

Dear members,

This month, we dedicate the entire Newsletter to an interesting security technology - zero knowledge proofs. We feel this technology could be a real contribution in solving the privacy issue for RFID.

Zero knowledge proofs

An interesting new approach to the privacy problem with RFID recently came to our knowledge. In Denmark, Stephan Engberg of Open Business Innovation has proposed a solution to the privacy issue that combines both the 'trusted third party' approach that underlies the EPC infrastructure, and the peer to peer approach of "trust communities" like PGP. However, the cryptographic technology applied is different from the public key scheme used by PGP. It is called "zero knowledge proofs". Stephan Engberg has presented about the benefits of this technology to the EU Security Taskforce, and a company called RFIDSEC has licensed the technology and is bringing products to the market.

What is the concept? The main point in this approach is to enhance RFID chips with additional cryptographic functions supporting "zero knowledge" identity proofs. The RFID chips should have two operating modes: "EPC mode", and "privacy mode". When the tagged goods are in the B2B supply chain, the tags operate in EPC mode and provide all the benefits that companies would want in their logistics operations. When the goods pass to the consumer at the Point Of Sale (POS), the tags are told to switch to privacy mode. From that moment on, the consumer is in control of how the tag operates, and can choose to let the tag keep silent (equivalent to a situation where a "KILL" command was issued) or have it give its 'identity' in controlled situations like warranty servicing or recall. However, no privacy related information is revealed in such situations, and any consumer data related to the tag can remain completely invisible.

How does that work? Let's give some details. The "zero knowledge" approach is a concept from the world of cryptography. It is a mechanism for identification and authentication that does not require any knowledge to be made available to the other party. The way it works is through an interactive protocol, where the "prover" P (who asserts that she/he is P) repeatedly responds to a certain challenge that the "verifier" V (who wishes to verify that the prover actually is P) poses to P. The protocol can be repeated as often as V wishes, until V is assured that the probability of the prover not being P is negligibly small. The protocol is applied in cryptography, which is the technology most often used in authentication, e.g. shared key or public key mechanisms, or zero knowledge proofs.

The following parallel is often used to explain how this works. You may skip the next two paragraphs if you are only interested in what it means, not how it works.

Suppose there is a cave, and at the back of that cave there is a tunnel starting at gate A and ending at gate B (or vice versa, depending on what gate you enter...) In the middle of that tunnel there is a door that can only be opened with a special key. Now P wants to convince V that he has the key, but he does not wish to give any information about that key itself - that is, he does not wish to show that key. Using the zero knowledge protocol, V will ask P to go into the cave and enter into the tunnel through either gate A or gate B. When P is in the tunnel, he will shout out to V that he may enter the cave. Now V will ask P to come out from a specific gate, say gate B. If P does not know the password for opening the door in the middle of the tunnel, there is only a 50% chance that he can come out at the requested gate. This procedure is repeated as often as V

wishes, until he is convinced that the chances are too small for P to come out repeatedly at the requested gate – or is convinced that P is a fraud because he comes out too often from the wrong gate...

You may have noticed that this key could be someone's private key from a public/private key pair such as used in asymmetric cryptography applications. A private key can be used as an identity assertion, yet you will never want to expose your private key itself. Using a zero knowledge protocol, this can be achieved, as has been explained by the above example.

The interesting thing about this approach, it that is is very unlike the EPC infrastructure, that relies on an ONS that is globally centralised. The “EPC discovery services” use locally synchronised indexes on the ONS for identification purposes. What are the main differences from the EPC approach on identification and authentication?

First of all, the zero knowledge approach has an innate limitation – it cannot make any additional information available above and beyond the identity assertion that is being made. Therefore it is very suitable for authentication purposes (which are an essential ingredient of secure applications of RFID) but cannot be used for the other things you want to do with RFID.

Second, the EPC approach is not fully interactive: it relies on a centralised data repository that holds ID's, the ONS (object name service). At the local level, “EPC discovery services” use an indexing mechanism on locally replicated subsets of the ONS repository. The EPC approach presupposes a considerable infrastructure to function. Zero knowledge protocols are interactive by nature and (when implemented in software) don't require any infrastructure beyond a computer to run on.

Third, the EPC approach is not 'zero knowledge' – in order to authenticate a tag, data exchange with at least an index of valid tag ID's is required, and there is no control over the amount of information that might be made available through that index. In fact, much effort is currently being put into developing 'information hubs' that would store all information that gets collected during a tag's life.

Finally, the EPC approach is less robust. In any zero knowledge protocol, the verifier V can decide the “threshold of trust” he wishes to use: if a million repetitions of the challenge are needed to convince him of P's identity then the protocol will be repeated a million times. This means that in a zero knowledge approach, an arbitrarily high level of robustness can be reached – limited only by the time and the computing resources that can practically be made available. So in high security applications, the zero knowledge approach can be made to scale to the desired level of (dis)trust.

Where does this all lead to? How can zero knowledge proofs help in solving the privacy issue in the application of RFID? In summary, the technique could solve issues of identity theft, and of counterfeit.

The proposed solution is to use RFID chips that combine the strengths of two approaches, both EPC and zero knowledge. The idea is to have three keys in the RFID tag: a manufacturer key (EPC, to be used with the infrastructure services of ONS and EPC-IS), an owner key, and a group convenience key. When a tagged product is bought, upon finishing the POS transaction the seller issues a “transfer” command to the tag and forwards a one-time key, which now belongs to the owner. The tag enters into “privacy mode” and only responds to the owner. The consumer *and* the seller can now check the tag – if it still responds to the seller's reader then either the transfer was not issued (privacy violation), or the consumer has not yet paid (theft control). So the interests of both the seller and consumer are covered.

As to other security related issues, it seems that most of these can be solved with this approach, too. Counterfeiting can be tackled by the authentication application. Eavesdropping is tackled by encrypting all data traffic between tag and reader. Traffic analysis will yield no information when there is only zero knowledge communications. Privacy is protected as the consumer is in control of the tag after he has received the "owner key" and the tag has switched to "privacy mode".

What is the impact on any existing investments in reader infrastructure? According to Engberg, the setup can use existing readers and infrastructure. Most if not all readers will be or are software upgradeable, and only those readers that are needed to support the zero knowledge security scheme would have to be upgraded – usually at the POS in shops, and not in DC's, warehouses or production areas.

All in all, this seems to be a very good example of one of RFID Society's principles for acceptable use: "fitness for purpose" – meaning that an RFID system should be designed in such a way as to preclude any unwanted use of the system. The concept is to have "privacy by design".

After these positive words, please be sure that we don't have any commercial ties to OBI or Stephan Engberg. The only reason we cover this topic in this Newsletter is that we really *do* think that this is a very interesting approach to the privacy problems related to item-level tagging. We have seen retailers shy away from item-level tagging and focussing on pallets and cases, partly because of systems complexities involved in item-level tagging, but certainly also partly because of the consumer attitude regarding the privacy issues with item-level tagging. A focussed marketing approach will be needed to convince the public of any technology that has threatening aspects – there will have to be real benefits from RFID, and it must be somehow 'self-evident' that the security techniques applied really work, in order for the legitimate fears and concerns to be taken away.

On a final note, please be aware that trying to make a complex subject matter seem simple – as we have dared to undertake in this Newsletter – necessarily implies removing some of the details.

You may find more information on the technologies discussed here at the following links:

The homepage for Stephan Engberg's company is <http://www.obivision.com/>

Information on the EU Security Taskforce can be found at <http://www.securitytaskforce.org/>

The presentation that Stephan Engberg gave for the Security Taskforce is at http://www.securitytaskforce.org/dmdocs/workshop2/stephan_engberg.pdf

Technical backgrounds on zero knowledge: http://www.obivision.com/Papers/PST2004_RFID_ed.pdf

A presentation that summarizes it: http://www.obivision.com/Papers/PST2004_RFID_slides.pdf

The company that licensed the technology is RFIDSEC: <http://www.rfidsec.com/>

Events

- on September 22/23 the **Antenna Systems Conference** is organised in Santa Clara (CA, USA) by Webcom Communications. You can visit their website at http://www.antennasonline.com/ast_conf2005_index.htm for more information. For members of RFID Society, a reduced registration fee of \$595 applies.
- on September 26/27, Marcusevans is organising the **Total Logistics & Supply Chain 2005 Conference** in Dubai, United Arab Emirates. You can visit their website at <http://www.tls-me.com/> for more information. Members of RFID Society are eligible to a 10% discount.
- on September 26/27, Oxford International is organising the **RFID Technology Conference** in London, UK. It will be its third successful supply chain event. You can visit their website at <http://www.rfidtechnologyconference.com/> for more information. Members of RFID Society are eligible to a 15% discount on the entrance fee.
- on 17, 18 and 19 October IIR (Institute for International Research) organizes the **Track and Trace Summit** in Miami Beach (FL USA). You can visit their website at <http://www.iirusa.com/trackandtrace/index.cfm/newsection=yes/brochurekeycode=XE2003> for more information. Members of RFID Society are eligible to a 20% discount on the entrance fee. Please use priority code: XE2003RFS
- on October 18/19, Marcusevans is organising the **Transport, Logistics and Supply Chain Conference** in Shenzhen, China. You can visit their website at <http://www.marcusevanscongress.com/conghtml/congdetailportal.asp?eventid=9688&pageid=133&area=1&LangID=0> for more information. Members of RFID Society are eligible to a 10% discount.
- International Business Events is organising the **APTS Conference** on November 8-9 in London (UK). APTS offers high-level conferences, an exhibition of the latest products and services, a free workshop programme, the inaugural APTS dinner plus a host of networking opportunities. You can visit their website at <http://www.aptsexpo.com/> for more information.

As always, we welcome your comments and feedback.

Best regards,

Ralph Goossens

Frans Lambi

Founders, RFID Society