physical key, token, or equivalent; or

verification of personal characteristics (e.g., biometrics). Authentication data within a cryptographic module shall be protected against unauthorized disclosure, modification, and substitution.

The initialization of authentication mechanisms may warrant special treatment. If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialize the authentication mechanisms.

The strength of the authentication mechanism shall conform to the following specifications:

- For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods).
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.
- Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).
- Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.

Documentation shall specify:

- the authentication mechanisms supported by a cryptographic module,
- the types of authentication data required by the module to implement the supported authentication mechanisms,
- the authorized methods used to control access to the module for the first time and initialize the authentication mechanisms, and
- the strength of the authentication mechanisms supported by the module.

SECURITY LEVEL 1

For Security Level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module. If authentication mechanisms are not supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator.

SECURITY LEVEL 2

For Security Level 2, a cryptographic module shall employ *role-based* authentication to control access to the module.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4, a cryptographic module shall employ *identity-based* authentication mechanisms to control access to the module.

4.4 Finite State Model

The operation of a cryptographic module shall be specified using a finite state model (or equivalent) represented by a state transition diagram and/or a state transition table.

The state transition diagram and/or state transition table includes:

- all operational and error states of a cryptographic module,
- the corresponding transitions from one state to another,
- the input events that cause transitions from one state to another, and
- the output events resulting from transitions from one state to another.

A cryptographic module shall include the following operational and error states:

Power on/off states. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to a cryptographic module.

Crypto officer states. States in which the crypto officer services are performed (e.g., cryptographic initialization and key management).

Key/CSP entry states. States for entering cryptographic keys and CSPs into the cryptographic module.

User states. States in which authorized users obtain security services, perform cryptographic operations, or perform other Approved or non-Approved functions.

Self-test states. States in which the cryptographic module is performing self-tests.

Error states. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

A cryptographic module may contain other states including, but not limited to, the following:

Bypass states. States in which a bypass capability is activated and services are provided without cryptographic processing (e.g., transferring plaintext through the cryptographic module).

Maintenance states. States for maintaining and servicing a cryptographic module, including physical and logical maintenance testing. If a cryptographic module contains a maintenance role, then a maintenance state shall be included.

Documentation shall include a representation of the finite state model (or equivalent) using a state transition diagram and/or state transition table that shall specify:

- all operational and error states of a cryptographic module,
- the corresponding transitions from one state to another,

- the input events, including data inputs and control inputs, that cause transitions from one state to another, and
- the output events, including internal module conditions, data outputs, and status outputs resulting from transitions from one state to another.

4.5 Physical Security

A cryptographic module shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware, software, firmware, and data components within the cryptographic boundary shall be protected.

A cryptographic module that is implemented completely in software such that the physical security is provided solely by the host platform is not subject to the physical security requirements of this standard.

Physical security requirements are specified for three defined physical embodiments of a cryptographic module:

- ***Single-chip cryptographic modules*** are physical embodiments in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected. Examples of single-chip cryptographic modules include single IC chips or smart cards with a single IC chip.
- ***Multiple-chip embedded cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. Examples of multiple-chip embedded cryptographic modules include adapters and expansion boards.
- ***Multiple-chip standalone cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and the entire enclosure is physically protected. Examples of multiple-chip, standalone cryptographic modules include encrypting routers or secure radios.

Depending on the physical security mechanisms of a cryptographic module, unauthorized attempts at physical access, use, or modification will have a high probability of being detected

- subsequent to an attempt by leaving visible signs (i.e., tamper evidence)

and/or

- during an attempt so that appropriate actions can be taken by the cryptographic module to protect plaintext secret and private keys and CSPs (i.e., tamper response).

Table 2 summarizes the physical security requirements, both general and embodiment-specific, for each of the four security levels. The general physical security requirements at each security level are all three distinct physical embodiments of a cryptographic module. The embodiment-specific physical security requirements at each security level enhance the general requirements at the same level, and the embodiment-specific requirements of the previous level.

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage
Security Level 4	EFP or EFT for temperature and voltage	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

Table 2: Summary of physical security requirements

In general, Security Level 1 requires minimal physical protection. Security Level 2 requires the addition of tamper-evident mechanisms. Security Level 3 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for removable covers and doors. Security Level 4 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for the entire enclosure. Environmental failure protection (EFP) or environmental failure testing (EFT) is required at Security Level 4. Tamper detection and tamper response are not substitutes for tamper evidence.

Security requirements are specified for a maintenance access interface when a cryptographic module is designed to permit physical access (e.g., by the module vendor or other authorized individuals).

4.5.1 General Physical Security Requirements

The following requirements shall apply to all physical embodiments.

- Documentation shall specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented.
- Documentation shall specify the physical security mechanisms of a cryptographic module.
- If a cryptographic module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorized individual), then:
 - a maintenance access interface shall be defined,

- ❑ the maintenance access interface shall include all physical access paths to the contents of the cryptographic module, including any removable covers or doors,
- ❑ any removable covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms,
- ❑ all plaintext secret and private keys and CSPs shall be zeroized when the maintenance access interface is accessed, and
- ❑ documentation shall specify the maintenance access interface and how plaintext secret and private keys and CSPs are zeroized when the maintenance access interface is accessed.

SECURITY LEVEL 1

The following requirements shall apply to all cryptographic modules for Security Level 1.

- The cryptographic module shall consist of production-grade components that shall include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).
- When performing physical maintenance, all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be zeroized. Zeroization shall either be performed procedurally by the operator or automatically by the cryptographic module.

SECURITY LEVEL 2

In addition to the general requirements for Security Level 1, the following requirement shall apply to all cryptographic modules for Security Level 2.

- The cryptographic module shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.

SECURITY LEVEL 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements shall apply to all cryptographic modules for Security Level 3.

- If the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module shall contain tamper response and zeroization circuitry. The tamper response and zeroization circuitry shall immediately zeroize all plaintext secret and private keys and CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroization circuitry shall remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.
- If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material).

SECURITY LEVEL 4

In addition to the general requirements for Security Levels 1, 2, and 3, the following requirement shall apply to all cryptographic modules for Security Level 4.

- The cryptographic module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.5.

4.5.2 Single-Chip Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, the following requirements are specific to single-chip cryptographic modules.

SECURITY LEVEL 1

There are no additional Security Level 1 requirements for single-chip cryptographic modules.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements shall apply to single-chip cryptographic modules for Security Level 2.

- The cryptographic module shall be covered with a tamper-evident coating (e.g., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module.
- The tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to single-chip cryptographic modules for Security Level 3.

Either

- the cryptographic module shall be covered with a hard opaque tamper-evident coating (e.g., a hard opaque epoxy covering the passivation)

or

- the enclosure shall be implemented so that attempts at removal or penetration of the enclosure shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to single-chip cryptographic modules for Security Level 4.

- The cryptographic module shall be covered with a hard, opaque removal-resistant coating with hardness and adhesion characteristics such that attempting to peel or pry the coating from the module will have a high probability of resulting in serious damage to the module (i.e., the module will not function).
- The removal-resistant coating shall have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e., the module will not function).

4.5.3 Multiple-Chip Embedded Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, the following requirements are specific to multiple-chip embedded cryptographic modules.

SECURITY LEVEL 1

The following requirement shall apply to multiple-chip embedded cryptographic modules for Security Level 1.

- If the cryptographic module is contained within an enclosure or removable cover, a production-grade enclosure or removable cover shall be used.

SECURITY LEVEL 2

In addition to the requirement for Security Level 1, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 2.

Either

- the cryptographic module components shall be covered with a tamper-evident coating or potting material (e.g., etch-resistant coating or bleeding paint) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components, and
- the tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum,

or

- the cryptographic module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers,
- the enclosure shall be opaque within the visible spectrum, and
- if the enclosure includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys or shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 3.

Either

- the multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum

or

- the applicable Security Level 3 requirements for multiple-chip standalone cryptographic modules shall apply. (Section 4.5.4)

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 4.

- The cryptographic module components shall be covered by potting material or contained within an enclosure encapsulated by a tamper detection envelope (e.g., a flexible mylar printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure) that shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure to an extent sufficient for accessing plaintext secret and private keys cryptographic keys or CSPs.
- The cryptographic module shall contain tamper response and zeroization circuitry that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs. The tamper response and zeroization circuitry shall remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.

4.5.4 Multiple-Chip Standalone Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, the following requirements are specific to multiple-chip standalone cryptographic modules.

SECURITY LEVEL 1

The following requirement shall apply to multiple-chip standalone cryptographic modules for Security Level 1.

- The cryptographic module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 2.

- The enclosure of the cryptographic module shall be opaque within the visible spectrum.
- If the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys or shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 3.

Either

- the multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum

or

- the cryptographic module shall be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 4.

- The potting material or enclosure of the cryptographic module shall be encapsulated by a tamper detection envelope, by the use of tamper detection mechanisms such as cover switches (e.g., microswitches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described above for multiple-chip embedded cryptographic modules. The tamper detection mechanisms shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing plaintext secret and private cryptographic keys and CSPs.
- The cryptographic module shall contain tamper response and zeroization circuitry that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs. The tamper response and zeroization circuitry shall remain operational when plaintext cryptographic keys and CSPs are contained within the cryptographic module.

4.5.5 Environmental Failure Protection/Testing

The electronic devices and circuitry are designed to operate within a particular range of environmental conditions. Deliberate or accidental excursions outside the specified normal operating ranges of voltage and temperature can cause erratic operation or failure of the electronic devices or circuitry that can compromise the security of the cryptographic module. Reasonable assurance that the security of a cryptographic module cannot be compromised by extreme environmental conditions can be provided by having the module employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

For Security Levels 1, 2, and 3, a cryptographic module is not required to employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 4, a cryptographic module shall either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

4.5.5.1 Environmental Failure Protection Features (Alternative 1)

Environmental failure protection (EFP) features shall protect a cryptographic module against unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operating range that can compromise the security of the module. In particular, the cryptographic module shall monitor and correctly respond to fluctuations in the operating *temperature* and *voltage* outside of the specified normal operating ranges.

The EFP features shall involve electronic circuitry or devices that continuously measure the operating temperature and voltage of a cryptographic module. If the temperature or voltage fall outside of the cryptographic module's normal operating range, the protection circuitry shall either (1) shutdown the module to prevent further operation or (2) immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Documentation shall specify the normal operating ranges of a cryptographic module and the environmental failure protection features employed by the module.

4.5.5.2 Environmental Failure Testing Procedures (Alternative 2)

Environmental failure testing (EFT) shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that environmental conditions or fluctuations (accidental or induced) outside the module's normal operating ranges for temperature and voltage will not compromise the security of the module.

EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the cryptographic module resulting in a failure of the electronic devices or circuitry within the module, at no time shall the security of the cryptographic module be compromised.

The temperature range to be tested shall be from -100° to +200° Celsius (-150° to +400° Fahrenheit). The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry to the smallest positive voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry, including reversing the polarity of the voltages.

Documentation shall specify the normal operating ranges of the cryptographic module and the environmental failure tests performed.

4.6 Operational Environment

The *operational environment* of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate. The operational environment can be non-modifiable (e.g., firmware contained in ROM, or software contained in a computer with I/O devices disabled), or modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer). An operating system is an important component of the operating environment of a cryptographic module.

A *general purpose operational environment* refers to the use of a commercially-available general purpose operating system (i.e., resource manager) that manages the software and firmware components within the cryptographic boundary, and also manages system and operator(s) processes/thread(s), including general-purpose application software such as word processors.

A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides.

A *modifiable operational environment* refers to an operating environment that *may* be reconfigured to add/delete/modify functionality, and/or *may* include general purpose operating system capabilities (e.g., use of a computer O/S, configurable smart card O/S, or programmable firmware). Operating systems are considered to be modifiable operational environments if software/firmware components can be modified by the operator and/or the operator can load and execute software or firmware (e.g., a word processor) that was not included as part of the validation of the module.

If the operational environment is a modifiable operational environment, the operating system requirements in Section 4.6.1 shall apply. If the operational environment is a limited operational environment, the operating system requirements in Section 4.6.1 do not apply.

Documentation shall specify the operational environment for a cryptographic module, including, if applicable, the operating system employed by the module, and for Security Levels 2, 3, and 4, the Protection Profile and the CC assurance level.

4.6.1 Operating System Requirements

SECURITY LEVEL 1

The following requirements shall apply to operating systems for Security Level 1.

- For Security Level 1 only, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).
- For Security Level 1 only, the cryptographic module shall prevent access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators. Non-cryptographic processes shall not interrupt a cryptographic module during execution.
- All cryptographic software and firmware shall be installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.
- A cryptographic mechanism using an Approved integrity technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the cryptographic module. This cryptographic mechanism requirement may be incorporated as part of the Software/Firmware Integrity Test (Section 4.9.1) if an Approved authentication technique is employed for that test.

SECURITY LEVEL 2

In addition to the applicable requirements for Security Level 1, the following requirements shall also apply for Security Level 2.

- All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of
 - ❑ an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B and is evaluated at the CC evaluation assurance level EAL2, or
 - ❑ an equivalent evaluated trusted operating system.
- To protect plaintext data, cryptographic software and firmware, cryptographic keys and CSPs, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to:
 - ❑ Specify the set of roles that can *execute* stored cryptographic software and firmware.
 - ❑ Specify the set of roles that can *modify* (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), CSPs, and plaintext data.
 - ❑ Specify the set of roles that can *read* the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), CSPs, and plaintext data.
 - ❑ Specify the set of roles that can *enter* cryptographic keys and CSPs.

- The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.
- The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.
- The operating system shall provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data and CSPs.
 - The following events shall be recorded by the audit mechanism:
 - attempts to provide invalid input for crypto officer functions, and
 - the addition or deletion of an operator to/from a crypto officer role.
 - The audit mechanism shall be capable of auditing the following events:
 - operations to process audit data stored in the audit trail,
 - requests to use authentication data management mechanisms,
 - use of a security-relevant crypto officer function,
 - requests to access user authentication data associated with the cryptographic module,
 - use of an authentication mechanism (e.g., login) associated with the cryptographic module,
 - explicit requests to assume a crypto officer role, and
 - the allocation of a function to a crypto officer role.

SECURITY LEVEL 3

In addition to the applicable requirements for Security Levels 1 and 2, the following requirements shall apply for Security Level 3.

- All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of
 - an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL3 and include the following additional requirements: Trusted Path (FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1), or
 - an equivalent evaluated trusted operating system.
- All cryptographic keys and CSPs, authentication data, control inputs, and status outputs shall be communicated via a trusted mechanism (e.g., a dedicated I/O physical port or a trusted path). If a trusted path is used, the Target of Evaluation Security Functions (TSF) shall support the trusted path between the TSF and the operator when a positive TSF-to-operator connection is required. Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated from other paths.
- In addition to the audit requirements of Security Level 2, the following events shall be recorded by the audit mechanism:
 - attempts to use the trusted path function, and
 - identification of the initiator and target of a trusted path.

SECURITY LEVEL 4

In addition to the applicable requirements for Security Levels 1, 2, and 3, the following requirements shall also apply to operating systems for Security Level 4.

- All cryptographic software, cryptographic keys and CSPs, and control and status information shall be under the control of
 - ❑ an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL4, or
 - ❑ an equivalent evaluated trusted operating system.

4.7 Cryptographic Key Management

The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys, cryptographic key components, and CSPs employed by the cryptographic module. Key management includes random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization. A cryptographic module may also employ the key management mechanisms of another cryptographic module. Encrypted cryptographic keys and CSPs refer to keys and CSPs that are encrypted using an Approved algorithm or Approved security function. Cryptographic keys and CSPs encrypted using a non-Approved algorithm or proprietary algorithm or method are considered in plaintext form, within the scope of this standard

Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution. Public keys shall be protected within the cryptographic module against unauthorized modification and substitution.

Documentation shall specify all cryptographic keys, cryptographic key components, and CSPs employed by a cryptographic module.

4.7.1 Random Number Generators (RNGs)

A cryptographic module may employ random number generators (RNGs). If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the data output from the RNG shall pass the continuous random number generator test as specified in Section 4.9.2. Approved RNGs shall be subject to the cryptographic algorithm test in Section 4.9.1. Approved RNGs are listed in Annex C to this standard.

Until such time as an Approved nondeterministic RNG standard exists, nondeterministic RNGs approved for use in classified applications may be used for key generation or to seed Approved deterministic RNGs used in key generation. Commercially available nondeterministic RNGs may be used for the purpose of generating seeds for Approved deterministic RNGs. Nondeterministic RNGs shall comply with all applicable RNG requirements of this standard.

An Approved RNG shall be used for the generation of cryptographic keys used by an Approved security function. The output from a non-Approved RNG may be used 1) as input (e.g., seed, and seed key) to an Approved deterministic RNG or 2) to generate initialization vectors (IVs) for Approved security function(s). The seed and seed key shall not have the same value.

Documentation shall specify each RNG (Approved and non-Approved) employed by a cryptographic module.

4.7.2 Key Generation

A cryptographic module may generate cryptographic keys internally. Cryptographic keys generated by the cryptographic module for use by an Approved algorithm or security function shall be generated using an Approved key generation method. Approved key generation methods are listed in Annex C to this standard. If an Approved key generation method requires input from a RNG, then an Approved RNG that meets the requirements specified in Section 4.7.1 shall be used.

Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require as least as many operations as determining the value of the generated key.

If a seed key is entered during the key generation process, entry of the key shall meet the key entry requirements specified in Section 4.7.4. If intermediate key generation values are output from the cryptographic module, the values shall be output either 1) in encrypted form or 2) under split knowledge procedures.

Documentation shall specify each of the key generation methods (Approved and non-Approved) employed by a cryptographic module.

4.7.3 Key Establishment

Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually-transported key loading device), or a combination of automated and manual methods. If key establishment methods are employed by a cryptographic module, only Approved key establishment methods shall be used. Approved key establishment methods are listed in Annex D to this standard.

If, in lieu of an Approved key establishment method, a radio communications cryptographic module implements Over-The-Air-Rekeying (OTAR), it shall be implemented as specified in the TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, *Over-The-Air-Rekeying (OTAR) Protocol*, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association.

Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require at least as many operations as determining the value of the cryptographic key being transported or agreed upon.

If a *key transport* method is used, the cryptographic key being transported shall meet the key entry/output requirements of Section 4.7.4. If a *key agreement* method is used (e.g., a cryptographic key is derived from shared intermediate values), the shared values are not required to meet the key entry/output requirements of Section 4.7.4.

Documentation shall specify the key establishment methods employed by a cryptographic module.

4.7.4 Key Entry and Output

Cryptographic keys may be entered into or output from a cryptographic module. If cryptographic keys are entered into or output from a cryptographic module, the entry or output of keys shall be performed using either manual (e.g., via a keyboard) or electronic methods (e.g., smart cards/tokens, PC cards, or other electronic key loading devices).

A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.

All encrypted secret and private keys, entered into or output from a cryptographic module and used in an Approved mode of operation, shall be encrypted using an Approved algorithm. Public keys may be entered into or output from a cryptographic module in plaintext form. A cryptographic module shall associate a key (secret, private, or public) entered into or output from the module with the correct entity (i.e., person, group, or process) to which the key is assigned.

Manually-entered cryptographic keys (keys entered using manual methods) shall be verified during entry into a cryptographic module for accuracy using the manual key entry test specified in Section 4.9.2. During key entry, the manually entered values may be temporarily displayed to allow visual verification and to improve accuracy. If encrypted cryptographic keys or key components are manually entered into the cryptographic module, then the plaintext values of the cryptographic keys or key components shall not be displayed.

Documentation shall specify the key entry and output methods employed by a cryptographic module.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, secret and private keys established using *automated methods* shall be entered into and output from a cryptographic module in encrypted form. Secret and private keys established using *manual methods* may be entered into or output from a cryptographic module in plaintext form.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4:

- Secret and private keys established using *automated methods* shall be entered into and output from a cryptographic module in encrypted form.
- Secret and private keys established using *manual methods* shall be entered into or output from a cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

If split knowledge procedures are used:

- ☐ the cryptographic module shall separately authenticate the operator entering or outputting each key component,
- ☐ plaintext cryptographic key components shall be directly entered into or output from the cryptographic module (e.g., via a trusted path or directly attached cable) without traveling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed (see Section 4.2),
- ☐ at least two key components shall be required to reconstruct the original cryptographic key,
- ☐ documentation shall prove that if knowledge of n key components is required to reconstruct the original key, then knowledge of any $n-1$ key components provides no information about the original key other than the length, and
- ☐ documentation shall specify the procedures employed by a cryptographic module.

4.7.5 Key Storage

Cryptographic keys stored within a cryptographic module shall be stored either in plaintext form or encrypted form. Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators.

A cryptographic module shall associate a cryptographic key (secret, private, or public) stored within the module with the correct entity (e.g., person, group, or process) to which the key is assigned.

Documentation shall specify the key storage methods employed by a cryptographic module.

4.7.6 Key Zeroization

A cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module. Zeroization of encrypted cryptographic keys and CSPs or keys otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this standard) is not required.

Documentation shall specify the key zeroization methods employed by a cryptographic module.

4.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Cryptographic modules shall meet the following requirements for EMI/EMC. Radios are explicitly excluded from these requirements but shall meet all applicable FCC requirements.

Documentation shall include proof of conformance to EMI/EMC requirements.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, a cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4, a cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

4.9 Self-Tests

A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. *Power-up self-tests* shall be performed when the cryptographic module is powered up. *Conditional self-tests* shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other power-up or conditional self-tests in addition to the tests specified in this standard.

If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state. All data output via the data output interface shall be inhibited when an error state exists.

Documentation shall specify:

- the self-tests performed by a cryptographic module, including power-up and conditional tests,
- the error states that a cryptographic module can enter when a self-test fails, and
- the conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (i.e., this may include maintenance of the module, or returning the module to the vendor for servicing.)

4.9.1 Power-Up Tests

Power-up tests shall be performed by a cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.). The power-up tests shall be initiated automatically and shall not require operator intervention. When the power-up tests are completed, the results (i.e., indications of success or failure) shall be output via the “status output” interface. All data output via the data output interface shall be inhibited when the power-up tests are performed.

In addition to performing the power-up tests when powered up, a cryptographic module shall permit operators to initiate the tests on demand for periodic testing of the module. Resetting, rebooting, and power cycling are acceptable means for the on-demand initiation of power-up tests.

A cryptographic module shall perform the following power-up tests: cryptographic algorithm test, software/firmware integrity test, and critical functions test.

Cryptographic algorithm test. A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test shall fail.

Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below). Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Standard).

If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then:

- the known-answer test may be omitted,
- the outputs of two implementations shall be continuously compared, and
- if the outputs of two implementations are not equal, the cryptographic algorithm test shall fail.

Software/firmware integrity test. A software/firmware integrity test using an error detection code (EDC) or Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all validated software and firmware components within a cryptographic module when the module is powered up. The software/firmware integrity test is not required for any software and firmware components excluded from the security requirements of this standard (refer to

Section 4.1). If the calculated result does not equal the previously generated result, the software/firmware test shall fail.

If an EDC is used, the EDC shall be at least 16 bits in length.

Critical functions test. Other security functions critical to the secure operation of a cryptographic module shall be tested when the module is powered up as part of the power-up tests. Other critical security functions performed under specific conditions shall be tested as conditional tests.

Documentation shall specify all security functions critical to the secure operation of a cryptographic module and shall identify the applicable power-up tests and conditional tests performed by the module.

4.9.2 Conditional Tests

Conditional tests shall be performed by a cryptographic module when the conditions specified for the following tests occur: pair-wise consistency test, software/firmware load test, manual key entry test, continuous random number generator test, and bypass test.

Pair-wise consistency test (for public and private keys). If a cryptographic module generates public or private keys, then the following pair-wise consistency tests for public and private keys shall be performed:

1. If the keys are used to perform an approved key transport method, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail.
2. If the keys are used to perform the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.

Software/firmware load test. If software or firmware components can be externally loaded into a cryptographic module, then the following software/firmware load tests shall be performed:

1. An Approved authentication technique (e.g., an Approved message authentication code, digital signature algorithm, or HMAC) shall be applied to all validated software and firmware components when the components are externally loaded into a cryptographic module. The software/firmware load test is not required for any software and firmware components excluded from the security requirements of this standard (refer to Section 4.1).
2. The calculated result shall be compared with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware load test shall fail.

Manual key entry test. If cryptographic keys or key components are manually entered into a cryptographic module, then the following manual key entry tests shall be performed:

1. The cryptographic key or key components shall have an EDC applied, or shall be entered using duplicate entries.
2. If an EDC is used, the EDC shall be at least 16 bits in length.
3. If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

Continuous random number generator test. If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the module shall perform the following continuous random number generator test on each RNG that tests for failure to a constant value.

1. If each call to a RNG produces blocks of n bits (where $n > 15$), the first n -bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n -bit block to be generated. Each subsequent generation of an n -bit block shall be compared with the previously generated block. The test shall fail if any two compared n -bit blocks are equal.
2. If each call to a RNG produces fewer than 16 bits, the first n bits generated after power-up, initialization, or reset (for some $n > 15$) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n -bit sequences are equal.

Bypass test. If a cryptographic module implements a *bypass* capability where the services may be provided without cryptographic processing (e.g., transferring plaintext through the module), then the following bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext:

1. A cryptographic module shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.
2. If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services *with* cryptographic processing and some services *without* cryptographic processing, then the module shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g., an IP address source/destination table).

Documentation shall specify the mechanism or logic governing the switching procedure.

4.10 Design Assurance

Design assurance refers to the use of best practices by the vendor of a cryptographic module during the design, deployment, and operation of a cryptographic module, providing assurance that the module is properly tested, configured, delivered, installed, and developed, and that the proper operator guidance documentation is provided. Security requirements are specified for configuration management, delivery and operation, development, and guidance documents.

4.10.1 Configuration Management

Configuration management specifies the security requirements for a configuration management system implemented by a cryptographic module vendor, providing assurance that the functional requirements and specifications are realized in the implementation.

A configuration management system shall be implemented for a cryptographic module and module components within the cryptographic boundary, and for associated module documentation. Each version of each configuration item (e.g., cryptographic module, module components, user guidance, security policy, and operating system) that comprises the module and associated documentation shall be assigned and labeled with a unique identification number.

4.10.2 Delivery and Operation

Delivery and operation specifies the security requirements for the secure delivery, installation, and startup of a cryptographic module, providing assurance that the module is securely delivered to authorized operators, and is installed and initialized in a correct and secure manner.

SECURITY LEVEL 1

For Security Level 1, documentation shall specify the procedures for secure installation, initialization, and startup of a cryptographic module.

SECURITY LEVELS 2, 3, AND 4

For Security Levels 2, 3, and 4, in addition to the requirements of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators.

4.10.3 Development

Development specifies the security requirements for the representation of a cryptographic module security functionality at various levels of abstraction from the functional interface to the implementation representation. Development provides assurance that the implementation of a cryptographic module corresponds to the module security policy and functional specification.

Functional specification refers to a high-level description of the ports and interfaces visible to the operator and a high-level description of the behavior of the cryptographic module.

SECURITY LEVEL 1

The following requirements shall apply to cryptographic modules for Security Level 1.

- Documentation shall specify the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (see Section 4.1).
- If a cryptographic module contains software or firmware components, documentation shall specify the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module.
- If a cryptographic module contains hardware components, documentation shall specify the schematics and/or Hardware Description Language (HDL) listings for the hardware components.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirement shall apply to cryptographic modules for Security Level 2.

- Documentation shall specify a functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to cryptographic modules for Security Level 3.

- All software and firmware components within a cryptographic module shall be implemented using a high-level language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available.
- If HDL is used, all hardware components within a cryptographic module shall be implemented using a high-level specification language.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to cryptographic modules for Security Level 4.

- Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module security policy. The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.
- Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy.
- Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.
- For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. The preconditions and postconditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure.
- Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification.

RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES FOR ALL LEVELS

Implementation of software and firmware components within a cryptographic module using recommended development practices listed in Appendix B will facilitate the analysis of the components for conformance to the requirements in this standard and will reduce the chance of design errors.

4.10.4 Guidance Documents

Crypto officer guidance is concerned with the correct configuration, maintenance, and administration of the cryptographic module. *User guidance* describes the security functions of the cryptographic module along with instructions, guidelines, and warnings for the secure use of the module. If a cryptographic module supports a maintenance role, user/crypto officer guidance describes the physical and/or logical maintenance services for operators assuming the maintenance role.

Crypto officer guidance shall specify:

- the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the crypto officer,
- procedures on how to administer the cryptographic module in a secure manner, and
- assumptions regarding user behavior that are relevant to the secure operation of the cryptographic module.

User guidance shall specify:

- the Approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module, and
- all user responsibilities necessary for the secure operation of a cryptographic module.

4.11 Mitigation of Other Attacks

Cryptographic modules may be susceptible to other attacks for which testable security requirements were not available at the time this version of the standard was issued (e.g., power analysis, timing analysis, and/or fault induction) or the attacks were outside of the scope of the standard (e.g., TEMPEST). Susceptibility of a cryptographic module to such attacks depends on module type, implementation, and implementation environment. Such attacks may be of particular concern for cryptographic modules implemented in hostile environments (e.g., where the attackers may be the authorized operators of the module). Such types of attacks generally rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and CSPs within the cryptographic module. Brief summaries of currently known attacks are provided below.

Power Analysis: Attacks based on the analysis of power consumption can be divided into two general categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are obtained through monitoring the variations in electrical power consumption of a cryptographic module for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently values of cryptographic keys. DPA has the same goals but utilizes advanced statistical methods and/or other techniques to analyze the variations of the electrical power consumption of a cryptographic module. Cryptographic modules that utilize external power (direct current) sources appear to be at greatest risk. Methods that may reduce the overall risk of Power Analysis attacks include the use of capacitors to level the power consumption, the use of internal power sources, and the manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing.

Timing Analysis: Timing Analysis attacks rely on precisely measuring the time required by a cryptographic module to perform specific mathematical operations associated with a cryptographic algorithm or process. The timing information collected is analyzed to determine the relationship between the inputs to the module and the cryptographic keys used by the underlying algorithms or processes. The analysis of the relationship may be used to exploit the timing measurements to reveal the cryptographic key or CSPs. Timing Analysis attacks assume that the attacker has knowledge of the design of the cryptographic module. Manipulation of the individual operations of the algorithms or processes to reduce timing fluctuations during processing is one method to reduce the risk of this attack.

Fault Induction: Fault Induction attacks utilize external forces such as microwaves, temperature extremes, and voltage manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns can be used in an attempt to reverse engineer the cryptographic

module, revealing certain features and implementations of cryptographic algorithms and subsequently revealing the values of cryptographic keys. Cryptographic modules with limited physical security appear to be at greatest risk. Proper selection of physical security features may be used to reduce the risk of this attack.

TEMPEST: TEMPEST attacks involve the remote or external detection and collection of the electromagnetic signals emitted from a cryptographic module and associated equipment during processing. Such an attack can be used to obtain keystroke information, messages displayed on a video screen, and other forms of critical security information (e.g., cryptographic keys). Special shielding of all components, including network cabling, is the mechanism used to reduce the risk of such an attack. Shielding reduces and, in some cases, prevents the emission of electromagnetic signals.

If a cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the module to mitigate the attack(s). The existence and proper functioning of the security mechanisms will be validated when requirements and associated tests are developed.

APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS

The following check list summarizes the documentation requirements of this standard. All documentation shall be provided to the validation facility by the vendor of a cryptographic module.

CRYPTOGRAPHIC MODULE SPECIFICATION

- Specification of the hardware, software, and firmware components of a cryptographic module, specification of the cryptographic boundary surrounding these components, and description of the physical configuration of the module. *(Security Levels 1, 2, 3, and 4)*
- Specification of any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this standard and an explanation of the rationale for the exclusion. *(Security Levels 1, 2, 3, and 4)*
- Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics. *(Security Levels 1, 2, 3, and 4)*
- List of all security functions, both Approved and non-Approved, that are employed by a cryptographic module and specification of all modes of operation, both Approved and non-Approved. *(Security Levels 1, 2, 3, and 4)*
- Block diagram depicting all of the major hardware components of a cryptographic module and component interconnections; including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory. *(Security Levels 1, 2, 3, and 4)*
- Specification of the design of the hardware, software, and firmware components of a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.
- Specification of a cryptographic module security policy including the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor. *(Security Levels 1, 2, 3, and 4)*

CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

- Specification of the physical ports and logical interfaces of a cryptographic module and all defined input and output data paths. *(Security Levels 1, 2, 3, and 4)*

ROLES, SERVICES, AND AUTHENTICATION

- Specification of all authorized roles supported by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*

- Specification of the services, operations, or functions provided by a cryptographic module, both Approved and non-Approved. For each service, specification of the service inputs, corresponding service outputs, and the authorized role(s) in which the service can be performed. *(Security Levels 1, 2, 3, and 4)*
- Specification of any services provided by a cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.
- Specification of the authentication mechanisms supported by a cryptographic module, the types of authentication data required to implement supported authentication mechanisms, the authorized methods used to control access to the module for the first time and initialize the authentication mechanism, and the corresponding strength of the mechanisms supported by the module. *(Security Levels 2, 3, and 4)*

FINITE STATE MODEL

- Representation of a finite state model (or equivalent) using the state transition diagram and/or state transition table that specifies all operational and error states, corresponding transitions from one state to another, input events (including data inputs and control outputs) that cause transitions from one state to another, and output events (including internal module conditions, data outputs, and status outputs) resulting from transitions from one state to another. *(Security Levels 1, 2, 3, and 4)*

PHYSICAL SECURITY

- Specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are implemented. Specification of the physical security mechanisms that are employed by a module. *(Security Levels 1, 2, 3, and 4)*
- If a cryptographic module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access, specification of the maintenance access interface and how plaintext secret and private keys and CSPs are to be zeroized when the maintenance access interface is accessed. *(Security Levels 1, 2, 3, and 4)*
- Specification of the normal operating ranges of a cryptographic module. Specification of the environmental failure protection features employed by a cryptographic module or specification of the environmental failure tests performed. *(Security Level 4)*

OPERATIONAL ENVIRONMENT

- Specification of the operational environment for the cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Identification of the operating system employed by a cryptographic module, the applicable Protection Profile, and the CC assurance level. *(Security Levels 2, 3, and 4)*

CRYPTOGRAPHIC KEY MANAGEMENT

- Specification of all cryptographic keys, cryptographic key components, and CSPs employed by a cryptographic module.
- Specification of each RNG (Approved and non-Approved) employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of each of the key generation methods (Approved and non-Approved) employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*

- Specification of the key establishment methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of the key entry and output methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- If split knowledge procedures are used, proof that if knowledge of n key components is required to reconstruct the original key, then knowledge that any $n-1$ key components provides no information about the original key other than length, and specification of the split-knowledge procedures employed by a cryptographic module. *(Security Levels 3 and 4)*
- Specification of the key storage methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of the key zeroization methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4)*

ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY

- Proof of conformance to EMI/EMC requirements. *(Security Levels 1, 2, 3, and 4)*

SELF-TESTS

- Specification of the self-tests performed by a cryptographic module including power-up and conditional tests. *(Security Levels 1, 2, 3, and 4)*
- Specification of the error states that a cryptographic module can enter when a self-test fails, and the conditions and actions necessary to exit the error states and resume normal operation of a module. *(Security Levels 1, 2, 3, and 4)*
- Specification of all security functions critical to the secure operation of a cryptographic module and identification of the applicable power-up tests and conditional tests performed by the module. *(Security Levels 1, 2, 3, and 4)*
- If a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure. *(Security Levels 1, 2, 3, and 4)*

DESIGN ASSURANCE

- Specification of procedures for secure installation, generation, and start-up of a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. *(Security Level 2, 3, and 4)*
- Specification of the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (i.e., the rules of operation). *(Security Levels 1, 2, 3, and 4)*
- If a cryptographic module contains software or firmware components, specification of the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module. *(Security Levels 1, 2, 3, and 4)*

- If a cryptographic module contains hardware components, specification of the schematics and/or Hardware Description Language (HDL) listings for the hardware components. *(Security Levels 1, 2, 3, and 4)*
- Functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces. *(Security Levels 2, 3, and 4)*
- Specification of a formal model that describes the rules and characteristics of the cryptographic module security policy, using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory. *(Security Level 4)*
- Specification of a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy. *(Security Level 4)*
- Specification of an informal proof of the correspondence between the formal model and the functional specification. *(Security Level 4)*
- For each hardware, software, and firmware component, source code annotation with comments that specify (1) the preconditions required upon entry into the module component, function or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. *(Security Level 4)*
- Specification of an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification. *(Security Level 4)*
- For crypto officer guidance, specification of:
 - ❑ the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the crypto officer *(Security Levels 1, 2, 3, and 4)*,
 - ❑ procedures on how to administer the cryptographic module in a secure manner *(Security Levels 1, 2, 3, and 4)*, and
 - ❑ assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- For user guidance, specification of
 - ❑ the Approved security functions, physical ports, and logical interfaces available to the users of the cryptographic module *(Security Levels 1, 2, 3, and 4)*, and
 - ❑ all user responsibilities necessary for the secure operation of the module. *(Security Levels 1, 2, 3, and 4)*

MITIGATION OF OTHER ATTACKS

- If a cryptographic module is designed to mitigate one or more specific attacks, specification in the module's security policy of the security mechanisms employed by the cryptographic module to mitigate the attack(s). *(Security Levels 1, 2, 3, and 4)*

SECURITY POLICY

- See Appendix C. *(Security Levels 1, 2, 3, and 4)*

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

This Appendix is provided for informational purposes only and does not contain security requirements applicable to cryptographic modules within the scope of the standard.

Life-cycle software engineering recommendations (dealing with the specification, construction, verification, testing, maintenance, and documentation of software) should be followed. Software engineering practices may include documented unit testing, code reviews, explicit high-level and low-level design documents, explicit requirements and functional specifications, structure charts and data flow diagrams, function-point analysis, defect and resolution tracking, configuration management, and a documented software development process.

For all software development, both large and small, the following programming techniques are consistent with current practices and should be used to facilitate analysis of software components of a cryptographic module and to reduce chances of programming errors.

MODULAR DESIGN

- A modular design is recommended, especially for moderate to large-scale software development efforts. Each software module should have well-defined and readily understood logical interfaces.
- Software components should be constructed using the principles of data abstraction. If available, an object-oriented, high-level language that supports the construction of abstract data types should be used.
- The software should be hierarchically structured as a series of layers.

SOFTWARE MODULE/PROCEDURE INTERFACES

- Entries to a software module or procedure should be through external calls on explicitly defined interfaces.
- Each procedure should have only one entry point and at most two exit points, one for normal exits and one for error exits.
- Data should be communicated between software modules and between procedures through the use of argument lists and/or explicit return values. Global variables should not be used among procedures except where necessary for the implementation of abstract data types. Input values should be checked for range errors using assertion statements (if provided by the programming language in use).

INTERNAL CONSTRUCTION

- Each procedure should perform only a single, well-defined function.
- Control flow within a single thread of execution should be defined using only sequencing, structured programming constructs for conditionals (e.g., if-then-else or case), and structured constructs for loops (e.g., while-do or repeat-until).
- If concurrent execution is employed (e.g., via multiple threads, tasks, or processes), the software components should enforce limits on the maximum allowable degree of concurrency and should use structured synchronization constructs to control access to shared data.

- Equivalence of variables should not be used to permit multiple memory usage for conflicting purposes.
- Robust command parsing and range checking mechanisms should be implemented to guard against malformed requests, out-of-range parameters, and I/O buffer overflows.

IN-LINE DOCUMENTATION

- Each software module, procedure, and major programming construct should be documented specifying the functions performed along with a (formal or informal) specification of preconditions and postconditions.
- Each loop should be preceded by a convincing argument (as a comment) that termination is guaranteed.
- Variable names should be used in only one context within the same procedure.
- Each variable should have an associated comment identifying the purpose of the variable and noting the range of allowable values, including if the range is unrestricted.
- If concurrency is employed, the documentation should specify how limits are enforced on the maximum allowable degree of concurrency and how accesses to shared data are synchronized in order to avoid (possibly undetected) run-time errors.

ASSEMBLY LANGUAGE

The following additional programming practices should be used when the implementation is in assembly language.

- All code should be position independent except where appropriate security concerns, efficiency, or hardware constraints require position dependency.
- All register references should use symbolic register names.
- Self-modifying code should not be used.
- All procedures should be responsible for saving and restoring the contents of any register that is used within the procedure.
- Control transfer instructions should not use numeric literals.
- Each unit should contain comments describing register use in the unit.

APPENDIX C: CRYPTOGRAPHIC MODULE SECURITY POLICY

A cryptographic module security policy shall be included in the documentation provided by the vendor. The following paragraphs outline the required contents of the security policy.

C.1 Definition of Cryptographic Module Security Policy

A cryptographic module security policy shall consist of:

- a specification of the security rules, under which a cryptographic module shall operate, including the security rules derived from the requirements of the standard and the additional security rules imposed by the vendor.

The specification shall be sufficiently detailed to answer the following questions:

- What access does operator X , performing service Y while in role Z , have to security-relevant data item W for every role, service, and security-relevant data item contained in the cryptographic module?
- What physical security mechanisms are implemented to protect a cryptographic module and what actions are required to ensure that the physical security of a module is maintained?
- What security mechanisms are implemented in a cryptographic module to mitigate against attacks for which testable requirements are not defined in the standard?

C.2 Purpose of Cryptographic Module Security Policy

There are two major reasons for developing and following a precise cryptographic module security policy:

- To provide a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, satisfies a stated security policy.
- To describe to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

C.3 Specification of a Cryptographic Module Security Policy

A cryptographic module security policy shall be expressed in terms of roles, services, and cryptographic keys and CSPs. At a minimum, the following shall be specified:

- an identification and authentication (I&A) policy,
- an access control policy,
- a physical security policy, and
- a security policy for mitigation of other attacks.

C.3.1 Identification and Authentication Policy

The cryptographic module security policy shall specify an identification and authentication policy, including

- all roles (e.g., user, crypto officer, and maintenance) and associated type of authentication (e.g., identity-based, role-based, or none) and
- the authentication data required of each role or operator (e.g., password or biometric data) and the corresponding strength of the authentication mechanism.

C.3.2 Access Control Policy

The cryptographic module security policy shall specify an access control policy. The specification shall be of sufficient detail to identify the cryptographic keys and CSPs that the operator has access to while performing a service, and the type(s) of access the operator has to the parameters.

The security policy shall specify:

- all roles supported by a cryptographic module,
- all services provided by a cryptographic module,
- all cryptographic keys and CSPs employed by the cryptographic module, including
 - secret, private, and public cryptographic keys (both plaintext and encrypted),
 - authentication data such as passwords or PINs, and
 - other security-relevant information (e.g., audited events and audit data),
- for each role, the services an operator is authorized to perform within that role, and
- for each service within each role, the type(s) of access to the cryptographic keys and CSPs.

C.3.3 Physical Security Policy

The cryptographic module security policy shall specify a physical security policy, including:

- the physical security mechanisms that are implemented in a cryptographic module (e.g., tamper-evident seals, locks, tamper response and zeroization switches, and alarms) and
- the actions required by the operator(s) to ensure that physical security is maintained (e.g., periodic inspection of tamper-evident seals or testing of tamper response and zeroization switches).

C.3.4 Mitigation of Other Attacks Policy

The cryptographic module security policy shall specify a security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

C.4 Security Policy Check List Tables

The following check list tables may be used as guides to ensure the security policy is complete and contains the appropriate details:

Role	Type of Authentication	Authentication Data
...
...

Table C1. *Roles and Required Identification and Authentication*

Authentication Mechanism	Strength of Mechanism
...	...
...	...

Table C2. *Strengths of Authentication Mechanisms*

Role	Authorized Services
...	...
...	...

Table C3. *Services Authorized for Roles*

Service	Cryptographic Keys and CSPs	Type(s) of Access (e.g., RWE)
...
...

Table C4. *Access Rights within Services*

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
...
...

Table C5. *Inspection/Testing of Physical Security Mechanisms*

Other Attacks	Mitigation Mechanism	Specific Limitations
...
...

Table C6. *Mitigation of Other Attacks*

APPENDIX D: SELECTED BIBLIOGRAPHY

American Bankers Association, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998, Washington, D.C., 1998.

American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation*, ANSI X9.52-1998, Washington, D.C., 1998.

American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm*, American National Standard X9.62-1998, Washington, D.C., 1998.

Common Criteria Implementation Board (CCIB), *International Standard (IS) 15408, Common Criteria for Information Technology Security Evaluation*, Version 2, May 1998, ISO/IEC JTC 1 and Common Criteria Implementation Board.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985.

Information Technology Management Reform Act of 1996, U.S. Code, (Public Law 104-106), 10 February 1996.

Information Technology Security Evaluation Criteria (ITSEC), Harmonized Criteria of France – Germany – the Netherlands – the United Kingdom, Version 1.1, January 1991.

Keller, Sharon and Smid, Miles, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, Special Publication 800-17, Gaithersburg, MD, National Institute of Standards and Technology, February 1998.

Keller, Sharon, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, Special Publication 800-20, Gaithersburg, MD, National Institute of Standards and Technology, October 1999.

Lee, Annabelle, *Guideline for Implementing Cryptography in the Federal Government*, Special Publication 800-21, Gaithersburg, MD, National Institute of Standards and Technology, November, 1999.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.

National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards Publication 46-3, October 25, 1999.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements(DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, December 2, 1980.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January 27, 2000.

National Institute of Standards and Technology, *Digital Signature Standard Validation System (DSSVS) User's Guide*, June 20, 1997.

National Institute of Standards and Technology, *Entity Authentication Using Public Key Cryptography*, Federal Information Processing Standards Publication 196, February 18, 1997.

National Institute of Standards and Technology, *Guideline for the Use of Advanced Authentication Technology Alternatives*, Federal Information Processing Standards Publication 190, September 28, 1994.

National Institute of Standards and Technology and Communications Security Establishment, *Implementation Guidance (IG) for FIPS 140-2*, available at URL: <http://www.nist.gov/cnvp>.

National Institute of Standards and Technology, *Key Management using ANSI X9.17*, Federal Information Processing Standards Publication 171, April 27, 1992.

National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, April 17, 1995.

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-1, January 11, 1994.

Office of Management and Budget, *Security of Federal Automated Information Resources*, Appendix III to OMB Circular No. A-130, February 8, 1996.

Telecommunications Industry Association, *Over-The-Air-Rekeying (OTAR) Protocol*, New Technology Standards Project, Digital Radio Technical Standards, TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, TSB102.AACA, January 1996.

APPENDIX E: APPLICABLE INTERNET UNIFORM RESOURCE LOCATORS (URL)

Communications Security Establishment (CSE): <http://www.csc-cst.gc.ca>

Cryptographic Module Validation Program (CMVP): <http://www.nist.gov/cmvp>

NIST Information Technology Laboratory (NIST ITL): <http://www.nist.gov/itl>

NIST Security Publications including FIPS and Special Publications: <http://csrc.nist.gov/publications>

National Technical Information Service (NTIS): <http://www.ntis.gov>

National Voluntary Laboratory Accreditation Program (NVLAP): <http://ts.nist.gov/nvlap>

National Information Assurance Partnership® (NIAP): <http://niap.nist.gov/>

Validated Protection Profiles: <http://niap.nist.gov/cc-scheme/PPRegistry.html>

CHANGE NOTICES

Change Notice 1 (Superseded by Change Notice 2)

FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: 2001 October 10

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

This change notice provides a correction to the required intervals for the length of runs test indicated in Table 3 in Section 4.9.1 Power-Up Tests.

Table 3 as originally published, incorrectly specified the required intervals. The correct intervals are indicated.

Incorrect	
Length of Run	Required Interval
1	2,343 – 2,657
2	1,135 – 1,365
3	542 – 708
4	251 – 373
5	111 – 201
6+	111 – 201

Correct	
Length of Run	Required Interval
1	2,315 – 2,685
2	1,114 – 1,386
3	527 – 723
4	240 – 384
5	103 – 209
6+	103 – 209

Questions regarding this change notice may be directed to Annabelle Lee (annabelle.lee@nist.gov, 301-975-2941).

Change Notice 2

FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: 2002 December 03

TITLE: Random Number Generator Requirements

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

This change notice provides corrections to the requirements for random number generator used by cryptographic modules. These corrections involve paragraphs 4.7.1 and 4.9.1 of FIPS 140-2. Table 1 – *Summary of security requirements* has also been corrected and involves the random number generator requirements.

This change notice also provides a correction to the Table 1 – *Summary of security requirements*. The correction involves text found in the requirements of Physical Security at Security Level 4.

Finally, this change notice replaces the term “modes” used in paragraph 4.9.1 *Cryptographic algorithm test* with “cryptographic functions” which clarifies the standard.

In the corrected paragraphs and table below, the deleted text is struck out and the added text is underlined.

Change Notice 2 supersedes Change Notice 1.

The *Derived Test Requirements for FIPS 140-2* are also affected by these corrections.

Questions regarding this change notice may be directed to Annabelle Lee
(annabelle.lee@nist.gov, 301-975-2941).

4.7.1 Random Number Generators (RNGs)

A cryptographic module may employ random number generators (RNGs). If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the data output from the RNG shall pass the continuous random number generator test as specified in Section 4.9.2. ~~Depending on the security level, the data output from an Approved RNG shall pass all statistical tests for randomness as specified in Section 4.9.1.~~ Approved ~~deterministic~~ RNGs shall be subject to the cryptographic algorithm test in Section 4.9.1. Approved RNGs are listed in Annex C to this standard.

Until such time as an Approved nondeterministic RNG standard exists, nondeterministic RNGs approved for use in classified applications may be used for key generation or to seed Approved deterministic RNGs used in key generation. Commercially available nondeterministic RNGs may be used for the purpose of generating seeds for Approved deterministic RNGs. Nondeterministic RNGs shall comply with all applicable RNG requirements of this standard.

An Approved RNG shall be used for the generation of cryptographic keys used by an Approved security function. The output from a non-Approved RNG may be used 1) as input (e.g., seed, and seed key) to an

Approved deterministic RNG or 2) to generate initialization vectors (IVs) for Approved security function(s). The seed and seed key shall not have the same value.

Documentation shall specify each RNG (Approved and non-Approved) employed by a cryptographic module.

4.9.1 Power-Up Tests

Power-up tests shall be performed by a cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.). The power-up tests shall be initiated automatically and shall not require operator intervention. When the power-up tests are completed, the results (i.e., indications of success or failure) shall be output via the "status output" interface. All data output via the data output interface shall be inhibited when the power-up tests are performed.

In addition to performing the power-up tests when powered up, a cryptographic module shall permit operators to initiate the tests on demand for periodic testing of the module. Resetting, rebooting, and power cycling are acceptable means for the on-demand initiation of power-up tests.

A cryptographic module shall perform the following power-up tests: cryptographic algorithm test, software/firmware integrity test, and critical functions test.

SECURITY LEVELS 1 AND 2

~~For Security Levels 1 and 2, a cryptographic module shall perform the following power-up tests: cryptographic algorithm test, software/firmware integrity test, and critical functions test. Statistical random number generator tests may be performed by the cryptographic module but are not required at Security Levels 1 and 2.~~

SECURITY LEVEL 3

~~For Security Level 3, in addition to the tests specified for Security Levels 1 and 2, a cryptographic module shall perform all of the statistical random number tests on demand by the operator and may perform the tests when the module is powered up.~~

SECURITY LEVEL 4

~~For Security Level 4, in addition to the tests specified for Security Levels 1, 2 and 3, a cryptographic module shall also perform all of the statistical random number generator tests when the module is powered up.~~

Cryptographic algorithm test. A cryptographic algorithm test using a known answer shall be conducted for all modes cryptographic functions (e.g., encryption, decryption, authentication, and deterministic random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test shall fail.

Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below). Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Standard).

If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then:

- the known-answer test may be omitted,
- the outputs of two implementations shall be continuously compared, and
- if the outputs of two implementations are not equal, the cryptographic algorithm test shall fail.

Software/firmware integrity test. A software/firmware integrity test using an error detection code (EDC) or Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all validated software and firmware components within a cryptographic module when the module is powered up. The software/firmware integrity test is not required for any software and firmware components excluded from the security requirements of this standard (refer to Section 4.1). If the calculated result does not equal the previously generated result, the software/firmware test shall fail.

If an EDC is used, the EDC shall be at least 16 bits in length.

Critical functions test. Other security functions critical to the secure operation of a cryptographic module shall be tested when the module is powered up as part of the power-up tests. Other critical security functions performed under specific conditions shall be tested as conditional tests.

Documentation shall specify all security functions critical to the secure operation of a cryptographic module and shall identify the applicable power-up tests and conditional tests performed by the module.

~~Statistical random number generator tests. If statistical random number generator tests are required (i.e., depending on the security level), a cryptographic module employing RNGs shall perform the following statistical tests for randomness. A single bit stream of 20,000 consecutive bits of output from each RNG shall be subjected to the following four tests: monobit test, poker test, runs test, and long runs test.~~

~~The monobit test~~

~~Count the number of ones in the 20,000 bit stream. Denote this quantity by X.~~

~~The test is passed if $9,725 < X < 10,275$.~~

~~The poker test~~

~~Divide the 20,000 bit stream into 5,000 consecutive 4 bit segments. Count and store the number of occurrences of the 16 possible 4 bit values. Denote $f(i)$ as the number of each 4 bit value i , where $0 \leq i \leq 15$.~~

~~Evaluate the following:~~

$$\text{X} = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

~~The test is passed if $2.16 < X < 46.17$.~~

~~The runs test~~

A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros that is part of the 20,000 bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (≥ 1) in the sample stream should be counted and stored.

The test is passed if the runs that occur (of lengths 1 through 6) are each within the corresponding interval specified in the table below. This must hold for both the zeros and ones (i.e., all 12 counts must lie in the specified interval). For the purposes of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	Required Interval
1	2,343 — 2,657
2	1,135 — 1,365
3	542 — 708
4	251 — 373
5	111 — 201
6+	111 — 201

Table 3: *Required intervals for length of runs test*

The long runs test

A long run is defined to be a run of length 26 or more (of either zeros or ones).

On the sample of 20,000 bits, the test is passed if there are no long runs.

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope, EFP and or EFT
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15, Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, Conditional tests.			
			Statistical RNG tests—callable on-demand.	Statistical RNG tests—performed at power-up.
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs) Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available			

Table 1: Summary of security requirements

Change Notice 3

FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: 2002 December 03

TITLE: Pair-Wise Consistency Test

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

This change notice provides corrections to the requirements for pair-wise consistency test for public/private keys used for key agreement. These corrections involve paragraphs 4.9.2 of FIPS 140-2.

In the corrected paragraphs below, the deleted text is struck out and the added text is underlined.

The *Derived Test Requirements for FIPS 140-2* is also affected by these corrections.

Questions regarding this change notice may be directed to Annabelle Lee
(annabelle.lee@nist.gov, 301-975-2941).

4.9.2 Conditional Tests

Conditional tests shall be performed by a cryptographic module when the conditions specified for the following tests occur: pair-wise consistency test, software/firmware load test, manual key entry test, continuous random number generator test, and bypass test.

Pair-wise consistency test (for public and private keys). If a cryptographic module generates public or private keys, then the following pair-wise consistency tests for public and private keys shall be performed:

1. If the keys are used to perform an approved key transport method ~~or encryption~~, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail.
- ~~2. If the keys are used to perform key agreement, then the cryptographic module shall create a second, compatible key pair. The cryptographic module shall perform both sides of the key agreement algorithm and shall compare the resulting shared values. If the shared values are not equal, the test shall fail.~~
2. If the keys are used to perform the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.

Change Notice 4

FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: 2002 December 03

TITLE: Limited Operational Environment

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

This change notice provides a correction to the definition of a *Limited Operational Environment*. This correction involves paragraph 4.6 of FIPS 140-2.

In the corrected paragraph below, the deleted text is struck out and the added text is underlined.

Questions regarding this change notice may be directed to Annabelle Lee
(annabelle.lee@nist.gov, 301-975-2941).

4.6 Operational Environment

A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine ~~or~~ on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides.

