Design patterns and Business Models for a New Generation of RFID Solutions.

Henrik Granau
12/11/2007

Market expectations that widespread deployment of RFID for item-level tagging would by now be commonplace are being viewed as exaggerated by some industry watchers.

However, as Geoffrey Moore ("Crossing the Chasm") and others have observed, "bubbles" and their consequent shakeout are a natural process for most new technologies. Shakeouts typically mark the point at which an emerging technology is ready to take off. Clayton Christensen ("The Innovator's Dilemma") highlights how truly important breakthrough, 'disruptive', technologies are often rejected initially by mainstream customers.

Could it be that the early disappointments with expectations for item-level tagging now mark a turning point for RFID? **RFIDsec** and our global partners believe that RFID technology is now more important than ever. We see exciting new possibilities, based on the new generation of RFID Solutions" or "RFID 2.0."

Although the term "Web 2.0" suggests a new version of the Web, it does not imply an update to any technical specifications, but to changes in the ways that developers and end-users can now use the Web, moving from pure content provision to collaborative development of content.

With RFID, it is different. In addition to changes in the ways that developers and end-users can use RFID technology, "RFID 2.0" will require enhanced security in the RFID Tags and in the communication between Reader and RFID Tag.

This article is an attempt to clarify just what we at **RFIDsec** mean by "RFID 2.0", the new generation of RFID Solutions.

Today's perspective

Although the principles of RFID technology are more than 50 years old, **RFIDsec** considers that the AutoID Labs and EPCglobal initiatives, driven primarily by WalMart and DoD, mark the beginning of the widespread use of RFID technology.

In many cases it is still hard for manufacturers to justify an investment in RFID. When the focus is often only on replacing barcodes, the manufacturer has to carry the bulk of the costs, while the benefits are spread over the entire supply chain. This is seen as a major inhibitor to widespread adoption of RFID technology, at least until the involvement of the large retailers.

The lack of volume demand means a relatively high unit production cost of RFID tags, further limiting economic business cases for RFID. A variety of RFID implementations, based upon various standards, typically specifying just the lower level, technical communication interfaces, is a further obstacle to widespread adoption and significant volumes.

The WalMart mandate has now focused attention on EPC (and Gen2) as the standard to be adopted. This mandate has aligned nearly all providers of RFID technology, with the expectation of significant rewards when item-level tagging is widely adopted, with potentially billions of RFID tags.

Early adopters of RFID tag technology have mainly concentrated on replacing barcodes to optimize supply chain logistics, not addressing Point-of-Sales or Product Life Cycle issues. A significant assumption has been that the RFIDs will only contain the EPC number, without holding any additional information, and that the EPC number will be used as a key to centrally held product information databases.

Extending the horizons

However, many industries want to store significant amounts of data on the RFID tag itself. Aviation manufacturers want to attach the tags to the relevant parts on an aeroplane, typically to store product maintenance history on the part itself. This approach is now being adopted by manufacturers from other industries as well. It is evident that we must now protect data on the RFIDs in a secure, and at the same time, dynamic way.

In addition, privacy concerns raised by consumer groups are starting to materialise. The pharmaceutical industry now requires that the RFIDs be deactivated at the point of sale, and then 'reactivated' at a later stage, for example, when checking for authenticity and for recall at the point of consumption, in either domestic or hospital use. We at **RFIDsec** believe that the initial idea of addressing privacy concerns simply by killing the RFIDs at the point of sale is no longer feasible.

After some unfortunate implementations of RFID technology, several states in the U.S. are in the process of passing laws against the use of RFID tagging (in schools, in libraries, for vehicle identification etc.). The European Union has conducted an open consultation on RFID tagging where security and privacy were identified as the major issues that have to be addressed, otherwise regulation will be imposed on the RFID industry.

Many organizations within the RFID industry still appear to believe that once the users get a better understanding of the RFID technology (you can not be tracked by satellites just by wearing a simple passive tag and the tag only contains a dumb number) then the privacy issues will slowly disappear.

The "Internet of Things"[1] is a great vision. We are moving towards what the ITU has called a "ubiquitous network society", one in which networks and networked devices are everywhere. But what if much more was connected to a network: a microwave, a car, or a cup of coffee? When things (products) can communicate with each other over the internet, then RFIDs and RFID readers on or inside the products will play a major role. The "Internet of Things" will not happen if we kill all the RFID's at Point-of-Sale!

Once the security and privacy issues are resolved, new business models will appear, based on "The Long Tail"[2], with services based upon the RFIDs being on or inside the products. Even for the

[1] From the 7th ITU Internet Report, 2005 (see http://www.itu.int/osg/spu/publications/internetofthings/).
[2] The phrase ***The Long Tail*** was first coined by Chris Anderson in an article from October 2004's edition of Wired magazine to describe certain business and economic models such as Amazon.com or Netflix. Businesses with distribution power can profitably sell a far greater volume of items in small quantities, unlike high street chains that are limited to selling large quantities of a relatively small number of items (the "Top 40" mentality).

product manufacturers there will be the possibility (using pay-per-use) to sell additional products or related services, helping to justify the initial investment in RFID.

The way that we use RFID technology is changing; standardisation, privacy and security demands are all directly affecting the RFID industry. As a first step towards the "Internet of Things", **RFIDsec** recommends that the RFID industry adopts a new design template and business model for a new generation of RFID technology. This is what we are calling "RFID 2.0".

From Supply Chain (RFID 1.0) to Product Life Cycle Management (RFID 2.0)

The following high level points describe the key differences:

RFID 1.0		**RFID 2.0**
– Intelligent barcode	→	- RFID is a computer
– Static	→	- Dynamic
– Single purpose	→	- Context aware
– One access point	→	- Multiple access points
– Auto ID	→	- Collaborative usage
– Limited security	→	- Rich security
– Use in supply chain	→	- Use in full Product Life Cycle

But what was it that made us identify one approach as "RFID 1.0" and another as "RFID 2.0"?

The question is particularly urgent because the phrase "RFID 2.0" is starting to gain widespread use. There is now a risk that it will simply be used as a marketing buzzword, with no real substance.

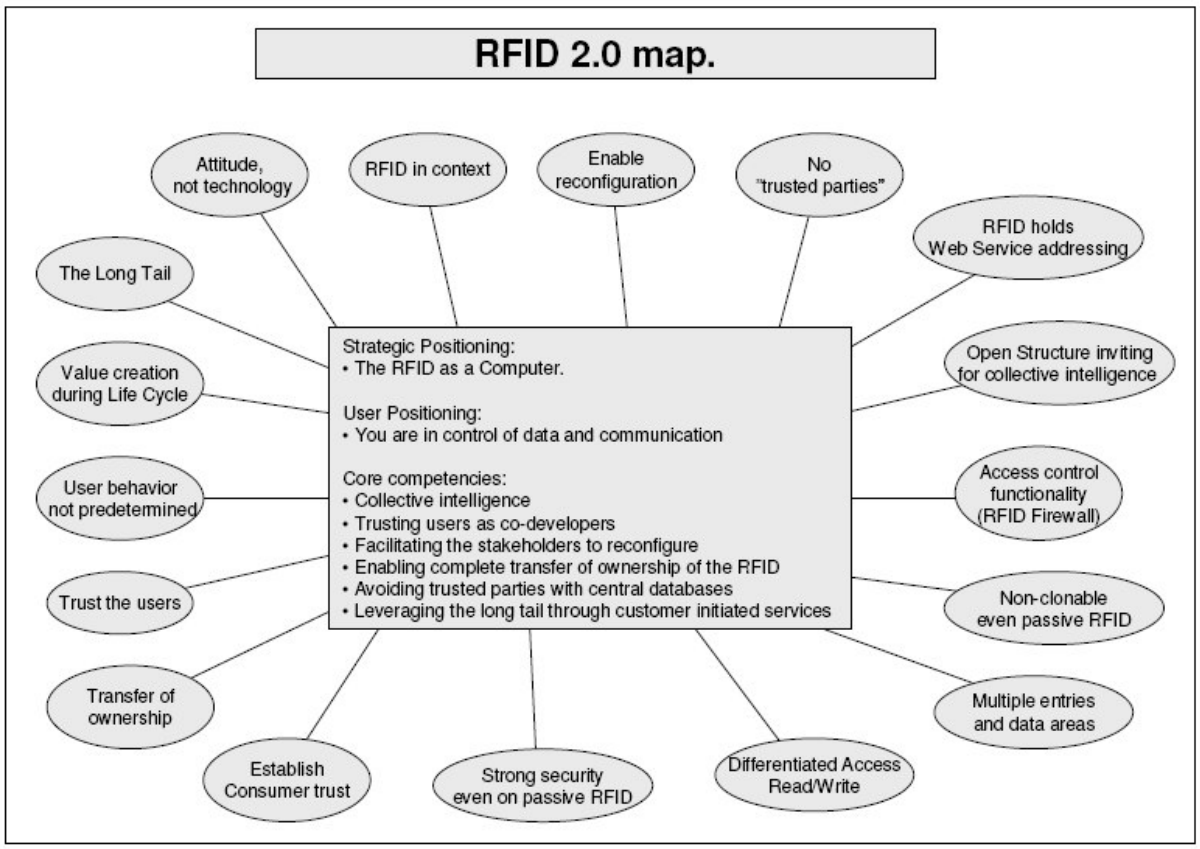
As we start to see RFID readers becoming embedded in PDA's, mobile phones (NFC initiative) and even in products for home medication, it is evident that we must now view the RFID as a computer and perhaps an intelligent storage device. Now is the time for the industry to define the requirements for the next generation of RFID solutions.

When the RFID is a computer, attached to a product, we want to have access to this computer. Since we can't control other readers from getting near to the RFID, unauthorised access must be prevented. We need a 'firewall' and an Access Control System, with multiple access points for clearly differentiated levels of access.

Once the RFID providers have included this level of security on the RFIDs, we can start using them throughout a product's complete life cycle, in a truly collaborative way. The RFID will then be 'context aware' and can be used for multiple purposes during the product's lifetime, right through to end of life and its eventual disposal.

RFID 2.0: The RFID as a Computer

RFID 2.0 can be visualized as a set of principles and practices that link together to form a complete 'ecosystem'. As with other important concepts, RFID 2.0 doesn't necessarily have rigid boundaries, but it does have a central core, within which the principles are defined.



The figure above shows a schematic defining the key elements of RFID 2.0.

The first element defines the RFID as a computer. The second element states that the owner of the RFID will have complete and exclusive control of the data as well as its communication. We at **RFIDsec** regard these two elements to be fundamental in the definition and strategic positioning of RFID 2.0.

Core competencies are also listed above. A clear, well-defined, relationship with the ultimate end-users is fundamental for successful deployment of RFID 2.0.

Core RFID 2.0 Design Elements

1. Open Structure
Standardisation within industries of product identifiers, data structures and data definitions, is vital for the use of RFIDs in a collaborative manner. However, central management of communication will prohibit more flexible user-driven usage. Therefore: The ability to erase data, create new entries, change the product identifier and set up communication channels to web services should be provided to the owner of the RFID; industries should be able to implement their own standards.

2. Strong security
The communication between the Reader and the RFID is wireless, hence the communication can be eavesdropped, recorded and replayed. Using RFID technology for personal identification is a severe problem (Access to buildings, e-Passport etc.). We believe AutoID should not be used for personal identification at all. Also, in product identification, AutoID can be problematic due to e.g. industrial espionage, and even terror threats (transport of explosives etc.). Therefore: The communication between Reader and RFID should be secured in a way that cannot be eavesdropped, so that the communication flow is unique for each transaction and can never be reused.

3. Differentiated Access
When the RFID has a memory space in addition to the product identifier, the impossibility of controlling access to the data is a problem, and is prohibiting companies from storing data on the RFIDs. Therefore: Access control functionality must be provided. In addition to preventing unauthorised access to data on the RFID, it should be possible to have one user authorised to update the data while other users can only read it. It should also be possible to structure the memory space into separate areas, each area with its own differentiated rights of access.

4. Transfer of ownership
RFIDs on products where the users of the product can not access the information and cannot control other people's access limits the use of RFID technology today. Therefore: Complete transfer of control to the next owner of the RFID (the owner of the product) enabling the user to control the communication with the RFID as well as the communication back to any previously established web services is needed. Expanding this transfer of control to include the end-user, whether as a business or as a consumer, will help to establish the level of trust that is needed.

5. Non-clonable even on passive RFID
RFID is an obvious technology to use in combating counterfeit products, but when the RFID can be cloned it is not effective and will provide a false feeling of security. Therefore: The ability to check an RFID's authenticity at any given time during the product's life is a necessity. A product manufacturer should provide this service, with assistance from the RFID manufacturer.

6. The Long Tail
A product manufacturer's investment in RFID technology can be significant, and holds back the use of the technology, because today it can not always be fully justified. Therefore: Promote customer self-service, exploiting the RFID, to reach out to the product's end-users, thereby adding value with a pay-per-use approach.

Summary

RFIDsec believes that we are now at the beginning of the second wave of RFID use. The first wave has concentrated on barcode replacement, in an environment with only basic international standards agreed, which has lead directly to some difficulties in justifying the cost of deployment.

RFID 2.0 extends the horizons dramatically. By viewing the RFID as a computer, and by ensuring that the RFID owner has complete and exclusive control of data and communication, a whole new range of applications across many industry sectors becomes feasible. The RFID industry must now solve the growing privacy and security challenges, by developing appropriate solutions.

We at **RFIDsec** are excited by the prospects of RFID 2.0. We are certain that the time is now right for our industry to exploit the potential that RFID 2.0 offers, and to enable applications that were previously too futuristic, or too expensive.

Henrik Granau
CEO, **RFIDsec**
henrik.granau@rfidsec.com