如何使用 Linux 作業系統完成安全銷售時點情報系統設計

■作者：Donnie Garcia /
恩智浦半導體系統架構師

隨著人們使用的裝置整合越來越多智慧技術，安全交易應用也迎來了成長新機會，例如透過電器支付，還有在車輛和住家中付款。

而針對能夠接受付款的裝置，其安全性與互通性功能也需要經過嚴格檢驗。恩智浦的 Linux 讀卡機解決方案將各式各樣的技術整合為單一嵌入式系統，滿足前述的需求。Linux 作業系統是支付終端最廣泛使用的作業系統，其開放原始碼特性，為廣泛的生態系統支援方面提供了許多效益；不過 Linux 仍存在一些漏洞必須加以消除，以確保資訊安全的設計。

支付架構

支付終端的架構可以分為三種類型：

最簡單的支付裝置包括安全密碼鍵盤、連接到智慧型手機的行動 POS(mobile Point-of-Sales, mPOS) 裝置，或是電池供電的可攜式 POS 裝置。這些裝置通常採用 MCU 架構建置，例如執行速度超過 100MHz 的 Arm Cortex-M CPU。裝置內建的記憶體會根據終端裝置的功能而有不同，從 256KB 至 1M 內建快閃記憶體，到 256KB 的 SRAM 都有。

圖 1 以最完整的方式說明此種採用 MCU 架構的細節，其中包括支援的所有裝置功能。

人機介面 (HMI) 功能包含了密碼鍵盤、顯示器、狀態 LED 燈和蜂鳴器，透過有線或無線的介面、系統時鐘與電源，以及讀卡機介面，提供連線能力。讀卡器介面可包含的磁卡、接觸式卡片及非接觸式卡片，或使用近場通訊 (NFC) 的智慧型手機。

在某些情況中，POS 裝置可能需要進行大量的處理，來播放高畫質的影片和顯示廣告，此時可

圖 1：適用於支付的 MCU

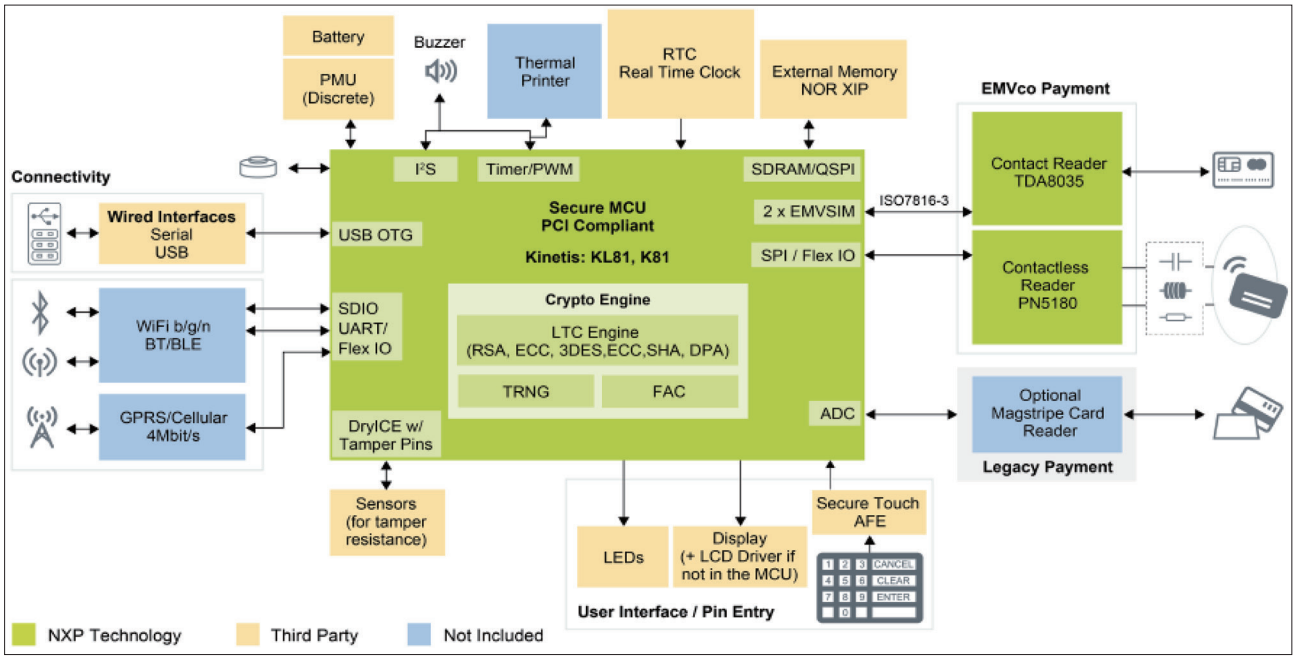
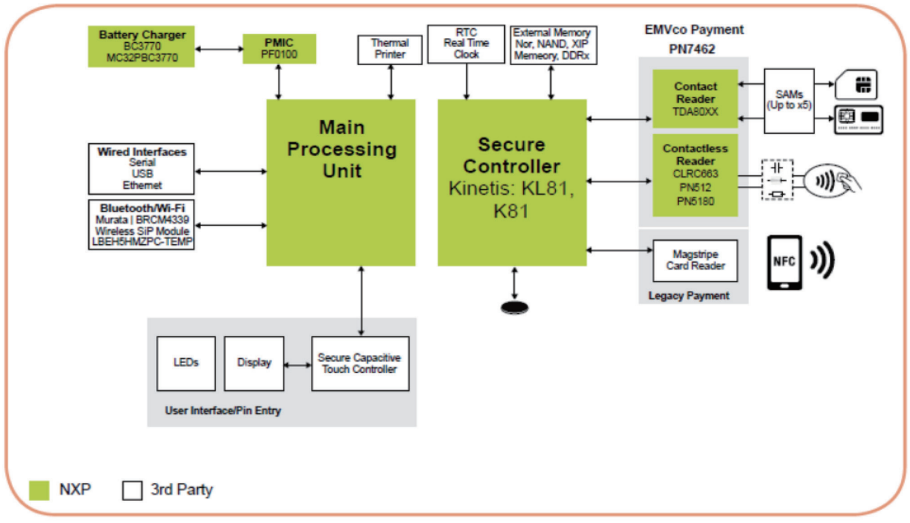


圖 2：分離式架構支付



以部署分離式架構。這主要是使用圖 1 所示的 MCU 系統架構，並加入如圖 2 中顯示的高階處理器，平板電腦或智慧型手機通常配備了此等處理器。

應用處理器通常會執行 Android，而 Android 會建置於 Linux 作業系統上。

此架構中的安全 MCU 作用為與接觸式、非接觸式讀卡機通訊，以及執行大部分功能，以支援終端裝置的安全性。高階應用處理器提供多媒體功能。RTOS 讀卡機解決方案為前述的兩種架構提供基礎，以利快速設計。

第三種架構適用於最常見的桌上型與可攜式 POS 裝置外型尺寸，採用執行 Linux 作業系統的應用處理器。如同使用微控制器的系統，此種架構所提供的功能範圍廣泛，這些功能可支援 mPOS 設計，並擴充為嵌入式系統，可使用自身的數據機完成支付交易。

運作 Linux 作業系統需配備 Arm Cortex-A CPU，這些 CPU 為終端使用者提供了更多的擴充能力；這類裝置可由商戶收單機構進行自訂配置，也可搭配既有的支付網路基礎架構使用。此種架構運用 Linux 作業系統，可提供更豐富的顯示畫面與更高的效能。

配合安全標準

由於保護消費者支付卡交易的標準限制，並非所有的 Linux 嵌入式處理器或設定都能使用於付款裝置中。支付終端必須遵循支付卡產業 PIN 交易安全標準 (PCI PTS)。根據 PCI PTS 準則，嵌入式系

統設計旨在滿足支援付款應用的終端應用程式所需的保護剖繪要求。

PCI PTS 標準將密碼鍵盤、支付卡介面與系統整合，視為需要最高安全保護的功能。恩智浦的 Linux 讀卡機解決方案實作了可信賴執行環境 (TEE)，可管理和保護敏感的使用者介面及資料。

恩智浦的低功耗 i.MX6UL 處理器搭配 Arm TrustZone，可支援四種處理器狀態，將系統內的資源進行邏輯式隔離。安全處理器狀態具備使用者模式與授權者模式；正常處理器狀態則分隔使用者 / 授權者模式。這些狀態在邏輯上彼此隔離，以減少安全區域 (Secure World) 受到攻擊。

TEE 是由應用層組成，而應用層是以安全區域使用者模式 (Secure World-User Mode) 執行 (圖表的右上方)，TEE 作業系統則是以安全區域授權者模式 (Secure World-Privileged Mode) 執行 (圖表的右下方)。TEE 作業系統中的元件，是受保護周邊裝置的周邊裝置驅動程式；這些周邊裝置包括 GPIO、LCD 等元件，以及加密保障與加速模組 (CAAM)。TEE 作業系統元件全都是在開機時載入，因此是靜態的。

TEE 作業系統元件的上層是可信賴應用程式，這些應用程式會在使用時動態載入。可信賴應用程式在邏輯上會與彼此及一般區域 (Normal World) 隔離。

在付款的使用案例中，可信賴應用程式每隔 24 小時進行自我測試、擷取使用者的 PIN 碼和讀取支付卡。如上圖所示，TEE 提供了開發安全應用程式的架構，但每個安全裝置會因提供不同服務，而需要特定功能。

為了加強安全性，恩智浦的 Linux 銷售點讀卡機解決方案，加入了安全管理員專用的可信賴應用程式。安全域間管理員 (Inter-Security Domain Manager, ISDM) 元件會學習支付卡的交易流程，並防護未預期的操作。存在於 TEE 內的可信賴應用程式包含了決策樹，此決策樹以受監督學習階段為基礎開發而成。這提供了強大的邏輯安全保護機制，是支援支付卡讀卡機等應用程式所必需的機制。

Linux 讀卡機解決方案結合了安全可靠的系統架構與認證報告，推出安全的嵌入式設計。另外，該方案也提供了元件，用以確保符合 EMVCo 標準。若要深入了解此項設計，請造訪：www.nxp.com/sln-pos-lrdr。

CTA

圖 3：使用 Arm TrustZone 以可信賴執行技術進行交易