新一代無線射頻標籤(Gen2v2)之創新與挑戰

簡宏宇
國立暨南國際大學資管系
hychien@ncnu.edu.tw

摘要

無線射頻辨識在現在生活中已被普遍應用，但也因其設計時的限制使得其市場上的發展似乎並不如預期的順利。這眾多因素包括：讀取距離、讀取穩定度、安全功能、隱私保護、及彈性化檔案管理等等。在過去無線射頻辨識的發展歷史中，不同的應用有不同的功能需求及安全需求，也因此發展出不同規格的無線射頻辨識的標準及卡片。EPC Global 為整合上訴需求及改善之前規格的弱點特發展新的 EPC Class 2 Generation 2 version 2(簡稱 Gen2v2) ，試圖以單一標準滿足多樣的功能需求；然而其功能複雜且彈性也讓非專業人員難以理解及應用。本論文旨在介紹 Gen2v2 標準、功能、指令，並討論其挑戰，希望透過這些介紹提供相關學界及業界一些參考並一起為此一新領域共同努力。

關鍵字：無線射頻辨識, Gen2, 認證, 隱私。

The Innovations and Challenges of a New RFID- EPC Class 2 Generation 2 Version 2

Abstract

Radio Frequency IDentification (RFID) has been one of the universal technologies applied in our daily life, and some weaknesses and limitations have blocked its penetration and application. These obstacles include reading distance, stead-ability of reading, security functions, privacy protection and flexible file management. Before various RFID standards and products have been ratified and produced to different market sectors. EPC Global then designs a new RFID standard- EPC Glass 2 Generation 2 Version 2 (Gen2v2 for short) - to integrate all the requirements and improve the weaknesses of existent standards. However, the new standard is powerful, flexible but quite complicated so that even the related industries find it difficult to comprehend and apply. This report tries to introduce the new standards, the commands, and the memories, and discuss the challenges. I hope this could introduce thie standard to the academia and industry.

Keywords: RFID, authentication, privacy, EPC global.

壹、前言

RFID 是無線射頻辨識(Radio Frequency Identification)，是一種無線通訊技術，經由標籤、讀取器、後端資料庫和伺服器這些系統架構所組成。RFID 的讀取器所發送的電波可依頻率區大致區分為：低頻(Low Frequency)簡稱 LF、高頻(High Frequency)簡稱 HF、超高頻(Ultra High Frequency)簡稱 UHF 和微波(Microwave)共 4 種。市場上常見的標準化的 RFID 產品包括 MIFARE、ISO 15693、EPC Gen 2 [2] 三種類型。MIFARE 系列是荷蘭商 PHILIP 公司所設計、開發的非接觸式智慧卡，其設計是遵循 ISO 14443A 規格；此類產品的特點包括高頻、具一系列不同等級的標籤記憶體保護，最常見的應用是身分辨識卡、悠遊卡等等；它的安全功能範圍極廣:從簡單的密碼或沒保護一直到橢圓密碼系統、數位簽章等等。ISO15693 標準定義了工作在 13.56Mhz 下智慧標籤和讀寫器的空氣介面及數據通信規範，符合此標準的標籤最遠識讀距離達到 2 公尺即可擁有較多的記憶體；以往常用在圖書館管理等等；安全保護只有最簡單的記憶體鎖定功能。EPC Global 設計了一系列的 RFID 標準，其中最廣為人知的是 EPC Class 2 Generation 2 Version 1 (Gen2)，它採用超高頻段(UHF) 860M～960MHz 頻寬工作，並能在十公尺距離每秒讀取多達一千個標籤，且傳輸速率較快，因此被視為物流應用的最佳技術；但讀取不穩定、隱私及安全保護弱一直是它的致命傷。

原本 EPCglobal 所推出的 Gen2 (簡稱 Gen2v1)[2]是針對物流辨識的應用所設計，但由於其大量、快速及提供較遠讀取距離等優異特性，使得 Gen2v1 已被大量用在其他產業，如零售、身份辨識、票卡、資產管理、圖書館及醫療等[16] [17][18][19][20][21]；這些應用也因此突顯出原本 Gen2v1 規格功能、安全及隱私保護上的不足[5]。因此，在 2013 年 11 月 EPCglobal 公布了新的 Gen2 規格，即 Gen2 version 2(簡稱 Gen2v2)[6]，以因應 Gen2v1 在眾多產業應用上安全及隱私保護的不足。

Gen2v2 功能包括新的安全架構及指令以支援各項隱私保護及安全機制的設計，以及新的檔案管理與存取權限等等。新的架構非常有彈性、功能強大且複雜，目前學界及產業界極缺乏相關的安全機制設計及應用設計參考；因此時至 2014 年市面上仍無相關產品，2015 年開始有少許產品宣稱符合 Gen2v2，但只支援其最簡單的指令及功能。面對此新的規格、指令及架構，再加上許多指令及功能都是選項 (標準中列為選項，廠商得自由選擇是否實作)，不僅學界及工業界不知如何發揮其功能及如何正確應用，連傳統標籤製造商也面臨不知如何組合那些功能選項生產以滿足市場需求；因此本報告旨在介紹其功能架構及指令，並討論其挑戰； 希望更多學界及工業界人士能投入此一領域以

期趕上國際上下一波的創新機會。

由於 Gen2v2 標準相當複雜，本文將著重在資安人士較關心的記憶體管理及指令部分，有興趣的讀者可以參考標準文件以了解更多細節。以下本報告組織如下：第二節介紹 Gen2v2 記憶體，第三節介紹指令，第四節介紹幾個現有商品，第五節是個人對其推廣的觀察，最後第六節是我們的結論。

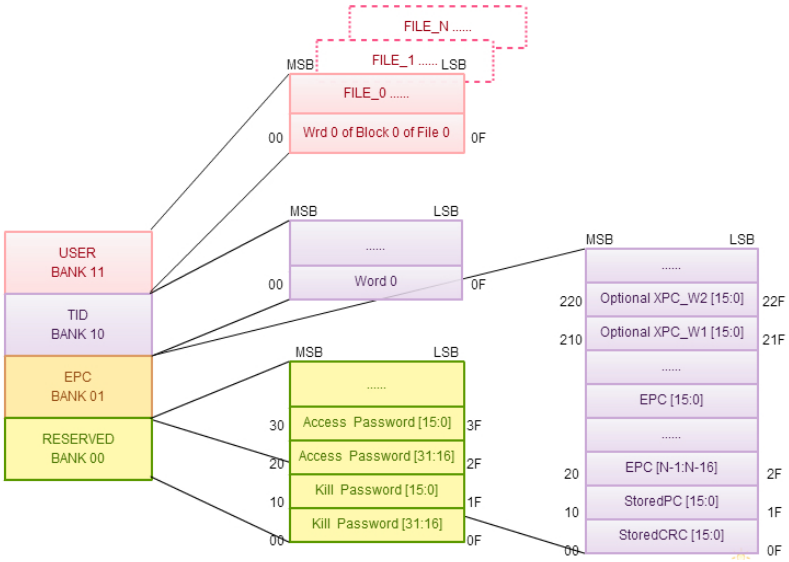

圖 1： Gen2v2 記憶體架構

貳、EPC Gen2 V2 記憶體介紹 [1][7][8][9][12]

Gen2v2 的記憶體分配在邏輯上分為四個 BANK：Reserved memory (BANK00)、EPC memory (BANK01)、TID memory (BANK10)、User memory (BANK11)。Reserved memory 存放著 kill password 及 access password，以用於對標籤執行 kill 指令、lock 指令及安全存取指令；此部分為選項，沒有實作此部分的標籤視同為 zero-value access password 或 zero-value kill password。

EPC memory 分成三個必要部分以及一個選項。三個必要部分包括 CRC-16、PC(Protocol-Control)及產品電子碼 (EPC)；選項為 第一 XPC word 及第二 XPC word。CRC-16 部分主要是當標籤 power up 或更新其 EPC 碼 (EPC code)時計算及儲存其對應之錯誤檢查碼。PC word 編碼主要是區分為 GS1 Global 計畫編碼及非 GS1 Global 計畫編碼。XPC word 是選項，其中與安全及隱私相關的部分包括: U bit 以控制是否可被追蹤，K bit 以控制標籤是否可被銷毀，NR bit 控制標籤是否可從被貼物件上移除，

H bit 代表是否貼在危險物品上等等。

TID memory 的編碼分兩類。若類別辨識碼 (class identifier)是 E0 則儲存唯一的標籤 ID，包含 8 bits 的類別碼(class-identifier value)、12 bits 的標籤製造商代碼(manufacturer identifier)及 48 bits 的標籤製造商定義的標籤序號。若類別辨識碼 (class identifier)是 E2 則依照 ISO/IEC 15963 編碼。

User memory 則是允許使用者自行定義、儲存資料和使用記憶體。User memory (BANK11)可以分割成零個、一個或數個 Files，如果只有一個 File 則為 File_0，若有數個 Files 則可支援 File_N，N >0。File-management 存取指令也是選擇性的指令，分別為 FileOpen, FileList, FileSetup, and FilePrivilege，File 數量最多可以擴充到 1023 個 files (0 to 1022)，而每個 file 可以 1023 blocks(0–1022)，每個 block 可以有 1–1024 words，所以整個 File 最多有 1.996MB 可以使用。

Gen2v2 與 Gen2v1 主要不同之處包括: (1) User memory 允許更彈性的檔案管理(可建置許多檔案以及各個檔案可以依不同的 key 來決定不同的存取權限)，(2)各個 Banks 可以設定不同的隱藏設定 (可依讀取器權限來設定可讀取段落)。

參、EPC Gen2 V2 指令介紹

Gen2v2 可簡化看成是以前所有的 RFID 標準的大整合，所以一些個別 RFID 標準的特性或長處在 Gen2v2 都看的到，尤其是長距離讀取及安全與隱私保護的加強；但因為很多功能都是選項，這使得生產及應用相對很複雜。本節我們從它的基本功能架構介紹起，再介紹其選項功能及指令。Gen2v2 延續 Gen2v1 的存取架構：原本 Gen2v1 指令旨在支援標籤讀取的三個階段：Select、Inventory、以及 Access [2][3][10][11]。Select 階段主要目的在設定那些標籤進入被選定狀態，Inventory 階段旨在取得個標籤的唯一識別碼以進行下階段的存取，最後是 Access 階段對個別標籤做存取。Gen2v1 指令包括: Select、Query、QueryRep、QueryAdjust、Req_RN、read、write、 kill, Lock、Access、BlockWrite、BlockErase；基於篇幅考量我們在此略過這些基本指令的介紹。新的 Gen2v2 延續了原先的三階段操作架構也繼承了原先的指令，但也擴充了三方面的指令：(1)安全部分- Challenge, BlockPermalock, Authenticate, AuthComm, SecureComm, Keyupdate, TagPrivilege, ReadBuffer ; (2) 隱私保護部分: Untraceabe ; (3) 檔案管理部分 : File-management: FileOpen, FileList, FilePrivilege, FileSetup。本文將針對與隱私保護及檔案讀取有關的指令做進一步介紹。

3.1 安全及隱私保護相關指令

Challenge

Challenge 指令主要用來讓讀取器指示標籤先行計算與安全套件所標示之密碼計算並儲存在暫存區以利後續的認證協定運行。Challenge 指令是一個廣播指令，可讓讀卡機一次向多個標籤發出請求，藉由標籤的回應來得知該標籤是否擁有對應密鑰，Challenge 指令至少包含 48 位元與一個 message 欄位，message 欄位用於存放認證所需要的參數。

表 1： Challenge Command (Table 6.31 of [6])

	Command	RFU	IncRepLen	Immed	CSI	Length	Message	CRC
# of bits	8	2	1	1	8	12	Variable	16
description	11010100	00	0: Omit length from reply 1: Include length in reply	0: Do not transmit result with EPC 1: Transmit result with EPC	CSI	length of message	message (depends on CSI)	CRC-16

Authenticate

Authenticate 指令是一個單一 (singlulated)指令，非廣播指令；主要功能為讓讀卡機與標籤相互進行身份認證，Authenticate 指令至少包含 64 位元與一個 message 欄位，message 欄位用於存放認證所需要的參數。

表 2： Authenticate (Table 6.58 of [6])

	Command	RFU	SenRep	IncRepLen	CSI	Length	Message	RN	CRC
# of bits	8	2	1	1	8	12	Variable	16	16
description	11010101	00	0: store 1: send	0: Omit length from reply 1: Include length in reply	CSI	length of message	message (depends on CSI)	handle	CRC-16

而 SecureComm 和 AuthComm 指令主要目的為建立溝通的通道；SecureComm 的功能為加密標籤的訊息；AuthComm 則是用來認證標籤的訊息；Keyupdate 的功能為允許讀卡機寫入或修改儲存在標籤內的金鑰。

Untraceable

Untraceable 指令可以：

1. 對標籤 EPC memory 選擇是否隱藏全部的 EPC 或是部分的 EPC；對 TID memory 可以選擇不隱藏、隱藏一部分及隱藏全部的 TID；對 User memory 可以不隱藏及隱藏全部。

2. 對沒有 Untraceable 權限的讀取器隱藏所有資料。
3. 減少標籤的讀取距離；範圍有三種，依序為 normal, toggle temporarily 及 reduced。

Untraceable 指令為選擇性指令，在 EPCglobal 的規格書中，若讀取器及標籤皆有實做 Untraceable 指令，就必須依照下表實作 (細部參數說明請參考 [6])：

表 3： Untraceable 指令

	Command	RFU	U	EPC	TID	User	Range	RN	CRC
# of bits	16	2	1	6	2	1	2	16	16
description	11100010 00000000	00	0: Deassert U 1: Assert U	MSB: 0: show memory above EPC 1: hide memory above EPC LSB: 5 bits	00: hide none 01: hide some 10: hide all 11: RFU	0: view 1: hide	00: normal 10: toggle temporarily 10: reduced 11: RFU	Handle	CRC-16

Keyupdate

Keyupdate 的功能為允許讀卡機寫入或修改儲存在標籤內的金鑰。

ReadBuffer

ReadBuffer 指令主要是為讀取器可以讀取之前標籤所計算及儲存之密碼計算以便做相關的認證(或其它密碼協定)之進行。

3.2 檔案管理相關指令

User memory (BANK 11_2)可以分割成零個、一個或數個 Files，如果只有一個 File 則為 File_0，若有數個 Files 則可支援 File_N，N >0。File-management 存取指令也是選擇性的指令，分別為 FileOpen, FileList, FileSetup, and FilePrivilege，File 數量最多可以擴充到 1023 個 files (0 to 1022)，而每個 file 可以 1023 blocks(0–1022)，每個 block 可以有 1–1024 words，所以整個 File 最多有 1.996MB 可以使用。

File-management 支援的指令包括：(1) FileOpen：開啟一個檔案，每一次只能開啟一個，開啟後的檔案才能做讀取、寫入等功能； (2) FileList：列出檔案的類型、大小、可讀取的權限；(3) FileSetup：設置檔案的類型、大小；(4) FilePrivilege：設置檔案的讀取權限。

肆、EPC Gen2V2 現有商品

雖然 Gen2v2 標準在 2013 年年底已公布，但相關商品至 2014 年底及 2015 才有少量的發表。 個人認為與其彈性及複雜的指令架構有關係。目前國際上支援 Gen2v2 產品包括幾個大 RFID 晶片設計商:MicroElectronic、 NXP 與 Impiji。

EM MicroElectronic 的 EM4423 是 NFC 與 Gen2v2 雙頻晶片，其對 Gen2v2 的支援 160-bit or 64-bit USER memory bank 與 32-bit access password[13]。

NXP 的 UCode 7 IC- SL3S1204 支援 Gen2v2 128-bit EPC 碼，沒有 User Bank，支援 32 位元 Access password 與 32 位元 Kill password [14]。

Impiji 也宣稱支援 Gen2v2，但迄今無法取得其相關產品的資料。Tagmaster 是一家 RFID 系統商，主要專精於長距離之交通工具辨識。 TagMaster 宣稱系統方案中將採用符合 NXP UCODE DNA tag IC 之讀取器 [15]。

伍、討論

從上節介紹中我們約略可見雖然 Gen2v2 功能強大可支援各式應用，但廠商產品仍只支援極少數的 Gen2v2 功能及指令。這現象與其複雜性有關析，工業界及學界對其指令的理解及掌握仍需要一段時間的努力，因而系統商須仰賴晶片製造商的支援，晶片製造商的生產需仰賴市場的反應需求及系統商的系統開發。然而使用者及系統商仍需一段時間去消化吸收這些技術。

個人認為另外一件挑戰 Gen2v2 推廣的因素是製造商如何選擇那些功能來設計及生產晶片。傳統製造商製造的晶片或產品就算是有些功能是選項，但選項都只佔規格功能的極少部分；但在 Gen2v2 規格中卻是佔極大部分，因此在生產時到底應選擇那些選項設計生產是項極大挑戰；這些關係到成本、目標應用市場、相容性等等。因此從業界、使用者及學界需要就潛力之應用去設計規畫可能的指令組合及應用[4]。當某些代表性應用被設計開發出來時，相對之指令組合產品才能被規劃與量產[4]。有了量產與相容性保證也才有助於產品價格被一般市場所接受。

EPC Global 到目前只規範了功能架構及指令，但後續的認證協定及其它密碼協議機制仍待發展、討論、及規範；從市面上產品也看出此一發展的落後，這部分亟待相關產業及學界的努力；但到目前為止，國際上只有極少數學界研究投入此一挑戰 [3][22]。依據相關新聞稿 EPC Global 預定於 2015 年底制定部分的密碼協議標準，但依據過去密碼技術研發的歷史來看，資訊的透通及透過更多人的努力才能使穩定及安全的機制能夠更快被發展出來。

陸、結論

本報告已介紹新的 Gen2v2 標準中主要功能及相關指令：記憶體規劃、安全指令、隱私保護指令、檔案管理指令；我們也粗淺的討論市場相關產品及可能面對的挑戰。由於這些新功能強大且有彈性，可以取代現有 RFID 標準以開發相關的應用及一些潛在的新應用。然而，也因為其功能選項組合頗為新穎且複雜，目前學術界及工業界尚無法掌握其功能以開發相關應用；利用相關的功能組合以設計生產合適的晶片以符合各主要應用之市場需求是另一項亟待解決的問題；最後，利用 Gen2v2 功能架構及指令設計各種密碼協議也需更多學界及工業界一起努力。

參考文獻

[1] C. Diorio, “What Capabilities Are Next for the UHF Gen2 Standard?,” *RFID Journal* , Apr. 2012. http://www.rfidjournal.net/masterPresentations/rfid_live2012/np/diorio_apr5_200_tech_infra_final.pdf

[2] EPCglobal, "EPC™ Radio-Frequency Identity Protocols," *in Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0* ed, 2006.

[3] D. W. Engels, Y. S. Kang and J. Wang, "On security with the new Gen2 RFID security framework," *IEEE International Conference on RFID (RFID)*, pp. 144-151, 2013.

[4] T.Y. Huang and H.Y. Chien, “Gen2v2-Security-and-Privacy- Features-Leveraged Application Designs”, *Ninth Asia Joint Conference on Asia JCIS*, Sep. 2014.

[5] C.-F. Lee, H.-Y. Chien, C.-S. Laih, and C.-S. Chen, "On the security of several Gen2-based protocols without modifying the standards," *Journal of the Chinese Institute of Engineers,* vol. 35, pp. 391-399, 2012.

[6] GS1, "EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID," *in Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.0 Ratified*, ed, 2013.

[7] GS1, "EPC Gen2v2 Fact Sheet," 2013.

[8] GS1. “EPC Gen 2 V2: What can it do for you?,” *RFID Journal*, 2013. http://www.rfidjournal.net/masterPresentations/rfid_live2013/np/repec_may1_220_techInfra.pdf

[9] T. INSTRUMENTS, "TI UHF Gen2 Protocol " *in Reference Guide*, 2006.
[10] Y. S. Kang, P. Dong-Jo, and D. W. Engels, "KeyQ: A Dynamic Key Establishment Method Using an RFID Anti-Collision Protocol," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 97, pp. 2662-2666, 2014.
[11] K. Krause. "UHF RFID Has Reached a Tipping Point," *Impinj*, 2014. http://rfididk.org/wp-content/uploads/2014/02/13.50-UHF-RFID-has-reached-a-tipping-point.pdf
[12] K. Mandal, X. Fan, and G. Gong, "Warbler: A Lightweight Pseudorandom Number Generator for EPC C1 Gen2 Passive RFID Tags," *Int. J. RFID Secur. Cryptogr*, vol. 2, pp. 82-91, 2013.
[13] EM Microelectronic, "Dual Frequency NFC Type 2 & EPC GEN2V2 Transponder IC," http://www.emmicroelectronic.com/sites/default/files/public/products/datasheets/4423-fs.pdf.
[14] NXP, "NXP's UCODE 7 IC-- SL3S1204," http://www.nxp.com/documents/data_sheet/SL3S1204.pdf.
[15] Tagmaster, "TagMaster supports NXP UCODE DNA TAG IC," http://www.tagmaster.com/ ?id=105&cid=4228.
[16] 韋一中, "運用無線射頻辨識系統與網際網路技術建構停車場管理之連鎖企業," *亞洲大學資訊工程學系碩士班學位論文*, pp. 1-57, 2006。
[17] 洪菁苗, "RFID 門禁及考勤系統之研究," *碩士論文, 義守大學資訊管理系研究所*, 2008。
[18] 侯進德, "行照 RFID 化之設計與開發," *暨南大學資訊管理學系學位論文*, pp. 1-125, 2014。
[19] 張忠智, "被動式 RFID 標籤應用於物流倉儲系統之安全性研究," 2009。
[20] 彭建贏, "具盤點與順架功能的 RFID 圖書管理系統," 2009。
[21] 謝長志, "RFID 應用於零售賣場作業流程之研究," *碩士論文, 國立第一科技大學行銷與流通管理研究所*, 2005。
[22] 簡宏宇, 施伯昌, "一改良之 EPCglobal Class 1 Gen2v2 標籤認證協定", *CISC 全國資安會議*,2014。