A Review of the Electronic Product Code Standards for RFID Technology

C.Bolan

School of Computer and Information Science, Edith Cowan University, Perth, Western Australia
e-mail: c.bolan@ecu.edu.au

Abstract

The Electronic Product Code (EPC) standards are on their way to becoming the defacto standards for a majority of RFID tags and applications. This paper reviews the applicable standards governing the usage and operational modes of EPC Class One Generation One and EPC Class One Generation Two RFID tags. The standards are compared and critiqued with attention to the secure operation of the technology.

Keywords

RFID, Security, Standards, Electronic Product Code

1. Introduction

Radio Frequency Identification (RFID) technology has been around for some time now and is now showing steadily growing market penetration with around a 60% overall growth in the last year (Commission of the European Communities, 2007). Such adoption promises both monetary and procedural benefits in areas such as stock ordering, delivery, inventory and general item tracking.

As many of the aforementioned operations may straddle multiple independent companies within a supply chain, it made sense for a standard to be created to govern the usage and operation of RFID technology in this area (Bolan, 2005, p.1). This need was eventually addressed by EPCglobal (formerly the Auto-ID Centre) who developed a set of Electronic Product Code standards (EPCglobal, 2005) which built upon the existing International Standard Organization (ISO) operational standards for RFID technology (Alien Technology, 2005, p.6).

"*The Electronic Product Code is an identification scheme for universally identifying physical objects via Radio Frequency Identification tags and other means*" (EPCglobal, 2005, p.6). While Juels (2004, p.138) states that "*the aim of EPCglobal is to see RFID tags supplant barcodes*", according to EPCglobal (2005b, p.11) their explicit aims were:

- "*To facilitate the exchange of information and physical objects between trading partners.*"

- "*To foster the existence of a competitive marketplace for system components.*"

- "*To encourage innovation.*"

In addition, while not explicitly focused on security the standards also purport to (EPCglobal, 2005c, p.12):

- Promote a secure environment for the use of RFID systems, through either built in security features or recommending 'best practice'.

- Protect both individual and organisational privacy.

To facilitate these goals, several interrelated standards have been created and combined with existing standards (such as the ISO's) in order to implement the 'EPCglobal Architecture' (EPCglobal, 2005c). This architecture (detailed in figure 1) demonstrates how proprietary technology can use different EPC standards to allow interoperation and a global supply chain.

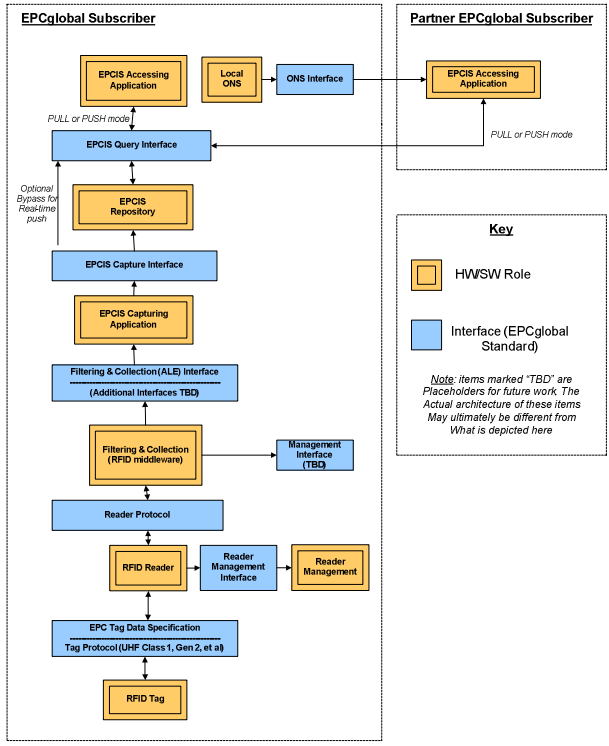

Figure 1: EPCglobal Architectural Framework (EPCglobal, 2005c, p.34)

The EPC tag data standard specifies the format of an EPC (or EPC Identifier) that allows the unique identification of a tagged object (EPCglobal, 2005a). Additionally,

the standard allows for the inclusion of user defined data, specifying the length and position of such data. To allow for adoption of the standard by various industries the EPC Identifier incorporates existing coding schemes (Domain Identifiers) and only specifies new schemes where necessary (ibid). Thus, the EPC tag data standard represents a 'family' of complementary schemes that still allows for unique identification across all possible EPC-compliant tags. The generic model of the standard is detailed in figure 2 below.

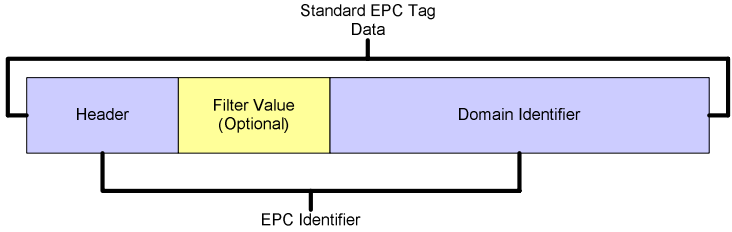

Figure 2: Overview of the EPC Tag Data standard (EPCglobal, 2005a, p. 9)

2. EPC Classes versus Generations

The EPC Tag Class Structure while simple, is often misunderstood with many authors confusing the distinction between 'Class' and 'Generation', often resulting in the incorrect assumption that Gen Two tags are in fact Class Two tags. In the EPC structure a 'Class' is distinguished by the basic functionality of the tag, for example passive versus active. The breakdown of EPC Classes is given in table 1 below.

Class 5	Class 5 tags are essentially readers. They can power other classes (1, 2 and 3) as well as communicate with class 4 and be able to communicate with each other wirelessly
Class 4	Class 4 tags are active tags. They are capable of broadband peer-to-peer communication with other active tags in the same frequency band and with readers
Class 3	Class 3 tags are semi-passive RFID tags. They may support broadband communication
Class 2	Class 2 tags are passive tags with additional functionality like memory or encryption.
Class 0 / Class 1	Class 1 / Class 0 tags are read-only passive identity tags.

Table 1: EPC Tag Classes (Adapted from GAOTek, 2006)

The 'Generation' of a tag occurs within an individual class and refers to the major release version of the specification to which a tag is compatible with.

3. Generation One versus Generation Two

The EPC Class One Generation One standard was ratified in 2004, the major feature of this standard was the write once/multiple read limitation of the tags (Alien Technology, 2005). However, ignoring this distinction, most modern compatible tags

actually allow multiple writes and reads. Generation one tags were designed to operate in the 860 MHz – 930MHz spectrum, which limits the allowable distribution of these tags due to differing telecommunication zones. The memory capacity was set at either 64 or 96 bits due in part to limits in technology and partially to keep the costs of individual tags to a minimum (Alien Technology, 2005).

As a by-product of the memory limitations, the standard only allows for two 8bit passwords (Symbol Technology, 2006). The first password is used to 'lock' the tag to protect from unauthorised writes and the second was set to control access to the 'Kill' functionality of the tags. As the possible number of passwords would only be 256 a delay between attempts of 10 seconds was added. However, due to the limitations of the technology and the effect of unresponsive tags on inventory based systems, no lockout after a given number of attempts was added (Bolan, 2007).

Another limitation of the standards was the fixed speed of communication signals, in order to allow for the widest range of conditions (e.g. noisy environments) a speed of 140kbits/sec was selected (Zebra Technologies, 2005). The read rate for the generation two standard was set to 460Tags/sec in the US, and 150Tags/sec in the EU (Symbol Technologies, 2005). The range of frequency is fairly different globally and this is the reason that EPCGlobal came up with standards to suite the environment continuum. It is vital to remember that these figures are theoretical, and as mentioned above the results are dependant on the environment and air traffic.

Due to the sudden increase in RFID usage and the rate in which the technology was improving the second generation was proposed in the same year as the generation one standards were ratified (Geary, 2005). This lead to confusion amongst potential adopters, as many wondered if they should purchase the available Generation One technology or wait for the second generation hardware to be made available. EPC addressed this issue by claiming that Generation One equipment would be accessible by Generation Two tags with the correct software (Alien Technology, 2005).

The obvious benefit of the generation two standards was in the area of available memory, with the Gen 2 tags allowing an accessible memory of up to 256 bits (Zebra Technologies, 2005). Beyond this both password lengths were extended from the eight bits of generation one to thirty two bits. The change increases the possible password combinations from the 256 in Generation One, up to 4,294,967,296 which significantly effects the time it would take to brute force the password on a tag. Also, Generation two tags are designed to work in the spectrum of 860 MHz – 960 MHz (Zebra Technologies, 2005). The addition of an extra 30 MHz to the tags operation frequency decreases the likelihood of the 10 channels being flooded causing tag communication difficulties. A further improvement was the increase in the size of the 96bit item ID to a 512bit version in generation two, along with the allowance for unlimited user memory in anticipation of future class 2 and class 3 improvements.

The reader operations for generation 2 are fairly similar to that of a generation 1 tags. Both use frequency hopping as well as listen before talk operations. Nevertheless, generation two tags have an additional dense reader mode. Dense reader mode was specifically designed for enterprise deployment (such as a warehouse or distribution centre) with many readers. The mode offers a communication function that claims to

practically eliminate usual interference associated with a large number of readers communicating with their concurrent tag population resulting in a maximum overall system stability, and reliability (Symbol Technologies, 2005). A summary of the two generations is given below in table 2.

Feature	**Class 1 Gen 1**	**Class 1 Gen 2**
Write Speed (for 96bit EPC)	3 tags/sec Rewritable many times	5 tags/sec minimum Rewritable many times
Tag Data Verification	16-bit CRC for reads	16-bit CRC for reads and writes
Multiple Reader Operation	Frequency Hopping (US FCC) Listen Before Talk (EU CEPT)	Frequency Hopping (US FCC) Listen Before Talk (EU CEPT) Dense Reader Mode Four Reader 'Sessions' allowing parallel communication by multiple readers with one tag.
Security	8-bit kill password, with lockout after incorrect queries	32-bit lock and kill passwords Option for handle based communication
Extensibility	Up to 96 bit item ID	Up to 512 bit item ID Unlimited user memory Anticipates class 2 and 3 systems.
Frequency	860MHz - 930MHz	860Mhz - 960MHz
Memory Capacity	64 or 96 Bits	96 to 256 Bits
Field Programmable	YES	YES
Re-programmable	YES	YES
Field Killable	YES	YES
Communication	140Kbits/sec	640Kbits/sec
Reads	460Tags/sec	1700Tags/sec
Reads (European Union)	150Tags/sec	460Tags/sec

Table 2: Comparison of EPC Generation One and Two

4. Documented Attacks against EPC Tags

4.1. Brute Force KILL Attack

The EPC Class 1 standard (EPCGlobal, 2005a, p.58) specifies "Interrogators and Tags shall implement the Kill command" and further that the successful usage of the command will "permanently disable a tag". The actual 'KILL' instruction consists of eight bits (11000100) and is standard to all compliant tags, however the instruction is actually part of an overall command illustrated in figure 3.

	Command	Password	RFU	RN	CRC-16
# of bits	8	16	3	16	16
description	11000100	(½ kill password) ⊗ RN16	000_2	handle	

Figure 3: The EPC 'KILL' Command (EPCglobal, 2005a, p.59)

It was documented by researchers at ECU that given the short key space of the document KILL password the time taken to brute force the entire range of possible KILL commands would be insignificant compared to the damage that such an attack would produce.

4.2. Lazarus Effect

In investigation of RFID systems (Bolan, 2006) it was found that the successful running of a KILL command did not actually cease the functioning of an RFID tag. Once a KILL command had been successfully the Tag overwrites the Tag ID, CRC, Kill code and lock bits with 0 padded values. The next time a Tag is 'pinged' by an Interrogator the tag responds with its zeroed Tag ID and the zeroed CRC value. As the CRC value does not match the calculated value for the Tag ID the Interrogator effectively ignores the response and thus the tag is in essence 'Killed'. This finding seems to go against the spirit of the standards aforementioned claim that a Tag that has been 'Killed' will "render itself silent and shall not respond to an Interrogator thereafter" (EPCglobal, 2005a, p.58). Given this finding it has subsequently been discovered that a tag may be resurrected by the re-initialisation of the ID, CRC, Kill code and lock bits (Bolan, 2006).

4.3. Response Flooding

The 'Blocker Tag' proposed by Juels *et al*. (2003) simulates the responses of the full range of unique serial identification numbers. The tag requires two antennas and responds to every request from the transponder forcing the 'tree walking algorithm' to recurse all nodes within the tree (*ibid*). As the usual size of the tree would be around 2^{64} nodes in even the most basic RFID system, the transponder would be unlikely to finish all nodes before stalling from an overload (most readers are designed to allow around 200 collisions only).
If the transponder was able to traverse the entire tree, it would return with the assumption that every possible node had been detected and it would be impossible to determine real responses from those of the blocker tag. Such an approach may not currently violate any legislation as the functionality of the blocker is superficially identical to that of any normal RFID tag. While this technique was initially proposed as an additional security method only affecting RFID 'tags' within a certain identification range, with minimal modification it has a large number of malicious uses. By expanding the effective tag identification range of the blocker tag, the blocker would by nature be malicious blocking all tags within broadcast range.

5. Conclusion

From the above discussion it is very clear that the second generation of the EPC Class One tag offers significant improvements over the initial generation. Yet, despite the obvious advantages of Gen 2 technology, Gen One equipment and tags are still being manufactured and sold by vendors. While this may be attributable to legacy installations the backwards compatibility of Gen 2 hardware along with the increased functionality and security should easily offset the cost of upgrades. However until the drivers of the technology such as Wal-Mart mandate the usage of Gen 2 technology both versions are likely to remain.

Some analysts predict that should generation two tags become the defacto standard that this will reduce the prices of the tags by as much as 80 percent. This will of course require the adoption of the standard across all major countries including China, who have been reluctant in recognising EPC Global standards. This may stem from the World Trade Organisations refusal to recognise EPC Global as a valid international standards body instead focussing on the International Standards Organisations (ISO) standards. This may have a flow on effect with Wal-mart, a major implementer and driver of RFID technology, purchasing around 70% of its merchandise from China (ibid). Thus the take up of Generation Two technology may be bypassed for an alternative standard.

If Gen 2 does become the default standard amongst retailers the security concerns raised by this paper will be of real concern. The lack of protection from the proven basic attacks listed in this paper show that any installation based on the standard will require additional protection. Failure to provide such protection allows for a substantial risk of attack and resultant financial losses.

6. References

Alien Technologies, (2005), "EPCGlobal Class 1 Gen 2 RFID Specification", Canada.

Bolan, C., (2005), "RFID - Evaluation of Tag Security Schemes", *6th Australian Information Warfare & Security Conference*, Geelong, Victoria.

Bolan, C., (2006), "The Lazerus Effect: Ressurecting Killed RFID Tags", *4th Australian Information Security and Management Conference*, Perth, Western Australia.

Bolan, C., (2007), "Radio Frequency Identification: a review of low cost tag security proposals", *International Journal of Information and Computer Security*, 1(4), 391-399.

Comission of the European Communities, (2007), "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework (No. SEC(2007) 312)" European Union.

EPCglobal, (2005a), "EPC Generation One Tag Data Standards (No. 1.1 Rev 1.27)", EPCglobal.

EPCglobal, (2005b), "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960MHz (No. 1.0.9)", EPCglobal.

EPCglobal, (2005c), "The EPCglobal Architecture Framework", EPCglobal.

Geary, S. (2005), "2005 CSCMP Annual Confrence RFID", Tennessee: The University of Tennessee.

Juels, A., (2004), "Yoking-proofs for RFID tags", *In R. Sandu and T. Roshan (Eds.), International Workshop on Pervasive Computing and Communication Security - PerSec 2004* (pp. 138-143). Orlando, Florida, USA: IEEE Computer Society.

Juels, A., Rivest, R. L., and Szydlo, M., (2003), "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", *10th ACM conference on Computer and Communications Security*, Washington D.C.

Symbol Technologies, (2006), "Understanding Gen2: What it is, How you will Benefit and Criteria for Vendor Assesment".

Zebra Technologies, (2004), "Managing the EPC generation Gap", Retrieved 25/10/2006, from http://library.govtech.net/detail/RES/1099935750_315.html?src=integb

Zebra Technologies, (2006), "Electronic Product Code (EPC)", Retrieved 25/10/2006, from http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/epc_rfid_technology.html