RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs

M.J.B. Robshaw and T. Williamson

Impinj, 701 N. 34th Street, Suite 300,
Seattle, WA 98103, USA
{mrobshaw,twilliamson}@impinj.com

NIST Lightweight Cryptography Workshop 2015

Executive Summary

In this position paper[1] we provide a snapshot of the UHF RFID industry. Typically referred to as RAIN RFID after the foundation of the *RAdio IdentificatioN* (RAIN) *Industry Alliance*, this technology will be an integral part of the *Internet of Things (IoT)*. The light and constrained devices encountered in RAIN RFID will be increasingly deployed in applications that exchange medical, location, personal, and sensor information. As this development takes hold, cryptographic security will be an important consideration. To fully realize the potential of both RAIN RFID and the Internet of Things we believe that more efficient alternatives to existing NIST standards will be required.

1. In the cryptographic community, we should not under-estimate the extent or breadth of deployments that will take place in RAIN RFID and the IoT.
2. Given the market volume and business opportunities, we believe it inevitable that device manufacturers will deploy solutions that offer significant performance advantages over existing standardized solutions.
3. To avoid drifting into a *wild west* of immature and insecure solutions, guidance on new cryptographic technologies is vital.
4. We believe that NIST is ideally placed to provide this guidance.
5. Given the diversity of devices within the Internet of Things, we believe that guidance would best be provided by the publication of a small portfolio of approved technologies, rather than the advocacy of one single technology. In this way NIST can address the very different priorities of different device manufacturers.
6. Since existing NIST standards can provide perfectly good solutions in many IoT applications, any such portfolio should be viewed as complementing—and not replacing—existing standards.

[1] This document reflects the opinions and views of the authors.

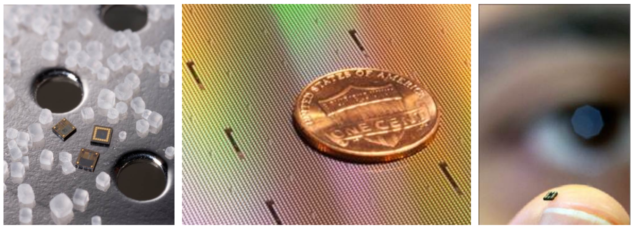


Figure 1. Previous generations of passive UHF RFID chips on a salt cellar, a silicon wafer, and a finger-tip.

1 Introduction

The *Ultra-High Frequency (UHF)* RFID chip is a remarkable piece of engineering. Small and cheap enough to be attached to billions of objects and requiring no onboard power supply, RFID tags that contain these chips can be reliably read at long range[2]. Figure 1 helps illustrate the size of previous-generation chips, though current devices are even smaller. Today, deployed systems can read hundreds of tags per second with close to 100% reliability.

The general public might not be aware, but there are billions of such tags in use today. Previously the preserve of supply-chain logistics, this particular form of RFID is experiencing significant deployment in retail where it provides exceptional granularity to product inventory and new in-store experiences for customers [7,19]. At the same time there are initiatives to increase the tagging of aircraft [17] and auto [20,25] parts as well as deployments in healthcare for pharmaceuticals, equipment, and personnel [22,23,24,26,27]. Consumer-facing deployments are expanding; beyond long-established race timing there are TV game shows, ice-cream parlors, vending machines, and consumer electronic products that all use the technology. There are even deployments in earth orbit [21].

The industry surrounding this technology has not had a particularly easy evolution. Early excitement failed to account for research-level difficulties in the technology and what was, at the time, an incomplete understanding of how best to effect a deployment. Today, however, there are numerous markets where the technology is established and deployments are spreading quickly. To reflect this growing presence the *RAdio IdentificatioN* (RAIN) *Industry Alliance* [16] was founded in 2014 and, as a result, it is increasingly common to refer to UHF RFID as RAIN RFID.

The *Internet of Things* (IoT) is a broad term that encompasses many devices and applications[3]. Certainly there is more to the IoT than RAIN RFID. However, accelerating adoption means that RAIN RFID will be an important part of the IoT and, in absolute numbers, the passive UHF tag will be by far the

[2] In contrast to HF RFID that is found in NFC applications.

[3] The term "Internet of Things" is attributed to Kevin Ashton, a pioneering contributor to the *Auto-ID Center*. The Auto-ID Center was one of the early drivers of UHF RFID adoption.

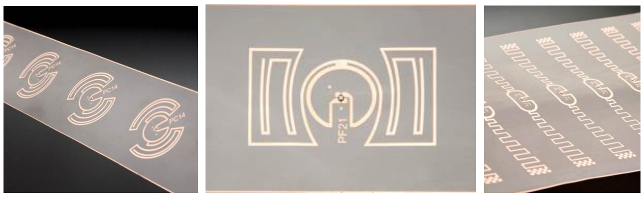


Figure 2. UHF RFID inlays sporting different antenna designs prior to integration into a tag. The chip can just be seen as the dot at the center of each antenna.

most deployed device. RAIN RFID provides the cheapest way to connect any object to the Internet and not only is each chip uniquely identifiable but users can dynamically interact with the chip to encode item- or application-specific information. During 2015 RAIN RFID will convey vast quantities of information from inanimate objects to global information systems.

Obviously not all this information is "equal". Most information transmitted today has little or no value outside the immediate application. However, some may be significant at a business or personal level and, as the range of applications broadens, we should anticipate increasing demands to protect information from eavesdropping, malicious corruption, or both. Further, irrespective of the information exchanged, a physical world filled with tagged and connected objects is quite unlike anything we have ever experienced and security technologies can help society manage some of the implications.

These issues have long been recognized by chip and tag manufacturers. The underlying communication protocol [4] requires that all compliant tags support a *Kill* mechanism and several RAIN RFID chips on the market provide switchable public/private profiles or long-/short-range modes for privacy. The goal of this position statement, therefore, is to highlight some additional technology steps that would work in tandem with, and further extend, the security techniques that are already deployed.

2 Performance, Capabilities, and Security

RAIN RFID communication depends on the EPCglobal Gen2v1 protocol [4] and its revision EPCglobal Gen2v2 [5]. The Gen2v1 protocol was ratified in 2008 and standardized[4] within ISO/IEC [9]. In 2013, the functionality of Gen2v1 was extended by the ratification of the Gen2v2. The most significant and far-reaching additions to this revision are optional over-the-air commands that support cryptographic security.

Tags vary widely in performance and form factor and Figure 2 shows a few different inlay designs prior to integration into a label or tag. The suitability of a final tag to a given application will depend on the chip feature set and its cost, its read-range, and the time required to complete the necessary task. Unfortunately,

[4] With the Gen2v2 specifications being incorporated as a revision.

the inherent tension between these three attributes poses a significant challenge to both implementation and business development.

2.1 Cost and area

Most of the costs in the design and manufacture of a chip can be treated as a fixed cost per silicon wafer. This means that the cost of a chip—and hence the final tag—will be closely related to its size. If the chip area increases there will be a reduced number of chips on a wafer and the cost per chip will need to increase.

All RAIN RFID chips must include the same essential building blocks. An *analog front-end* extracts power from the interrogator signal and provides the communication interface to the outside world. A *tag controller* is a hardware implementation of the underlying protocol plus additional tag-specific features. It also accesses the nonvolatile memory that stores the EPC number [4], equivalently referred to as the UII in [9], and all other memory that must persist without power.

Beyond such essentials, additional features will be determined by the manufacturers' business analysis and market priorities. One component that varies significantly between chips—because it is space-consuming—is an allocation of nonvolatile memory that is referred to as *user memory.* Anyone feeling constrained by smart cards will find RAIN RFID claustrophobic and manufacturers typically give figures for user memory in bits rather than bytes. Looking at the industry as a whole, RAIN RFID chips seem to fall into three broad families according to the amount of user memory they support.

1. A first group of chips that are highly optimized for cost and read performance. Such chips will have no more than 128 bits of user memory—in some cases none—and are likely to be used in retail applications.
2. A second group of chips that offer moderate amounts of user memory, perhaps running to around 512 bits, making them suited to a wide-range of applications.
3. A third group that comprises specialty chips with larger amounts of memory such as 2 Kbits, 8 Kbits, or even more. Such chips often include features that address specific applications.

Adding cryptography. When adding a cryptographic engine there will certainly be an impact to the area of a chip. However it is not accurate to equate that impact with the size of the cryptographic component in isolation since the net impact will depend on the following factors:

1. The size of the cryptographic engine including its operational parameters (*e.g.* the block and key size in the case of a block cipher).
2. The memory required to store the key along with associated key management support.

3. The data interface between the cryptographic engine and other components on the chip.
4. The necessity and/or choice of counter-measures for secure implementation.

The addition of cryptography should not be under-estimated and the implications of doing so are complex. While a larger cryptographic engine *might* fit on a chip, there will always be pressure to use something smaller. First, we don't want to use more space than we need lest we unnecessarily impact performance and cost. (RAIN RFID chip designers really do question the inclusion of every bit.) But second, the real benefit of a simple cryptographic engine is in the freedom it gives the implementor to find the right performance trade-off. The more complex the cryptographic engine, the fewer the implementation strategies that make economic sense. In an extreme case there might be only one viable architecture. With a more lightweight design, however, a cryptographic technology can be optimized for area, power, or speed in different ways which will help to broaden the total application space.

2.2 Read range and power

One of the significant benefits of RAIN RFID is the long read-range. While RAIN RFID can also be operated at short-range, many applications benefit from a read-range that is quoted in meters [8].

To increase tag readability, the chip, antenna, and tag designers strive to provide as much *sensitivity* as possible as the chip performs basic operations. Not all operations have the same requirements. For instance, the power required to read data from the most sensitive RAIN RFID chips is less than half the power required to write data to the chip. This difference in power consumption leads to different operating ranges for different applications.

A primary use case for RAIN RFID is to singulate a tag and recover its EPC. This requires a memory read operation and the operational range of a RAIN RFID tag is gated by the read sensitivity. However, if an application requires that we write to a tag then the operational range of a tag in that application will be gated by the write sensitivity. So, as we add new features to a tag we need to understand the use case to know how the power consumed by a new feature will affect its operational range.

As an aside we note that it is difficult to directly translate a sensitivity figure into an explicit read range. Environmental conditions, especially the type of material to which a tag is attached, can have an enormous impact in the field. Instead we need to rely on deployment experience to arrive at the read ranges we find quoted in the literature.

Adding cryptography. It turns out that for most applications adding cryptography needn't *necessarily* impact the operational range of a tag. One likely implementation scenario is that while the encryption engine is operational much of the rest of the tag remains quiet. In this mode the encryption engine would dominate the power consumption of the tag and, provided the power consumption of the encryption engine is less than the power consumption for reading memory, the operational range of the RAIN RFID tag will remain unchanged. Of course, if a more complex cryptographic engine is used then the operational range can be affected. We note that since the power consumption for an implementation can often be traded with transaction time, then earlier conclusions also hold here. Namely, that the more complex the cryptographic engine, the less chance of finding an appropriate implementation option.

2.3 Transaction time

The time required to complete a tag interaction can be a vital consideration from a system perspective. However what is important in one application might be irrelevant in another. To illustrate, consider four very different scenarios.

1. For single-item tag identification using a hand-held reader we might expect only a few tags to be in view of the interrogator at any one time. The reader would likely be close to the tag and, since a human is involved, the time available to interact with a tag would likely be generous.
2. There is a trend in retail to continually perform item inventory on the shop floor from installed overhead readers which is sometimes referred to as "always on". Despite the very large number of tags, tag inventory is continuous and after an initial sweep incremental. The acceptable transaction time per tag can be long.
3. If we wanted to bulk encode or track boxes of goods in the supply chain then we may be faced with moving cartons that contain a large number of tags. This would likely result in a short acceptable per-tag transaction time in a dense tag environment.
4. We might imagine a road-tolling deployment with a windshield badge being read from an overhead gantry as a car travels at speeds over 100 kph. While tags may be sparse, they will be in range and reliably powered for only a very short period of time.

These are very different use cases and the chip designer will aim to satisfy the constraints attached to the most strategically important use case.

Adding cryptography. In academic comparisons of cryptographic technologies, it is customary to give the time to complete the cryptographic operation. However, in a deployment, the user is not concerned about the time for a cryptographic operation but rather the time to complete the entire transaction. For this we need a system-wide view that encompasses the cryptographic engine, the cryptographic protocol, and the communication protocol in combination.

As an example we might consider tag authentication. The Gen2v2 protocol [5] defines an *Authenticate* command[5] and its response format. These definitions

[5] There is also a *Challenge* command that could provide system performance benefits in certain situations.

include a variety of fixed headers and trailing blocks that are required by the protocol but which impact the net transaction time. The *Authenticate* command transports messages defined by the cryptographic protocol. These messages contain the payloads for the cryptographic engine plus another layer of overhead. For instance, Section 3 discusses a set of standards among which two, ISO/IEC 29167-10 and ISO/IEC 29167-11, outline tag authentication using different block ciphers[6] [10,11]. Looking at these standards we can identify the amount of data that is passed over-the-air between the interrogator (I) and tag (T) by the cryptographic protocols. These different amounts of data will impact the transaction time.

	I ⇒ T (bits)	T ⇒ I (bits)
ISO/IEC 29167-10	96	128
ISO/IEC 29167-11	48	64

Finally, the third component of the total transaction time will be the performance of the encryption engine itself. This is where the implementor has the most flexibility and a simple cryptographic technology gives additional trade-offs to explore.

2.4 Security

The diverse uses of RAIN RFID make detailed discussion of cost, operational range, and transaction time difficult. When we add cryptography we add a new trade-off: security. To many, security is an issue of key length, but we believe the issue to be more nuanced.

Looking at key length first, it is clear that for some—but not all—applications the security provided by a symmetric cryptosystem with an 80-bit key will be adequate. Equally, for some—but not all—applications a 128-bit key will be a real benefit. Chip manufacturers will make their choice depending on their business analysis. Typically a shorter key will translate into a smaller chip so, provided the security level is good enough, there may be little incentive to burden the chip with more.

In RAIN RFID deployments it is unlikely a symmetric cryptosystem with a key of length $\geq$80 bits will be compromised by brute-force, even using clever data-time-memory trade-offs [1]. Nor are cryptanalytic attacks likely on most modern symmetric cipher designs where, barring disaster, many of the foundations to secure design appear to be well-founded[7]. Instead the greatest threat of key compromise comes from side-channel analysis which pays little respect to key length. The reality is that a 128-bit cipher with a vulnerable power profile can be far more exposed than a safer implementation of an 80-bit cipher. Furthermore, if the additional space freed by having an 80-bit cipher can be used for additional

[6] Our purpose is not to judge one of these standards as necessarily better than the other; the most suitable choice will depend on the use case.

[7] This is in contrast to asymmetric designs where new schemes typically rely on new hard problems.

counter-measures, then the total *delivered security* can be in complete opposition to conclusions based solely on the key length.

In the remainder of this section we draw attention to the fact that different security goals can impose different requirements on an implementation. To illustrate, we consider the case of using symmetric encryption to provide device authentication and channel security.

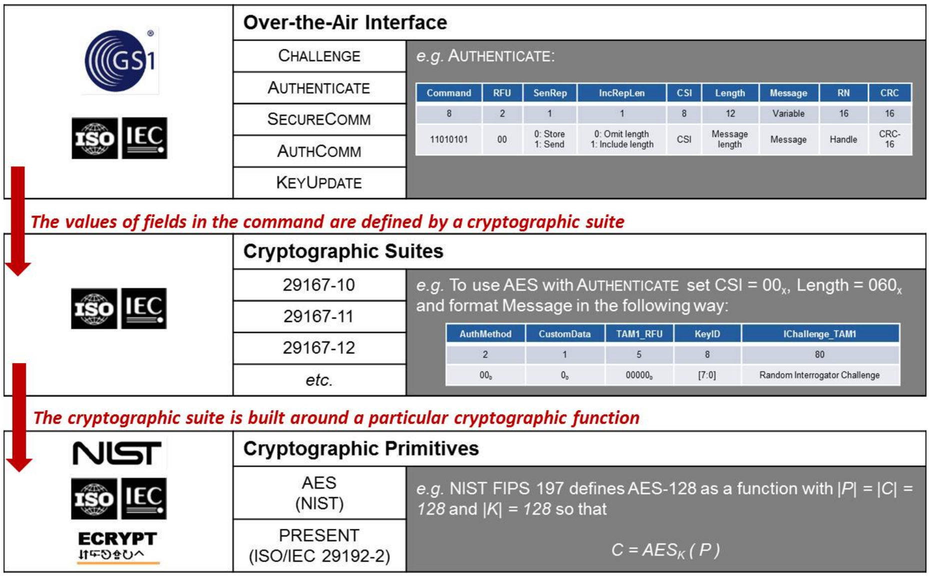
Authentication. Tag, interrogator, and mutual authentication are (typically) provided by means of challenge-response protocols. These are simple cryptographic operations on small amounts of data. With regards to symmetric cryptography the conventional wisdom is that while stream ciphers can certainly accomplish the task, an initialization phase—whereby key and a so-called *initialization vector* are mixed prior to generating the keystream—would be a significant operational penalty. By contrast, block ciphers would avoid this set-up time which would be beneficial for authentication-only applications.

Our prototyping confirms this, though we note one partially-compensating issue that is not often covered in academic publications. By focusing on the encryption engine in isolation, many implementors do not address the manner in which a cryptographic module is loaded with the encryption key and the plaintext. This turns out to be particularly important in the case of block ciphers which operate on nibbles, bytes, words, or blocks whereas the underlying protocol conveys data bit-wise. There are therefore subtle timing and loading issues to consider during the integration of a block cipher with the tag controller, issues that are largely absent when using a stream cipher.

Secure channel. The goal of a secure channel is to protect information exchanged over-the-air. There are various ways to do this. For instance, application-level solutions might be employed to protect stored and transported data independent of the communication protocol. Alternatively, we might use protocol-level protection—perhaps to protect or hide commands as well as payloads—and the Gen2v2 protocol provides two encapsulating commands *SecureComm* and *AuthComm* for this purpose (see Section 3 for more details).

It is probably a useful data point to consider the amount of data that might need protecting in RAIN RFID. For efficiency reasons, commands and payloads are short with most being less than 80 bits in length even when including a session ID—the so-called *handle*—and a 16-bit CRC[8]. While the commands *Read* (which reads data from memory), *BlockWrite* (which efficiently writes data to memory) and *KeyUpdate* (which allows a key to be updated over-the-air) might be longer, there are still tight limits in practice. First, the amount of user memory on a RAIN RFID chip imposes a modest upper limit on the payloads for memory access operations. Second, at least for symmetric cryptography, keys would likely be 128 bits in length or less.

[8] When commands are encapsulated in *SecureComm* or *AuthComm* the handle and CRC-16 are omitted.



Over-the-Air Interface

CHALLENGE
AUTHENTICATE
SECURECOMM
AUTHCOMM
KEYUPDATE

e.g. AUTHENTICATE:

Command	RFU	SenRep	IncRepLen	CSI	Length	Message	RN	CRC
8	2	1	1	8	12	Variable	16	16
11010101	00	0: Store 1: Send	0: Omit length 1: Include length	CSI	Message length	Message	Handle	CRC-16

The values of fields in the command are defined by a cryptographic suite

Cryptographic Suites

29167-10
29167-11
29167-12
etc.

e.g. To use AES with AUTHENTICATE set CSI = 00_x, Length = 060_x and format Message in the following way:

AuthMethod	CustomData	TAM1_RFU	KeyID	IChallenge_TAM1
2	1	5	8	80
00_b	0_b	00000_b	[7:0]	Random Interrogator Challenge

The cryptographic suite is built around a particular cryptographic function

Cryptographic Primitives

AES (NIST)
PRESENT (ISO/IEC 29192-2)

e.g. NIST FIPS 197 defines AES-128 as a function with $|P| = |C| = 128$ and $|K| = 128$ so that

$$C = AES_K(P)$$

Figure 3. The top-level bodies—GS1 and ISO/IEC SC31—define over-the-air commands that are crypto-agnostic. The lower-level bodies—NIST, ISO/IEC SC27, ECRYPT (not formally a standards body)—provide definitions for cryptographic primitives. Work in ISO/IEC SC31, the middle body, is intended to link the two.

Our prototyping suggests that when implementing some form of secure channel via encapsulation [5], an existing NIST standard like the AES [14] will operate at a distinct disadvantage to a stream cipher, a more efficient block cipher, or to a dedicated design. Indeed, this helps to confirm the importance of an area of active research that is encompassed by the ongoing CAESAR project [3]. Here dedicated designs as well as proposals to use a block cipher in constrained environments are all under consideration as a way of providing authenticated encryption. After sufficient cryptographic review, it is not inconceivable that some of these CAESAR proposals may find application in RAIN RFID.

3 Cryptography and RAIN RFID Today

Earlier this year the first chip extending cryptographic authentication to RAIN RFID was announced [15]. Here we provide an overview of the industry initiatives that have helped make this a reality, and which will support future security solutions.

The Gen2v1 and Gen2v2 protocols define over-the-air commands for RAIN RFID but they are independent of any specific cryptographic technology. For instance, we have already seen that Gen2v2 includes a command *Authenticate* that is intended to be used as part of a solution for tag, interrogator, or mutual authentication. The format of the *Authenticate* command is given below, with the field descriptions, lengths, and possible values given by the three rows of the table. The `handle` and `CRC-16` are part of the communication protocol while `SenRep` and `IncRepLen` are application options. The most important fields for our purposes are marked $\star$ and their values are not defined by Gen2v2. The *Cryptographic Suite Indicator* `CSI` identifies the cryptographic algorithm/protocol while the `Length`/`Message` fields identify the cryptographic payload being carried by the command.

	`command`	`RFU`	`SenRep`	`IncRepLen`	`CSI`	`Length`	`Message`	`RN`	`CRC`
length	8	2	1	1	8	12	*variable*	16	16
value	$\texttt{d5}_\mathrm{h}$	$\texttt{00}_b$	$\texttt{0}_b/\texttt{1}_b$	$\texttt{0}_b/\texttt{1}_b$	$\star$	$\star$	$\star$	`handle`	`CRC-16`

For the choice of cryptography we need to turn to other sources. NIST standards such as the *Advanced Encyption Standard (AES)* [14] are a natural choice. Other cryptographic technologies have been standardized within ISO/IEC SC27 with some, such as PRESENT [2,12] and CRYPTOGPS [6,13], explicitly targeted at constrained environments. Even a research initiative such as eSTREAM [18], while not formally a standards body, is well-regarded as a source of cryptographic primitives.

But we might now observe an implementation gap between the Gen2v2 over-the-air commands and the cryptographic primitives (see Figure 3). For example, the *Authenticate* command says nothing about how to achieve tag authentication using, say, a *challenge-response* authentication protocol. It doesn't even say what algorithms might be supported on the tag or interrogator. Similarly, the AES standard (FIPS-197) doesn't tell us how to use the AES block cipher to perform tag authentication. Instead, FIPS-197 tells us how a 128-bit output is derived from a 128-bit input and a key. It is the goal of the work in ISO/IEC SC31/WG7, therefore, to provide a mapping between the cryptographic primitive and the generic over-the-air commands. This mapping is referred to as a *cryptographic suite* and the ISO/IEC 29167 standard consists of several parts, each describing a cryptographic suite and a solution. Each cryptographic suite gives the allocated *CSI* number and specifies the composition of messages between interrogator and tag as well as the actions of the tag and interrogator. An annex to each cryptographic suite specifies which of the Gen2v2 commands—such as *Authenticate*—might then be used.

Many cryptographic suites in ISO/IEC 29167 follow the separation outlined in Figure 3 and build on previously standardized primitives. Others use less familiar and non-standardized technologies. A list of the current parts to ISO/IEC 29167 is given in Table 1 along with the claimed security services. We see that tag authentication is supported by all cryptographic suites. *Interrogator* and *mutual authentication* are provided less often while *channel security*—the protection of data transferred over the air—is supported in only a few cases. This is not surprising. While two encapsulating commands *SecureComm* and *AuthComm* are defined by Gen2v2, it is up to the cryptographic suite to define how the channel might be instantiated. Those familiar with some of the system design issues involved will be immediately aware how difficult this might be, particularly while striving to remain efficient.

Table 1. The different parts of ISO/IEC 29167 along with the different services they provide. See the accompanying text for more details. Symmetric-key schemes are given in black while asymmetric-key schemes are given in blue.

	Name/	Authentication			Channel
	Primitive	Tag	Reader	Mutual	Security
29167-10	AES-128	Y	N	N	N
29167-11	PRESENT-80	Y	N	N	N
29167-12	ECDH	Y	N	N	N
29167-13	Grain-128a	Y	Y	Y	Y
29167-14	AES-OFB	Y	Y	Y	N
29167-15	XOR	*Paused*			
29167-16	ECDSA	Y	N	N	N
29167-17	CryptoGPS	Y	N	N	N
29167-18	Hummingbird	*Withdrawn*			
29167-19	RAMON	Y	Y	Y	Y
29167-20	Algebraic Eraser	Y	Y	Y	Y

4 Conclusion

In this position paper we have provided a snapshot of the RAIN RFID industry and its place in the Internet of Things. As deployments evolve and the technology moves into more applications, cryptographic security will become increasingly important.

The first commercially available RAIN RFID chip with cryptography has been announced and the designers of that chip opted to use the AES. This may well be a good choice for specific use cases. However, to fully realize the potential of RAIN RFID and the Internet of Things we believe that more efficient alternatives to the AES and other NIST standards will be needed. This should not be construed as negative comment on existing NIST standards. In the case of the AES, this remarkable cipher remains as strong and vital as ever; it is an important deployment option. Nevertheless, tomorrow's connected world was (almost) inconceivable when the AES and its immediate pre-cursors were being designed twenty years ago. With our current know-how on algorithm design and a deployment landscape that has changed significantly, it is possible that other options will be better-suited to the full diversity of RAIN RFID applications. With this in mind we close with the list of observations that were highlighted in the *Executive Summary*:

1. In the cryptographic community, we should not under-estimate the extent or breadth of deployments that will take place in RAIN RFID and the IoT.
2. Given the market volume and business opportunities, we believe it inevitable that device manufacturers will deploy solutions that offer significant performance advantages over existing standardized solutions.
3. To avoid drifting into a *wild west* of immature and insecure solutions, guidance on new cryptographic alternatives is vital.

4. We believe that NIST is ideally-placed to provide this guidance.
5. Given the diversity of devices within the Internet of Things, we believe that NIST guidance would best be provided by the publication of a small portfolio of approved technologies, rather than the advocacy of one single technology. In this way NIST can address the very different priorities of different device manufacturers.
6. Since existing NIST standards can provide perfectly good solutions in many IoT applications, any such portfolio should be viewed as complementing—and not replacing—existing standards.

References

1. A. Biryukov. Some Thoughts on Time-Memory-Data Tradeoffs. Available via eprint.iacr.org/2005/207.pdf.
2. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Proceedings of CHES 2007*, Lecture Notes in Computer Science, vol. 4727, 450–466, Springer, 2007.
3. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness Available via competitions.cr.yp.to/caesar.html.
4. EPCglobal. EPC Radio Frequency Identity Protocols, Generation 2 UHF RFID. Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 1.2.0. Available via www.gs1.org/gsmp/kc/epcglobal/uhfc1g2.
5. EPCglobal. EPC Radio Frequency Identity Protocols, Generation 2 UHF RFID. Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.1. Available via www.gs1.org/gsmp/kc/epcglobal/uhfc1g2.
6. M. Girault, G. Poupard and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, vol. 19, number 4, 463–488, 2006.
7. E. Holmes. Designer Rebecca Minkoffs New Stores Have Touch Screens for an Online Shopping Experience. Available via www.wsj.com/articles/.
8. Impinj. The Different Types of RFID Systems. Available via www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/.
9. ISO/IEC 18000-63:2013. Information technology – Radio frequency identification for item management – Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C.
10. ISO/IEC 29167-10:2015 – Information technology – Automatic identification and data capture techniques – Part 10: Crypto suite AES-128 security services for air interface communications.
11. ISO/IEC 29167-11:2014 – Information technology – Automatic identification and data capture techniques – Part 11: Crypto suite PRESENT-80 security services for air interface communications.
12. ISO/IEC 29192-2:2011 – Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers.
13. ISO/IEC 29192-4:2013 – Information technology – Security techniques – Lightweight Cryptography – Part 4: Asymmetric Techniques.
14. National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard, November 2001.

15. NXP Introduces Worlds First RAIN RFID Tag with Cryptographic Security and Long Read Range. Available via http://www.nxp.com/news/press-releases/2015/04/nxp-introduces-world-s-first-rain-rfid-tag-with-cryptographic-security-and-long-read-range.html.
16. RAIN RFID. Available via www.rainrfid.org.
17. M. Roberti. Airbus Enters New Phase of RFID Usage, Digitalization. Available via www.rfidjournal.com/articles/view?12731.
18. M. Robshaw and O. Billet. New Stream Cipher Designs: The eSTREAM Finalists. ISBN 978-3-540-68351-3. Springer.
19. C. Swedberg. Marc O'Polo Discovers RFID's Benefits. Available via www.rfidjournal.com/articles/view?12657.
20. C. Swedberg. Porsche Uses RFID to Track Prototype Testing, Improve Security. Available via www.rfidjournal.com/articles/view?12700.
21. C. Swedberg. Johnson Space Center Seeks Partners to Market NASA-Developed RFID Technologies. Available via www.rfidjournal.com/articles/view?11633.
22. C. Swedberg. Smart Septa System Uses RFID to Authenticate Medications. Available via www.rfidjournal.com/articles/view?12649.
23. C. Swedberg. Barcelona-area Hospital Manages Surgical Supplies Via Smart Cabinet. Available via www.rfidjournal.com/articles/view?12012.
24. C. Swedberg. East Midlands Ambulance Service Uses RFID to Track Equipment Quickly. Available via www.rfidjournal.com/articles/view?11948.
25. C. Swedberg. Audi Launches RFID Deployment for Tracking Assembled Vehicles Worldwide. Available via www.rfidjournal.com/articles/view?12496.
26. C. Swedberg. Hanmi Pharmaceutical Uses RFID to Automate Picking, Shipping. Available via www.rfidjournal.com/articles/view?9455.
27. C. Swedberg. Technologies Solutions Group Markets RFID Hand-Hygiene Compliance System. Available via www.rfidjournal.com/articles/view?11725.