RFID Product and Brand Protection

Finding the privacy and security settlement for the mass market

Dave Birch mailto:dave.birch@chyp.com

Consult Hyperion http://www.chyp.com

Please note that extract from an earlier version of this article was perpared for *Product and Image Security* (Oct. 2004).

This draft 10/18/03 10:28 am, 1877 words (5 pages)

The RFID Race

In the retail world, the introduction of Radio Frequency Identification (RFID) technology is well underway. The technology is built on tiny computer chips that can communicate wirelessly with nearby readers (hence the generic "contactless" name for this kind of chip technology). It has been around for some time and is already widely used other sectors [1]: mass transit being one of the largest (London's *Oyster* cards work this way).

When you add an RFID chip to something valuable that you want to track or trace, a cow or a laptop computer, they're known as smart tags. When you add them to a can of beans, they become a sort of clever bar code containing data that can be read through boxes and packaging. In this context, they store Electronic Product Codes (EPCs). There is an international standard for EPCs coming together, and this defines the data that EPCs will transmit to readers (see Figure 1 for an example standard format).

Figure 1. EPC Format.

EPC and RFID are not the same thing at all: barcodes could hold the EPC and an RFID chip could (and should) hold more than the EPC [2]. The RFID chip might, for example, contain information about how something should be stored or stacked, expiration dates or manufacturing dates and many other items of data.

The introduction of RFID chips storing EPCs (initially at the case or pallet level, but moving on to the item level) means substantial economic benefits: small improvements in the supply chain can mean big savings and these savings can be passed on to customers. When EPCs are linked with pervasive wireless networks and sophisticated management systems, the potential improvements in business efficiency could be substantial [3]. The world's biggest retailer,

Walmart, is a prime mover in this field and they expect the introduction of case-level EPCs to save them more than a billion dollars every year in their supply chain [4].

Some retailers are already experimenting with EPC at the item level. A UK example is Marks & Spencer, which has been trialling tags in some stores for some items of clothing. The tags currently being used by Marks & Spencer cost 34p each [5]. When the worldwide EPC standard is finalised (within the next year) then volumes of RFID chips for EPC will climb and costs will start to tumble. In the relatively near term, EPCs will become affordable for a great many products at the item level.

So if all items are going to sprout EPCs, does this mean a revolution in product security, brand protection and related fields? It does, but a number of issues will have to be dealt with first before the introduction of EPCs will make a real difference. From the security perspective, we can separate these issues into distinct groups: protecting the product and protecting its provenance.

Protecting Product

EPC technology was specifically designed to be open: there is nothing secret in EPCs and anyone can read them [6]. There is nothing to stop someone from sticking the wrong EPC on an item. If all bottles of scotch have an EPC, then counterfeiters could copy those EPCs and put them on fake bottles of scotch. This is not true of all RFID tags. The more sophisticated RFID tags used for payments, for example, include a tamper-resistant microprocessor with on-board cryptography [7] to add a digital signature to the data sent back to the reader. Microprocessors therefore mean significant additional functionality (and expense, of course).

How will EPCs be used for product security in practice? Pharmaceuticals provide a useful case study. Worldwide, about 6% of pharmaceuticals are counterfeit [8]. The US Food & Drugs Administration (FDA) has said that using EPCs to identify all drug products intended for use in the United States is the "single most powerful tool available to secure the U. S. drug supply" [9]. But as they go on to point out, the tag is only part of the story: to combat drug counterfeiting the industry needs "information systems that allow all users to identify each package of drugs and its associated data". They expect to see these develop quickly. In fact, they hope to have all drugs tagged by 2007, as shown in the roadmap below (Figure 2).

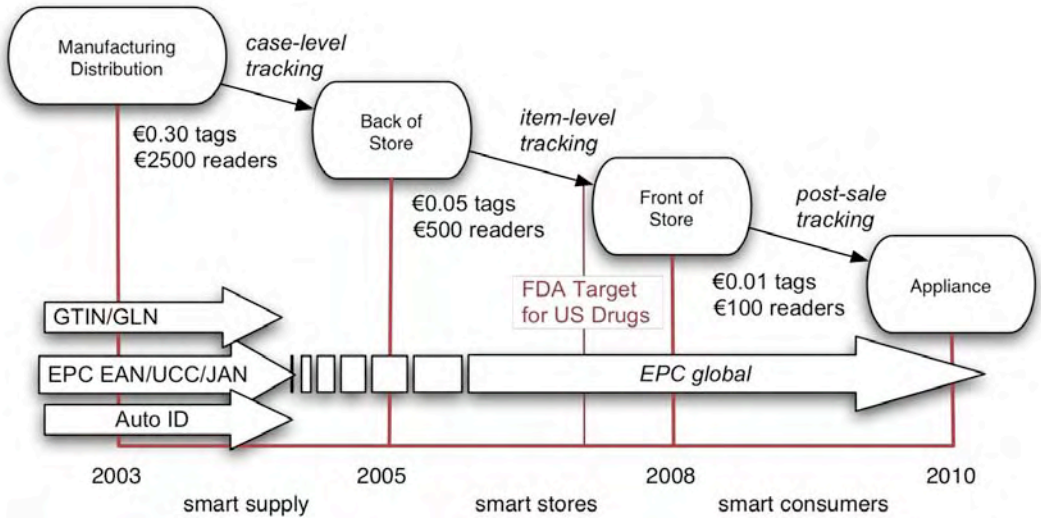

Figure 2. EPC Roadmap (Source: CHYP Retail Alliance, 8/04).

There are a number of US distribution centres already involved in a pilot project shipping tagged drug bottles from manufacturing plants to pharmacies, where readers are linked to a computer to check for theft, recalled drugs, outdated drugs and other logistical errors [10]. It is reasonable to expect the same technology to spread to all sorts of other products: CDs, aircraft parts, perfume and everything else.

Protecting Provenance

For planning purposes, then, we can assume that a few years from now all items will have EPCs on them and anyone will be able to read those EPCs. If I see a Gucci handbag on sale in a shop, I will be able to point my Bluetooth EPC-reading pen at it[1] and read the EPC. My mobile phone can then tell me that the handbag is Gucci product 999, serial number 888. This information is, by itself, of little use to me. I could go onto the Gucci-lovers web site and find out that product 999 is a particular kind of handbag, but nothing more: yet I need to know more to make a decision about whether to buy the bag or not. I may know that the ***tag*** is "valid", but that doesn't tell much about the bag. For that, I need more data.

The EPC network architecture defines the infrastructure for finding that data. Organisations that read EPCs (eg, a retail chain) will have networks of servers that collect the tag data and turn it into meangingful information[2]. These servers (called "savants") can then use this information to query corporate databases: these databases can then query other databases. There's an XML schema, known as "physical markup language" (PML) that they can use to talk to each other.

If I wanted to know if the handbag is real or fake, then I need to have access to its provenance (known by that savant network) as well as its product details. The provenance may be distributed quite widely across the network. The retailer's database knows which distributor the bag came from, the distributor's database knows which factory the bag came from and Gucci's

[1] These are already on sale.
[2] They actually turn it into a pointer to meaningful information but it's logically the same thing.

database should know all of this. I need access to this data to get the data I need to decide whether the bag is real or fake.

All well and good, but why would the retailer, the distributor or Gucci tell me? How do they know whether I am a retailer, one of their best customers, one of their own "brand police", a counterfeiter (who would love to know which tags are in which shops and so on) or a law enforcement officer with a warrant?

The technology to solve that problem already exists: smart cards and digital signatures. A Gucci brand policeman might have a Bluetooth pen tag reader connected to a PDA with a smart card and a GPRS connection. They could then point the pen at a bag and fire off a query: the query would have a digital signature attached (from the smart card) and the Gucci savant could check that signature before processing the query. Gucci could then send a digitally-signed and encrypted query to the distributor's savant which would then send back a digitally-signed and encrypted response to be passed back to the brand policeman: "no we've never heard of this bag" or "we shipped this bag to retailer X on this date" or "we've just been queried on this bag in Australia" or something similar.

The central security issue for brand protection is therefore the protection of (and access to) the provenance data. It is this area that demands industry attention. The foundation of the "privacy settlement" between government, business and the public must be open: every stakeholder must understand how, why and when savants will be allowed to answer queries and under what circumstances they will send a result (and who they will tell they sent the result to, for later auditing).

Looking Forward

The purpose of this article is not to reiterate the widely-expressed concerns about security and privacy in the EPC world, but to point out that if the world of product and brand security is to capitalise on the worldwide deployment of EPC it will have to tackle these issues in an open way to find a privacy settlement that works. Many of the questions that need to be answered to reach this settlement are not much to do with technology and almost nothing to do with tags. Should customers have the right of access to the provenance of their purchases? Should retailers have access only to the provenance of the finished product they are selling or all of its components? Should there be one tag or many? This last question is important. Since EPCs are not (in themselves) secure, the future may see the use of multiple tags. One could envisage high-value or controlled goods having both a simple EPC tag for tracing (linked to savants) and a microprocessor tag (perhaps even one that can remember where it's been, what the temperature was and so forth) linked to private databases.

Finally, it is important to note that the primary purpose of EPCs is not and has never been brand protection and they are not the "silver bullet" for brand protection that companies such as Procter & Gamble are looking for [11]. Having said that, there is no doubt that brand protection can be significantly enhanced by exploiting EPCs stored in RFID chips in the right way and that organisations should begin developing their strategy for that exploitation.

REFERENCES

1. Finkenzeller, K. *Example Applications* in *RFID Handbook*. p. 227-274, John Wiley (Chichester: 1999).

2. Crawford, J. *The Electronic Product Code (EPC) and EPC Network Services* in proc. of *RFID Europe*, Shorecliff (London: Oct. 2004).

3. Keenan, F. *If Supermarket Shelves Could Talk* in *Business Week.* p. 66 (31st Mar. 2003).

4. Avenel, Y. *Privacy: Fears and Facts* in *Smart Card Trends.* **1**(7): p. 1,16 (Sep. 2004).

5. Hankins, T. *To What Extent is Privacy Compromised by Digital Identity Management?* in proc. of *Identity Management Summit*, IIR (London: Jul. 2004).

6. Willoughby, M. *Securing RFID information* in *Computerworld* (20th Sep. 2004).

7. Birch, D. *Chips That Chat* in proc. of *Wireless World*, Digital World Research Centre (University of Surrey: Jul. 2004).

8. Cox, G. *The Need for Brand Protection* in proc. of *Brand Protection Europe*, Pira (London: Sep. 2004).

9. *Combating Counterfeit Drugs*. Food and Drug Administration report (Washington: Feb. 2004).

10. Newmarker, C. *High-tech fight vs. counterfeit drugs* in *Associated Press* (13th Sep. 2004).

11. Kennedy, J. *Defining a Successful Global Brand Protection Strategy* in proc. of *Brand Protection Europe*, Pira (London: Sep. 2004)