技術文件

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

總覽

本文件探討保護不在使用者能控制範圍的硬碟機資料之困難。文中將介紹可用於兩種狀況的加密硬碟機 (SED)：一種狀況是提供立即的安全刪除 (密碼清除或讓資料再也無法讀取)，另一種狀況則是當硬碟機在使用中從系統內遺失或遭竊時，可啓用自動上鎖以保護作用中的資料。文章結尾附上兩篇附錄：第一篇附錄比較 SED 與其他用於保護硬碟機資料安全的加密技術。第二篇附錄提供立即安全刪除與自動上鎖 SED 技術的詳細分析資料，說明如何在伺服器、NAS 與 SAN 陣列、虛擬化環境、RAID、JBOD 以及獨立硬碟機中使用 SED。

序言

當汰換硬碟機而必須將硬碟機從受到全面保護的資料中心移交至他人之手時，硬碟機上的資料便極可能會曝光。IT 部門常因各種因素而必須汰換硬碟機，包括：

- 因保固、維修或租約到期而退回硬碟機
- 硬碟機移除與棄置
- 將硬碟機移到其他儲存設備另作他用

幾乎所有硬碟機最後都會在資料中心與其擁有者能控制的範圍外；Seagate 預估資料中心每天會淘汰掉 50,000 台硬碟機。這些硬碟機上面都存放著公司資料，而當硬碟機離開資料中心時，大部分硬碟機上所包含的資料都還是可以讀取的。即使資料分置於 RAID 陣列中的多部硬碟機，資料也難免遭竊，因為即使是現今高容量陣列中的一般單一分置，也有成千上百的人名或身份字號可能曝光。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

硬碟機控制的困難與棄置成本

為了避免資料露洞及隨後必須依照資料隱私權法律通知客戶的相關事端，公司紛紛嘗試許多方法，要先將淘汰的硬碟機上之資料悉數刪除，以免該些硬碟機在離開公司後落入不法人士手中。目前專門針對要讓資料變成不可讀取而設計的淘汰方式，在處理上必須大量仰賴人為操作，因此容易出現技術與人為疏失。

當前的淘汰方式尚有為數眾多且種類不一的缺點：

- 覆寫硬碟機資料相當昂貴，而且會耗用好幾天寶貴的系統資源。完成後硬碟機並不會產生通知，而覆寫也無法涵蓋重新分配過的磁區，導致資料有曝光的危險。
- 消磁或直接將硬碟機毀壞都很浪費成本。由於很難判斷各硬碟機適合的消磁強度，因此硬碟機上可能殘存可讀取的資料。毀壞硬碟機則會對環境造成傷害，而且再也無法因保固或租約結束而將硬碟機退回。
- 某些公司認為，只有將硬碟機儲存在倉庫並加以控管，才是唯一安全的淘汰方式。不過事實上這個方式並不全然安全，因為人為保存且儲存了大量資料的硬碟機，很難保證不會遺失或遭竊。
- 其他公司可能選擇僱用專業的棄置服務，不過這些服務相當昂貴，而且後續還得花費協調服務以及內部報告與稽核的成本。更麻煩的是，將硬碟機運送到服務商的過程中，等於將硬碟機上的資料置於危險中。只要遺失一台硬碟機，就可能害公司為了補救資料漏洞而損失上百萬。

由於上述種種缺點，因此對於 IBM 調查發現近九成硬碟機退回 IBM 後資料仍可讀取的結果，我們並不感到意外。這彰顯出什麼問題？離開資料中心的不僅是硬碟機，還包括儲存在硬碟機上的資料。

加密

每天都有超過上千 TB 的資料因汰換老舊系統而被帶離資料中心。不過，如果那些硬碟機都能自動並徹底將資料加密，而且可立即並安全的將資料刪除呢？美國大部分的州皆已頒布資料隱私權法律，明文規定只要將資料加密，即可得到強制報告資料漏洞的豁免權。而如果資訊無誤的話，資料曝光的處理成本相當高 — 平均需要花上 6 千 6 百萬美元[1]。

效能、擴充性與複雜度的挑戰，讓 IT 部門不得不回頭去面對要求使用加密的安全性策略。此外，不熟悉金鑰管理的人會覺得加密具有風險，因為這種程序必須確保公司永遠能將資料解密。加密硬碟機可全面解決這些問題，而且讓淘汰硬碟機的加密作業變得輕鬆而且價格實惠。

我們將針對下列兩種安全性狀況加以探討：

- 不需要使用管理金鑰便可提供立即安全刪除的 SED
- 保護遭竊之作用中資料安全的自動上鎖 SED，其內建金鑰生命週期管理

1 2008 Annual Study: Cost of a Data Breach，Ponemon Institute，2009 年 2 月

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

不使用管理金鑰立即安全刪除

加密硬碟機可透過密碼清除立即將資料銷毀。一般使用 SED 時，其擁有者並不需要維護驗證金鑰 (亦稱為認證或密碼) 才能存取硬碟機上的資料。SED 會將寫入硬碟機的資料加密，並將從硬碟機讀取的資料解密，所有過程都不需要使用擁有者的驗證金鑰。

要汰換硬碟機或移作他用時，擁有者只要傳送一道指令給硬碟機來清除密碼。密碼清除將完全取代加密硬碟機內的加密金鑰，讓硬碟機再也無法將利用已刪除之金鑰所加密的資料解密 (有關安全刪除如何運作的詳細說明，請參閱附錄 A)。

加密硬碟機可大幅降低 IT 的作業費用，因為 IT 作業無需再面對硬碟機控管的難題與棄置成本。SED 政府等級的資料安全性，不但能助您符合資料隱私權規範的「豁免」情況，亦不會妨礙 IT 效率。此外，SED 還簡化了汰換程序，並保存住硬體可以退回或重新利用的價值，包括：

- 免除覆寫或銷毀硬碟機的需求
- 確保可在保固期和租約到期後退還
- 讓硬碟機可以安全無虞地移作他用

自動上鎖加密硬碟機，內建金鑰生命週期管理

使用加密硬碟機除了可以在汰換硬碟機時進行立即的安全刪除外，硬碟機擁有者也可以選擇讓同一部 SED 進入自動上鎖模式，以便在硬碟機遭竊時也能保護作用中資料的安全。不管何種規模的企業，對於監守自盜或資產遺失的重視乃與日俱增；此外某些分公司和小型企業的經理，因為缺乏強大的實體安全體制，也面臨更頻繁的外部竊盜問題。

只要硬碟機在一般使用時是由驗證金鑰所保護，就能採用 SED 自動上鎖模式。當利用此種作法來保護硬碟機的安全時，只要一不供電，硬碟機的資料加密金鑰便會上鎖。換句話說，只要 SED 一關閉或斷電，SED 會自動將硬碟機的資料上鎖。

當 SED 恢復供電後，SED 需要經過驗證才能打開鎖上的加密金鑰並讀取硬碟機上的任何資料，藉此保護遺失及內部或外部人士竊取的硬碟機。

驗證金鑰的生命週期可透過 IBM Tivoli Key Lifecycle Manager (舊稱為 Encryption Key Manager) 來管理，它是 Java 型的軟體程式，可集中產生、保護、儲存並備份驗證金鑰。這是一項統一的金鑰管理服務，可支援各形式儲存設備 (以及其他安全應用設備) 的金鑰管理需求。由於 IBM、LSI 與 Seagate 在開放式標準程序上的進展，還可支援送出給 OASIS 的金鑰管理互通性通訊協定 (Key Management Interoperability Protocol)。透過 IBM Tivoli Key Lifecycle Manager 的平台中立性，其提供一個簡單並有效的方式以管理企業內數量與日俱增的加密金鑰。

加密硬碟機的自動上鎖模式與 IBM Tivoli Key Lifecycle Manager 將於附錄 A 再深入探討。

加密硬碟機的擁有者可以先使用 SED 的僅安全刪除模式，日後再將 SED 變更為自動上鎖模式。而在執行立即安全刪除並將硬碟機移作他用之後，可以再將硬碟機改回使用僅安全刪除模式。因此一開始，硬碟機擁有者可能選擇在一般作業期間讓 SED 維持僅安全刪除模式，目的只是為了在需要時執行立即安全刪除。日後，可能因為考量到日益攀升的竊盜問題，擁有者決定以後使用硬碟機時要改成 SED 的自動上鎖模式，那麼擁有者只要簡單地建立一個覆蓋掉現有加密金鑰的驗證金鑰即可。接著，當 SED 安全地刪除資料並移作他用後，硬碟機新的擁有者可能決定往後硬碟機不要再使用自動上鎖模式，而只要使用僅安全刪除模式來確保硬碟機使用年限快到之前能安全地刪除其資料。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

僅使用加密硬碟機的立即安全刪除功能來保護汰換的硬碟機，雖然是可以提升效率的作法，不過使用 SED 的自動上鎖模式有更多好處。簡而言之，硬碟機或系統一從資料中心移除那一刻開始 (不管有沒有使用驗證)，硬碟機就已鎖上。資料中心的系統管理員不需花費心思或採取任何措施來保護該資料。如此有助於避免因硬碟機處理不當而造成漏洞，並協助保護資料安全，免受內外部竊賊的威脅。

硬碟機資料保護技術比較

沒有任何一種加密技術可以有效地保護資料對抗所有威脅。不同的威脅會使用不同的技術防護。例如，當加密硬碟機不在擁有者控制範圍內時，可協助資料抵禦威脅，不過卻無法防止資料遭受資料中心內發生的某些威脅。舉例來說，如果攻擊者取得了伺服器的存取權，而後可存取未上鎖的硬碟機，那麼攻擊者將能夠讀取來自硬碟機的純文字。因此，使用者須牢記 SED 加密技術並無法取代資料中心的存取控制，頂多只能輔助這些控制。

保護核心資料的安全並不能取代保護移動中的資料安全，而該視為一種輔助。大部分沿著檔案系統下游移動 (無論是透過乙太網路在 NAS 上或 SAN 的區塊層級上移動) 的移動中資料，實際都掌握在 IT 儲存設備系統管理員的控制之下，因此不需要考慮這些資料的安全性風險。不過針對那些不在系統管理員控制範圍內的移動中資料，最廣為大眾接受也最常用的加密方式，便是使用 IPSec 或 FC over IP，這個方法會使用短暫的階段作業加密金鑰為少量的資料加密。雖然看起來與其使用此種階段作業安全性技術，在光纖中加密以保護硬碟機上的資料似乎是更好的解決方案：不僅硬碟機上的資料受到加密保護，當資料在光纖中傳輸時也受到加密保護。不過這種作法其實有個嚴重的缺點：它不僅無法提升安全性，事實上反而降低了安全性並增加複雜性，因為這會洩漏需長久保存的加密金鑰，並洩露大量只使用單一加密金鑰所加密的密碼文字。如果需要為移動中資料加密，最好還是使用 IPSec 或 FC over IP 加密。基於以下的種種原因，硬碟機資料加密最好還是由硬碟機本身來執行。

應用程式、資料庫、OS 和檔案系統加密 (請參閱圖 1) 都是可用來對付在資料中心內形成並會對硬碟機資料造成危害之威脅 (不論是來自資料庫、檔案或系統管理員還是來自駭客) 的技術。不過由於會明顯地造成效能衰減，而且需要對加密的應用程式、資料庫、OS 或檔案系統進行非擴充性的變更，因此對特定資料以外的部份加密顯得相當不實用。系統管理員面對這樣的限制，也只能將加密保留給最機密的資料。

為了辨識並區別機密資料，系統管理員被迫仰賴資料分類；不幸的是，現已證實此程序尚無法確實辨別出所有機密資料。資料分類既困難又費力，而且很難維護，尤其是當機密資訊可以從受保護的來源複製到未受保護的目標時，更顯得窒礙難行。此類問題會導致太多未加密的機密資料寫入硬碟機，以致於硬碟機達使用年限後，這些資料仍殘存於硬碟機上。

因此，最好還是在檔案系統下游執行加密技術，以提供全磁碟加密並彌補當資料分類無法擷取出機密資料時所造成的差距。這些技術可分攤資料保管人在資料離開資料中心的控制時為資料機密性分類的責任，減輕管理工作的困難與額外的成本負擔。在光纖、RAID 硬碟機控制器 (在伺服器或儲存設備子系統控制器) 或硬碟機上加密都是可行的作法。不過應該在哪裡加密最好呢？

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

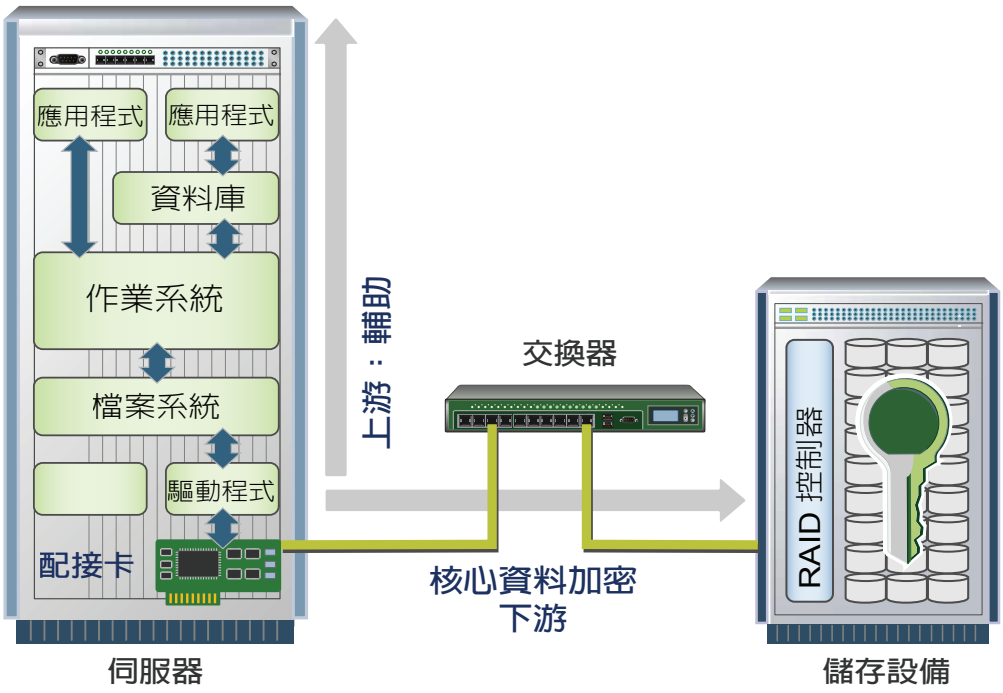

圖 1

早在多年前 Seagate 還沒開始研究硬碟機加密之前，美國國家安全局 (NSA) 就曾針對資料安全問題進行分析，結論為硬碟機是最適合加密的地方。這個結論已成為眾所周知的圭臬，而且應奉為至寶。另外，最適合在硬碟機中加密的另一個原因，乃因硬碟機正是資料存在的地方。SED 具備最優異的技術，可提供全磁碟加密、降低伺服器之直接連接儲存 SAN 與 NAS 儲存設備的總持有成本，同時提供無與倫比的優勢：

- **簡化金鑰管理**：SED 不再有追蹤或管理資料加密金鑰的需求；當用於唯安全刪除模式時，也不需要追蹤或管理驗證金鑰。
- **透過標準化的技術降低成本**：採用業界標準技術減少成本並確保在 SAN、NAS、伺服器、桌上型電腦、筆記型電腦與可攜式儲存平台上皆使用相同的技術。
- **最佳儲存效率**：不像某些加密技術，SED 可壓縮資料並刪除重複資料，將硬碟機的儲存容量提升到最大。
- **增加資料完整性**：SED 可啓用讓未來資料更完整性的「防護資訊」功能，而且不會影響到硬碟機的可靠度或保固。
- **最佳的效能與擴充性**：SED 可以硬碟機最高速度來執行，同時具備自動線性擴充能力。
- **毋需資料分類**：不再需要進行昂貴耗時的資料分類，可維持頂級效能。
- **減少重新加密**：SED 可確實減少重新產生金鑰和重新加密的需求，因為資料加密金鑰永遠不會過期。
- **卓越的安全性**：創新的 SED 機型合乎 NSA 的品質要求。因為 SED 不需要對光纖加密，因此不會暴露長久保存的密碼文字和金鑰，安全性當然不會減弱。SED 並在技術上保留了專為保護移動中資料安全所設計的沿線 (over-the-wire) 加密技術。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

加密硬碟機標準化同時也是降低採購成本的最佳保證。全球六大硬碟機製造商合力開發出最終的企業規格，並委由 Trusted Computing Group (TCG) 發佈。建立此項規格的目的是要作為開發與管理加密硬碟機的標準，以便讓不同廠商的 SED 可以互通。此互通性有助於確保更強的市場競爭力，以及降低此類解決方案建置商與一般使用者的價格。在硬碟機產業史上已屢見不鮮，統一的業界標準可提升量的規模，進而降低整體成本。而這些經濟規模有助於確認 ASIC 中的增量邏輯仍舊佔了硬碟機物料成本的一小部分(附錄 B 將提供硬碟機加密技術比較的詳細資料，並說明 SED 的優勢為何)。

結論

伺服器、SAN 與 NAS 陣列的系統管理員有充分的理由要將資料加密。加密硬碟機不僅可以滿足那些理由，而且解除了某些 IT 專業人士至今無法採用資料加密的顧慮。

加密硬碟機的優點顯而易見。立即安全刪除可減少 IT 汰換不需要使用管理金鑰之硬碟機的作業費用。此外，藉由讓硬碟機可以安全地移作他用或在服務、保固或租約到期後退還，保留住汰換之硬碟機的價值。當從系統移除硬碟機時，自動上鎖 SED 可以在發生硬碟機遭竊或遺失的情況下，自動協助保護資料的安全硬碟機可能會受損，但絕對不會導致資料暴露。

加密硬碟機還提供無與倫比的優勢。不需要追蹤或管理加密金鑰就能復原資料，因為加密金鑰從不離開硬碟機，因此可降低無法將資料解密的顧慮。只有驗證金鑰必須加以追蹤或管理，但可透過安全的方式在災難復原中心內備份、複製和鏡射驗證金鑰。而如果 SED 僅用於立即安全刪除，系統管理員甚至不需要採用及管理金鑰。

SED 加密不但自動化且清楚明瞭，可避免掉對一般儲存管理、OS、應用程式與資料庫進行變更的開銷。對於要徹底維護儲存系統，能有效地壓縮資料並刪除重複資料，省下大筆成本。此外，效能亦具備近線與自動化的規模，因為所有資料在加密時並不會降低效能，因此不需要執行費時費力又耗成本的資料分類。

加密硬碟機的規格經過標準化，具備最佳的管理能力、互通性，並兼具成本效益，而且幾乎所有大型硬碟機製造商都參與了此標準的開發。金鑰管理也變得夠具互通性，因為大部分的儲存設備廠商都承諾支援 OASIS 的金鑰管理互通性通訊協定。SED 乃專為整合到執行典型儲存升級排程的標準產品而打造。

與其他加密技術相比，安裝簡單以及硬碟機加密可提供較佳的經濟效益、效能、管理能力與安全性。這就是為什麼許多著名的分析師、系統製造商和政府機關 (例如 NSA) 強烈要求硬碟機必須具備加密功能。總結來說：SED 在改善全球伺服器、SAN 與 NAS 陣列的安全性與降低擁有權成本上的貢獻居功厥偉。

由於 SED 可降低硬碟機的汰換成本，並減少 IT 管理的困難，許多公司開始考量在安全性策略中採用 SED 所能帶來的好處。安全性策略撰寫者應考慮更新他們的策略，以具體要求未來所有的硬碟機都應該採用 SED。IBM 與 LSI 率先將加密硬碟機納入解決方案，而 Seagate 也隨即將旗下所有硬碟機產品組合全部改用 SED。其他硬碟機製造商也正積極採用 SED，相信不出多久，市面上所有硬碟機必定皆為加密硬碟機。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

附錄 A：加密硬碟機技術

嶄新推出的加密硬碟機

每部加密硬碟機 (SED) 在出廠時會隨機產生一個加密金鑰並內建於硬碟機中。SED 會主動執行全磁碟加密；當進行寫入時，純文字會輸入硬碟機，而且會在寫入之前 (使用硬碟機內建的加密金鑰) 先進行加密。執行讀取時，硬碟機上加密的資料會在離開硬碟機前進行解密。SED 在一般作業期間對系統完全透明化，運作方式就與非加密硬碟機無異。加密硬碟機會持續加密 — 不會有意外關閉的情況。

當擁有者取得硬碟機時，此內建加密金鑰會以純文字形式呈現，直到硬碟機變更為自動上鎖模式後，才會採用驗證金鑰。硬碟機會加密和解密所有寫入磁碟和從磁碟讀取的資料；不過此時並不會建立驗證金鑰，而且任何使用者皆可在磁碟上寫入或讀取純文字資料。

系統設定相當簡單。擁有者必須決定是否要使用 SED 的自動上鎖模式，或只要使用立即安全刪除功能。以下段落將個別探討每種使用狀況。

立即安全刪除技術

如果擁有者只想要在硬碟機上使用立即安全刪除，擁有者只需要簡單地開始在一般作業中使用硬碟機即可。僅安全刪除模式表示擁有者不需要驗證金鑰或密碼就可以將資料解密並讀取資料。此舉可免除因疏於管理驗證金鑰而導致資料遺失的可能性。

SED 技術大幅簡化了硬碟機的再利用與棄置作業。擁有者若希望將硬碟機移作他用，只需簡單地執行金鑰消除置換加密金鑰即可。硬碟機將刪除加密金鑰，並以隨機產生的新加密金鑰來置換。消除金鑰後，任何寫入硬碟機的資料都再也無法讀取 — 當使用新的加密金鑰為解密時，使用先前金鑰加密的資料就會變得無法辨識 (請參閱圖 2)。硬碟機將回到最初出廠時的情形，以供新的擁有者以僅安全刪除模式或自動上鎖模式來使用。

圖 2

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

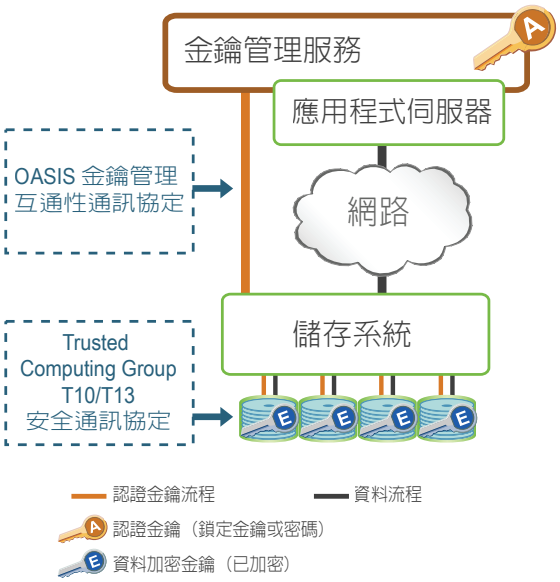

圖 3

金鑰管理與管理自動上鎖加密硬碟機

當使用 SED 自動上鎖模式時，SED 需要一個來自外部來源的驗證金鑰，才能解除鎖定硬碟機以進行讀取/寫入作業。內有自動上鎖加密硬碟機的資料中心，會使用一個儲存、管理和提供驗證金鑰的金鑰管理服務，以及將這些驗證金鑰傳送到正確硬碟機的儲存系統 (請參閱圖 3)。Seagate、IBM 和 LSI 已通力合作，將各家公司所擁有的技術整合起來，並打造完整的加密解決方案，例如 IBM System Storage DS8000 和 IBM System Storage DS5000 中便包含此一先進技術。

除了傳統的功能外，儲存系統也會定義安全的磁區群組，從金鑰管理服務取得驗證金鑰，然後將金鑰傳送到正確的硬碟機。圖 3 的橘色線代表此項作業。在這個方法中，儲存系統會讓加密功能保持對於主機、OS、資料庫和應用程式的透明化。

一旦在開機期間完成驗證後，加密會對儲存系統保持透明化，讓儲存系統可以執行一般的傳統功能。圖 3 中的深灰色線代表純文字資料的資料動向。儲存系統可壓縮資料並刪除重複資料，以利未加密資料使用。

金鑰管理服務可能會採用軟體或硬體式金鑰儲存以建立、指定和管理整個企業的相關驗證與加密金鑰。有效的金鑰管理應能與組織現有的安全性策略完美地整合，以確保服務和金鑰本身受到妥善保護，未經授權無法存取。

此外，有效的金鑰管理系統應包括備份、同步化、生命週期管理、稽核與長期長期保存。當能夠善加利用組織現有的高可用性和災難復原解決方案時，金鑰管理服務的部署就能大幅簡化。

IBM Tivoli Key Lifecycle Manager (舊稱為 Encryption Key Manager) 是 Java 型的軟體程式，它可產生、保護、儲存並維護驗證金鑰，以搭配 IBM 加密磁帶機以及內建全磁碟加密贏碟機的 IBM System Storage DS8000 一起使用。IBM Tivoli Key Lifecycle Manager 這項 Java 應用程式可在 z/OS、i5/OS、AIX、Linux、HP-UX、Sun Solaris 和 Windows 作業系統上執行，而且專門打造成可部署於企業內多個位置的分享資源，以協助確保應用程式的高可用性。

IBM Tivoli Key Lifecycle Manager 可藉由平台中立性以及能夠利用組織內最安全的伺服器平台上現有之安全性策略與高可用性環境的能力，提供一個簡單並有效的方式以管理企業內數量與日俱增的加密金鑰。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

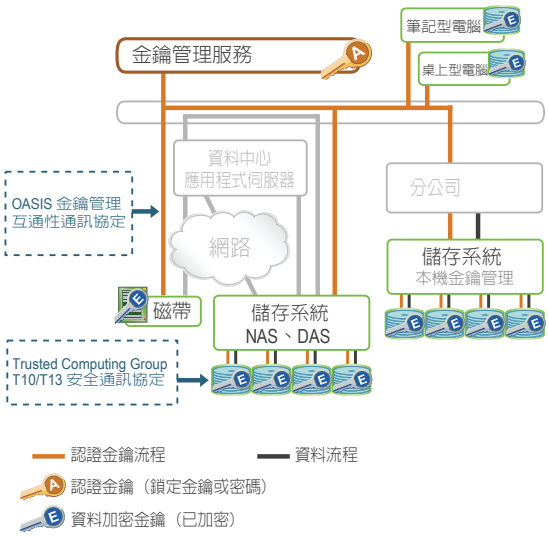

圖 4

IBM Tivoli Key Lifecycle Manager 會在使用時提供金鑰，以便將金鑰物件集中儲存於同一個安全位置，這種獨特的作法可支援多個提供金鑰的通訊協定，並管理認證以及對稱和不對稱的金鑰。使用者也可使用可自訂的圖形使用者介面 (GUI) 集中建立、匯入、散佈、備份、封存和管理這些金鑰和認證的生命週期。此外，IBM Tivoli Key Lifecycle Manager 透明化的加密作業表示金鑰是在集中的位置產生並從該處提供，且絕不會以「純文字」傳送或儲存。

最後這項技術將會運用到整個資料中心，如圖 4 所示。加密硬碟機可以運用在資料中心、分公司以及小型企業的儲存陣列、SAN、NAS 和伺服器。這是一項統一的金鑰管理服務，可支援各形式儲存設備 (以及其他安全應用設備) 的金鑰管理需求。

自動上鎖加密硬碟機技術

為了使用加密硬碟機的自動上鎖模式，硬碟機擁有者可能希望先使用 SED 的安全刪除變更加密金鑰，以讓安全性更加安心；此舉也可保護硬碟機免於在倉儲過程遭受攻擊。之後擁有者必須先輸入硬碟機外殼標籤上的 SID (安全識別碼，證明所有權) 以建立一個驗證金鑰，然後設定該驗證金鑰，以便讓硬碟機為加密金鑰進行加密。現在 SED 已進入自動上鎖模式。硬碟機正處於安全的狀態中；當硬碟機關機後將會上鎖，而再開機時需要驗證才能解除鎖定。在自動上鎖 SED 中，加密金鑰和驗證金鑰會一起運作，以便能夠存取儲存於硬碟機上的資料。

而配置成使用驗證的自動上鎖 SED，本身並不含任何被他人得悉時，會導致加密資料洩漏的秘密資訊。下面將簡單說明解鎖過程來證明此道理。解鎖過程是能讓您存取加密資料的硬碟機開機作業流程之一。硬碟機會等待提供認證 (驗證金鑰)，以確認硬碟機是由獲得授權的使用者在進行存取。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

以下說明先前已受保護之硬碟機的驗證程序步驟 (請參閱圖 5)：

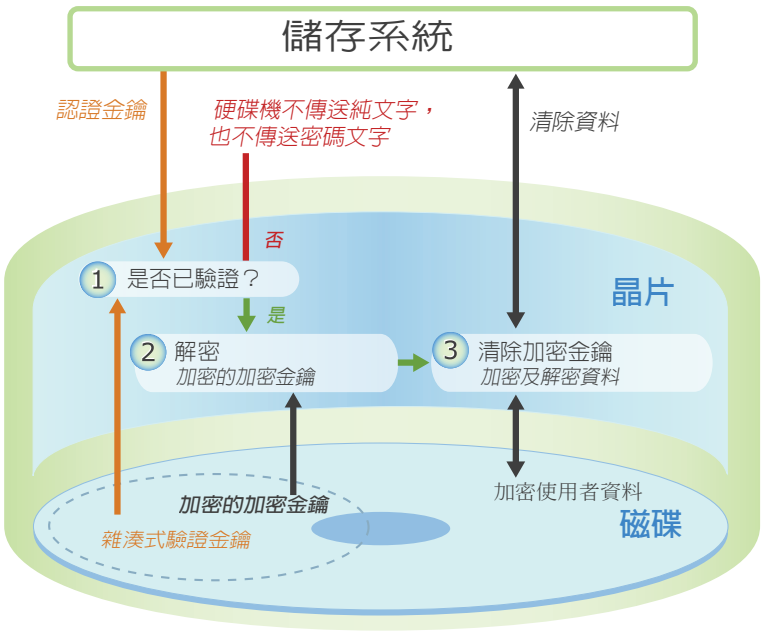

圖 5

1. 驗證

- 儲存系統從金鑰管理服務取得驗證金鑰，並將其傳送到正確的已上鎖硬碟機。
- 硬碟機會將驗證金鑰進行雜湊處理，並將結果與儲存於硬碟機安全區域的雜湊驗證金鑰加以比對。
- 如果兩個雜湊驗證金鑰的值不相符，便會中止驗證程序，且硬碟機將不允許從磁碟讀取資料。硬碟機將保持鎖定。請注意，硬碟機不會傳送出密碼文字

2. 為已加密的加密金鑰解密

- 如果兩個雜湊值相符，硬碟機會解除鎖定並使用其從儲存系統收到的驗證金鑰，為儲存於硬碟機安全區域的加密金鑰副本 (先前已使用驗證金鑰加密) 解密。一旦驗證程序順利完成後，硬碟機會在下一次關機前保持解除鎖定。請注意，此驗證程序只會在硬碟機首次開機時進行；每次進行讀取和寫入作業時，並不會再重複進行驗證。

3. 使用純文字加密金鑰加密和解密資料

- 然後，純文字加密金鑰會用於加密寫入硬碟機的資料，並為從硬碟機讀取的資料解密。
- 現在硬碟機會在資料傳輸期間以標準方式運作，而加密和解密會直接在背景進行。

一旦使用硬碟機的自動上鎖模式，只有在執行過安全刪除程序後，才能再將硬碟機改成僅安全刪除模式。如果擁有者想要汰換硬碟機或將硬碟機移作他用 (例如將硬碟機從自動上鎖模式改成僅安全刪除模式，好讓其他人也可以使用硬碟機)，那麼擁有者只要簡單地執行安全消除置換加密金鑰即可。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

附錄 B：硬碟機資料保護技術比較

沒有任何一種加密方式能全面對付核心資料的所有威脅。每一種方式都有成本、互通性、效率以及一些潛在性的問題必須考量，因此選擇要從何處加密時，必須先經過通盤考量。資料加密有許多種形式，包括：

- 主機軟體
- 加密硬體設備
- 儲存於配接卡、交換器、RAID 控制器或硬碟機上的加密 ASIC

當評估如何保護資料以及從何處對 SAN、NAS 或伺服器直接連接儲存設備上的核心資料加密時，最佳的解答就是盡量靠近儲存設備加密，而最理想的情況就是從硬碟機加密。

金鑰管理與建立互通性範例

SED 可以大幅減輕金鑰管理的責任，因為加密金鑰不會離開硬碟機，因此不需要追蹤或管理加密金鑰。此外，資料中心系統管理員不需要委付加密金鑰以維持資料復原能力，因為硬碟機本身會將加密的加密金鑰保存在硬碟機的多個位置。

只有 SED 不需委付加密金鑰，因為如果一般硬碟機遺失所有加密金鑰的副本，則硬碟機可能是故障了，導致不管在何種情況下都無法讀取資料。額外的加密金鑰會隨著資料備份自動新增，亦即每當資料鏡射到另一部加密硬碟機時便會新增，而該硬碟機將擁有其專屬的加密金鑰組。相較之下，光纖和控制器加密便凸顯出追蹤、管理和委付加密金鑰才能讓端點讀取和寫入資料的問題。

而硬體加密的重大問題則會出現在交換器或配接卡上。將加密作業與資料存放地點切割，讓解決方案變得更複雜，也更可能發生錯誤。例如，當需要在

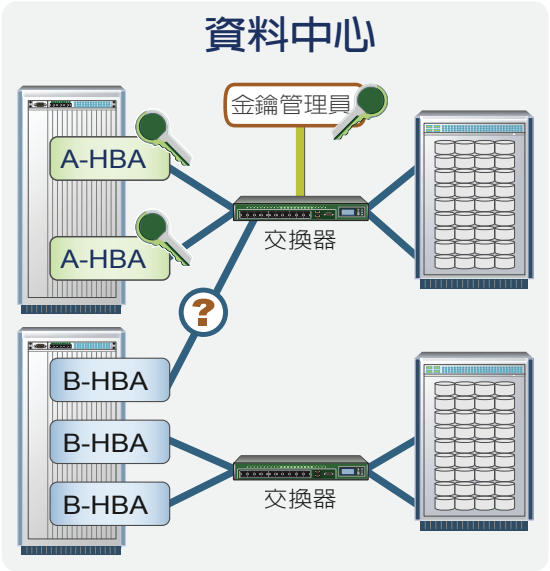

圖 6

虛擬環境中為資料加密時，不見得隨時可以取得正確的金鑰。而共用的設備越多也表示有更多實體必須共用某個特定的金鑰，而光纖上需要追蹤的金鑰動向越多，表示資料洩漏、複雜性和效能低落的問題也越大。

含有內建加密 ASIC 的配接卡則可能有互通性的問題，因為許多廠商的配接卡不支援內建加密。透過裝載配接卡之硬體加密的資料，只能在使用相同加密演算法以及存取相同金鑰管理基礎架構的相容硬體上才能讀取。例如，圖 6 中底下伺服器中的藍色 HBA (主機匯流排配接卡) 便無法讀取使用資料，因為資料是在目標中加密或是使用金鑰管理或加密交換器來驗證，而該 HBA 並無法存取金鑰管理或與加密硬體不相容。

加密硬碟機內建有管理功能，因為加密金鑰不會離開硬碟機。此外將具有不同內建加密引擎的硬碟機

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

加入現有陣列中並非難事。因此加密演算法對系統而言相當透明化，因此資料中心可以在同一陣列中使用多種加密引擎。隨著硬碟機機型變更以及較新的加密技術不斷運用於硬碟機，因此新款硬碟機可以在儲存系統中混合使用支援加密、且不會特別變更新款硬碟機較高保護層級的舊款硬碟機。

金鑰管理也變得更具互通性。由於 IBM、LSI 與 Seagate 在開放式標準程序上的進展，還可支援送出給 OASIS 的金鑰管理互通性通訊協定 (Key Management Interoperability Protocol)。

政府等級安全性

加密硬碟機提供更卓越的安全性，所以它不像某些資料安全性解決方案，在未來可能會因規格更嚴格而遭捨棄及取代。如先前提到的，SED 不需要對可能會洩漏需長期保存之密碼文字和金鑰的儲存光纖加密，因此不會減弱安全性。SED 還提供其他一個具備其他優勢的主機，使得 SED 的安全性比全磁碟加密技術更高。

美國國家安全局 (NSA) 已證明全球首創的加密硬碟機 Momentus® 5400 FDE 硬碟機擁有最高的資訊防護安全性，適合安裝於美國政府政府機關及承包商所部署的電腦中，以維護國家資訊安全。此外，此款首創機型所採用的加密演算法符合 NIST AES FIPS-197 規範。Seagate 正在努力讓未來製造的 SED 都能保持相同的高規格。

圖 7 說明如果攻擊者取得此關機時會上鎖的 SED，可能進行的攻擊。加密金鑰不會離開硬碟機；金鑰為該硬碟機專用，也是由硬碟機本身所產生。還有，硬碟機中也找不到純文字的加密金鑰 — 硬碟機中只會保存已加密的加密金鑰版本。硬碟機中並沒有純文字的密碼，只有驗證金鑰的指紋 (雜湊)。此外，硬碟機也不會使用可能遭受「冷開機」攻擊的記憶體類型。

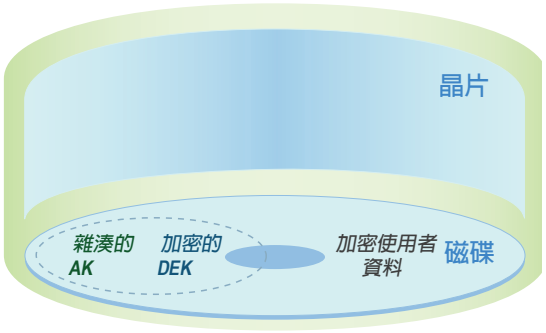

圖 7

資料和加密金鑰都會使用 AES 128 演算法加密，這是和獲得美國政府認證用以保護機密等級重要資訊的相同加密演算法。當設計硬碟機時，Seagate 假設攻擊者可能十分瞭解硬碟機的設計和硬碟機保存密祕資訊的位置。由於在硬碟機上沒有任何可以將資料解密的線索，因此，所以瞭解硬碟機設計和結構複雜的細節資訊對駭客並沒有幫助。同樣的，即使破解某部硬碟機，也不會讓攻擊者更容易破解其他硬碟機的密碼。

通常，洩漏密碼文字可能對攻擊者有所助益。例如，如果硬碟機上的檔案系統是眾所周知的架構，駭客可能會利用特定磁區固定會含有已知內容的事實，從該加密處開始進行攻擊。資料庫也幾乎是眾所周知的架構。但加密硬碟機最顯著的優勢就是 SED 本身並不會傳送密碼文字，所以此類攻將無法得逞。

SED 可以預先定義嘗試驗證失敗的次數，一旦超過這個數字便自行鎖定。相較於某些以其他方式加密的非 SED，攻擊者可以不斷嘗試驗證直到攻破為止，使得這一類硬碟機的防護如同虛設。此外，SED 具有韌體下載保護，駭客無法將修改的韌體置入硬碟機。最後，為了將可攻擊弱點減至最少，Seagate 並沒有在 SED 上設置安全性後門。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

以硬碟機最高速度來執行；不需要資料分類

加密硬碟機具備專用的引擎，可以最高介面速度執行加密。利用硬體加密，SED 的加密引擎位於控制器 ASIC 中。每個硬碟機連接埠都使用專用的加密引擎，可配合連接埠的最高速度。簡而言之，加密不會減緩系統的速度。

SED 效能也具備自動線性擴充能力。當加入更多硬碟機時，加密頻寬會等量的增加。當增加更多硬碟機到陣列中，或增加更多陣列到資料中心時，資料中心系統管理員不需要擔心平衡加密工作量的問題。

因為資料中心系統管理員可以隨心所欲為資料加密，而且不僅效能不打折，更無需進行資料分類。如先前所述，嘗試識別所有個案的機密資訊不僅費時而且費力。這些資料也很難維護及更新，尤其是當資料可以輕易地從受保護的來源複製到未受保護的目標時，更顯得窒礙難行。降低資料分類的需求，可大幅簡化資料中心的加密規劃與管理程序。

充分維護壓縮資料與刪除重複資料的效率

壓縮儲存系統的資料並刪除重複的資料，表示可以大幅降低儲存成本，不過這只有在資料並未加密時才能實現，因為當執行資料壓縮與刪除重複資料時，儲存系統只根據未加密的資料進行最佳化。有了 SED，就能充分地維護儲存系統壓縮與刪除重複資料的效率。

充分維護資料完整性的「防護資訊」標準

SED 讓未來的資料更完整，PI (防護資訊，亦稱為「資料完整性功能」) 是以 T-10 SCSI 為標準的端對端資料防護規格。在 SAS 和光纖通道系統中採用此 SCSI 通訊協定標準，可讓資料路徑中的每個元素都對資料進行審查，並確認沒有任何損害發生。此功能需使用資料的特殊附件來執行，不過如果資料在已加密的元素中傳遞，便無法執行該功能。

因為 SED 是在資料的路徑尾端進行加密 (例如，在資料儲存的硬碟機上進行加密)，所以 SED 是唯一能在整個資料路徑上支援「防護資訊」的解決方案。而當採用此項卓越的資料完整性功能時，SED 並不會影響到硬碟機的可靠度、可用性或服務能力/保固。

標準化技術降低成本

全球六大硬碟機製造商 (Fujitsu、Hitachi、Samsung、Seagate、Toshiba 與 Western Digital) 合力開發出最終的企業規格，並於最近委由 Trusted Computing Group (TCG) 發佈。建立此項規格的目的是要作為開發與管理加密硬碟機的標準，以便讓不同廠商的 SED 可以互通。此互通性有助於確保更強的市場競爭力，以及降低此類解決方案建置商與一般使用者的價格。

往後從各廠商購得的所有硬碟機，都將會是加密硬碟 (目前已有半數的廠商可在市場上供應 SED)。如此就不會再有資料漏洞的風險，當硬碟機離開擁有者控制範圍時，也不必擔心會洩漏資料了。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

依預料，加密硬碟機最後會普及於所有端點，包括下列各種設備：

- 伺服器、SAN、NAS 陣列 (不論虛擬化與否)、RAID、JBOD 或個別硬碟機
- 磁帶機
- 固態硬碟機
- 桌上型電腦硬碟機
- 筆記型電腦硬碟機
- 可攜式硬碟機

減少重新加密的需求

將驗證金鑰和加密金鑰分開，能為硬碟機擁有者帶來許多管理上的好處。由於加密金鑰本身會進行加密且不會離開硬碟機，資料中心管理員不需要定期變更加密金鑰，因此使用者也不必因基於安全考量而必須定期變更密碼。如此一來，可以減少進行大量耗費資源的解密和重新加密資料流程。

驗證金鑰可以視需要頻繁變更，而不需要重新加密。當儲存設備系統管理員離職或更換新的操作者時，他們存取儲存設備的權限可以合併，不會影響加密的資料。

相較之下，控制器和光纖型的加密則必須將資料加密金鑰在金鑰管理員間移動以保持儲存設備和加密點的安全，而且必須委付金鑰。這兩種加密的加密金鑰比起驗證金鑰已不再安全，因此必須定期重新產生金鑰，導致必須重新加密資料，連帶將效能都耗盡。

實際保護或使用階段作業加密保護移動中資料的安全

大部分沿著檔案系統下游移動 (無論是透過乙太網路在 NAS 上或 SAN 的區塊層級上移動) 的移動中資料，實際都掌握在 IT 儲存設備系統管理員的控制之下，因此不需要考慮這些資料的安全性風險。

不過針對沿著檔案系統下游移動的移動中資料，如果並未實際掌握在 IT 儲存設備系統管理員的控制之下，最廣為大眾接受也最常用為沿線傳輸之資料加密的方式，便是使用短暫的階段作業加密金鑰。單一傳輸可以使用當開始傳輸後便會立刻捨棄的階段作業金鑰來加密 — 也就是說所有後續的傳輸都會使用新的、不同的階段作業金鑰來保護資料安全。不像用來加密硬碟機儲存資料的那些長期保存金鑰，這些非常短暫的金鑰可以將資料弱點降到最低。

以下舉出三種可能使用階段作業加密的狀況：

狀況一

當從資料中心撤離光纖通道光纖連結，以及將 SAN 擴充到遠端辦公室、其他校園或遠端位置以進行災難復原時，可能會有潛在的風險產生。在以上案例中，可以使用網際網路通訊協定光纖連結 (FC over IP) 方法來應付安全性需求，並利用 IP 安全性來保護資料的安全。

狀況二

路由器和交換器使用 IPSec 之類的技術來保護 SAN，並透過 WAN 來連結 SAN。為了特別對付這一類的安全性威脅，只要交換器和路由器支援 IPSec 資料加密，就不需要主機/配接卡加密。光纖通道技術最遠只能達到 10 公里左右的距離，不過 IT 管理員必須在更遠的距離下共用、保護和移動資料，有時甚至得跨越國界。QLogic 提供的路由器和交換器，可以讓 SAN 流量透過 IP 來移動，並透過 WAN 來連結 SAN。

適用於伺服器、NAS 與 SAN 陣列的加密硬碟機

狀況三

當 IP 透過網際網路或專用線路來擴充 SAN 時，將在這個遠端連結上使用 IPSec 安全性以保護遠方有價值的移動中資料，並支援資料複製、SAN 資料設備共用，並確保備份和業務的永續性。Secure Sockets Layer (SSL) 階段作業將用於 WAN 連結 (搭配短暫的金鑰) 以協助確保連結仍舊安全，而且金鑰不會長時間暴露。

無論對光纖是否有實際的安全性防護，只要硬碟機離開擁有者的控制，便有需要保護硬碟機上的資料安全。若不使用上述的階段作業安全性技術，在光纖上加密以保護硬碟機資料，乍看是一個不錯的長期解決方案：資料不只在硬碟機上加密，當資料在光纖上傳輸時也會加密。不過這種作法其實有個嚴重的缺點：它不僅無法提升安全性，事實上反而降低了安全性並增加複雜性，因為這會洩漏需長久保存的加密金鑰，並洩露大量只使用單一加密金鑰所加密的密碼文字。

如果需要為移動中資料加密，最好還是使用 IPSec 或 FC over IP 加密。基於上節所述的種種原因，硬碟機資料加密最好還是由硬碟機本身來執行。

其他資訊

有關儲存安全性的其他資訊，請參閱 Trusted Computing Group 的網站：
www.trustedcomputinggroup.org

以及儲存網路產業協會 (Storage Networking Industry Association，SNIA) 的儲存安全產業論壇 (Storage Security Industry Forum，SSIF)：
www.snia.org/forums/ssif/knowledge_center

如需加密硬碟機白皮書、網路廣播與效能展示影片，請參閱：www.SEDSecuritySolutions.com。

美洲地區　Seagate Technology LLC　920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
亞太地區　Seagate Technology International Ltd.　7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
歐洲、中東和非洲　Seagate Technology SAS　130—136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00