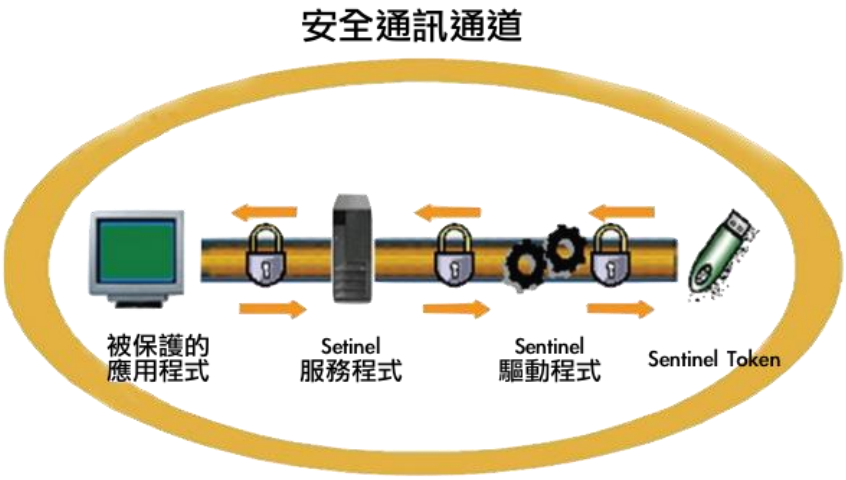
PRONEW TECHNOLOGIES
正新電腦有限公司　SafeNet-Taiwan 代理商
40857 台中市南屯路二段 290 號 7 樓之 1
TEL: 04-2473-8309　FAX: 04-2473-8311

SafeNet 白盒加密安全通道技術

【什麼是安全通訊通道？】

安全通訊通道是客戶端與 Sentinel 之間的安全通道，提供安全的私密通訊。通訊封包使用 AES 演算法加密，執行階段的金鑰是使用基於 ECC 的金鑰交換(ECKAS-DHI)產生而成。



【黑盒（傳統）密碼技術】

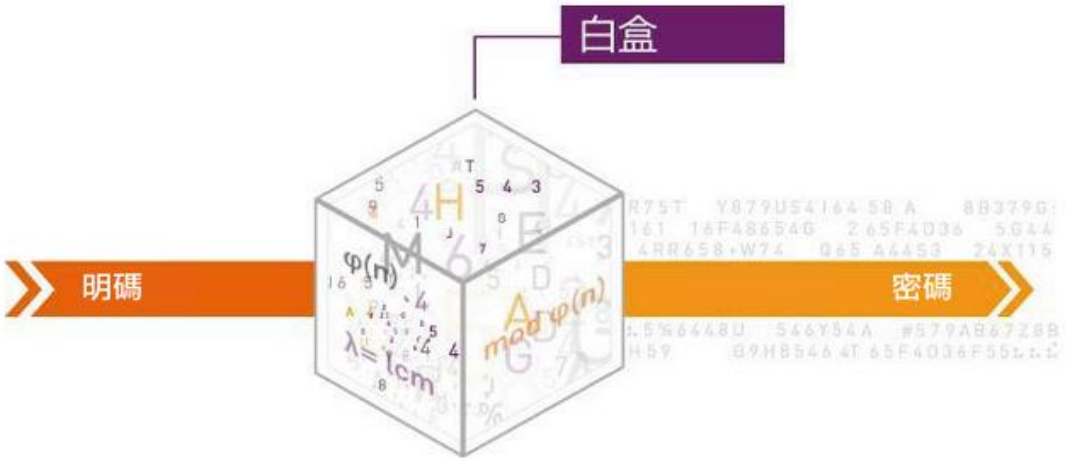
傳統狀態，黑盒方案認為攻擊者並沒有實質性地接觸到金鑰（執行加密或者解密的演算法）或者內部運作，僅能觀察到一些外部資訊或者運作。這些資訊包括系統內的明碼（輸入)或者密碼（輸出），並且認為程式碼執行以及動態加密不可被觀察。

PRONEW TECHNOLOGIES
正新電腦有限公司　SafeNet-Taiwan 代理商
40857 台中市南屯路二段 290 號 7 樓之 1
TEL: 04-2473-8309　FAX: 04-2473-8311

【白盒密碼技術的概念】

白盒密碼技術與上述傳統安全模式完全相反。與以前的執行過程相反，以前的執行過程中攻擊者僅得到一個黑盒，即在攻擊下接觸到明碼或者密碼以及加密演算法，但是認為他們是看不到內部運作的，但是白盒環境裡卻是完全可見的。

白盒密碼技術旨在保護加密演算法的軟體運行過程以防止金鑰被複製，就是在攻擊者完全控制了正在進行加密的機器，也能保持安全狀態。這在數位著作權管理(DRM)環境下最為管用。



【白盒密碼技術】

與之前描述的方案相比，白盒密碼技術假設攻擊者已經完全了解整個運作過程，在此情況下來處理面臨的更為嚴重的威脅。駭客們可以自如地觀察動態密碼運行過程（擁有範例金鑰），並且內部演演算法的詳細內容完全可見，可隨意更改。儘管白盒密碼技術的方法完全透明，但是它將密碼進行了組合使得金鑰不容易被提取。

因此可以明確的一點，在不可信賴的主機上運作黑盒模式建立的演算法是不切實際的。駭客們不會試圖僅僅利用黑盒方案的現有方法來破解密碼，而是會觀察未受保護的金鑰被使用時的執行過程，而後直接竊取。

白盒加密演算法在白盒方案中會受到保護，金鑰不會在記憶體中出現，即便是動態的也不能被取出。

因此，白盒加密想要實現選擇最合適的、最安全的密碼模型來做為阻止惡意威脅防線。

PRONEW
TECHNOLOGIES

正新電腦有限公司　SafeNet-Taiwan 代理商
40857 台中市南屯路二段 290 號 7 樓之 1
TEL: 04-2473-8309　FAX: 04-2473-8311

【白盒安全通道對比黑盒安全通道的優點】

1.完全透明化作業

2.加密秘鑰被打散，嵌入到演算法裡去，不在記憶體中出現，不會被跟蹤。駭客無法從驅動來破解加密鎖，會更安全。

SafeNet 是首家也是唯一一家將白盒密碼技術作為其軟體授權解決方案一個重要部分的廠商。

這一新技術可在任何時候保護金鑰，而不是將金鑰分成很多小部分並一次洩露其中一份。從安全角度來看，白盒密碼技術使得受保護的金鑰組駭客仍然是不可見的，因此在潛在的攻擊中該金鑰亦不會被重建。

白盒加密技術是一個附加的基本要素，它可以使開發人員保護自己的應用程式免受逆向工程、篡改、以及自動攻擊。 SafeNet 的白盒加密在軟體設計過程，直接在原始程式碼時就嵌入了額外的保護層，從而提供了一種高度的軟體保護方法。