

From : Jan E. Hennig [jhennig@rvs.uni-bielefeld.de]

To: MARKT PRIVACY-CONSULTATIONS

Subject: Consultation on RFID Working Document 105

EU Article 29 Data Protection Working Party
Consultation on RFID Working Document 105

Germany, March 31, 2005

From Bernd Sieker and Jan Hennig, RVS Group, University of Bielefeld

The RVS Group [0] (German: AG RVS - Arbeitsgruppe Rechnernetze und Verteilte Systeme - Networks and Distributed Systems Research Group) is headed by Prof. Peter B. Ladkin Ph.D. and performs research and teaching in:

- Failure analysis and accident analysis of complex, heterogeneous, open systems
- System safety analysis and forward engineering
- Specification and verification of system requirements, designs and implementations
- Computer and telecommunications networking, particularly practical security

The Article 29 Data Protection Working Party has expressed wish for comments [1] on the "working document 105 on data protection issues related to RFID technology" (WP105). We hereby refer to the english version of the document available at [2] unless stated otherwise and would like to obey with this statement.

Overall the WP105 is a comprehensive account of the topic. We would kindly suggest to take the following points of constructive criticism into consideration:

a) Ticketing

RFID tags used for ticketing is a major application with a vast possibility of privacy implications. A usual citizen does not have much of a choice not to use the tickets offered. If e.g. the railway tickets were to be equipped with RFID tags a major means of transportation would not be usable without RFID. In Germany the tickets for stadium access for the football world championship 2006 are to be equipped with RFID tags with personal information expressively to enable individuum recognition. There are no other kind of tickets. Anyone willing to see a match is forced to use and carry a RFID-equipped ticket containing personal information. The infrastructure that is now being built will most probably be used after the championships. With rail tickets the enforcement would be similar as for a majority of people other means of transportation would not be usable.

To be a threat to privacy there is no need for personal information on the ticket itself. Learning that this is e.g. a monthly ticket would probably be enough for an eavesdropper to conclude that he will most likely be able to encounter this person nearby the train station every day - even if he/she reads this somewhere else tag, e.g. at the market.

The WP105 only mentions this application as a side note. We would suggest to use a fourth example with ticketing in section 3. The

existing three examples are well-chosen, the ticketing example should not substitute one of them.

b) Passive eavesdropping

The section on the possibilities of learning of a communication between RFID reader and RFID tag by means of eavesdropping should take into account that eavesdropping can also be done passively without a reader device used by the eavesdropper him/herself. While the scenario with actively using a reader device should be clearly visible, an eavesdropper could use a device to listen to a regular reader-tag-communication from a distance.

The argument that RFID tags can be designed to be only readable from a short distance, e.g. 10cm, and would thereby be safe to privacy implications is weak because of not considering this form of eavesdropping. The signal from a regular communication of such tags can very well be recognised by a hidden device that is several meters away. In c't magazin issue 5/2005 p. 85 [4] Harald Kelter writes about this kind of attack and successful experiments.

c) Tag presence detection implications, Privacy Enhancing Technologies

The WP105 only weakly references the possibilities to track a person by nothing else than the presence of one or more RFID tags carried. We believe that this can be used to harm a persons privacy without the person knowing. The only solution to this problem would be to ensure that the tags will remain quiet unless they receive an allowed authorisation sequence or to entirely disable ("kill") the tags.

While the kill method is obviously not usable for RFID usage afterwards, there is a solution to make the tags remain quiet until activated by a secure activation code. Such a concept is put forward by Stephan Engberg et al, Open Business Innovation, Denmark [5]. They use a zero-knowledge-authentication approach for their Privacy Enhancing Technology (PET) concept. We have scrutinised several PET concepts for their conformity with privacy and data protection demands [6]. Even though no concept could solve or avoid all implications the most advanced concept is from Stephan Engberg et al and it is currently the only one to solve the presence detection issue.

PET only plays a small role in the WP105, although it is the only means available to ensure at least basic privacy requirements technically. We suggest to include a section on PET including that research has to continue and should be funded.

d) Active protection means

Apart from PET the only protection means designated by the industry involve active participation by the citizens. Examples are using manual deactivation devices after the point of sale, using blocker tags to flood reader-tag-communication, using metal foil to wrap around items containing live tags. We are of the opinion that, apart from poor usability of the suggested means, no action should be required by the citizen to protect his/her privacy. There are possibilities to ensure this (e.g. the PET proposed). We kindly suggest to include a statement against the necessity of using active protection means. Privacy must be the default, enhancements the option.

e) Translation of PET

We regard a small but important part of the existing translation to German language as weak (referring to the paper available at [3]): In section 5.2 passage 4 in the last sentence the term "nature of PET technology" (with PET standing for Privacy Enhancing Technology) is translated as "Art datenschutzfreundlicher Techniken". We would kindly suggest to use "datenschutzsteigernde und privatsphaerenschuetzende Technologien" to express the original meaning of PET more precisely or use "PET" as mnemonic reference to the technical term and explain it using a footnote or similar construction. As stated above, PET as technical term lacks introduction in the English language version, too.

f) Delayed linking implications

The WP105 mentions the possibilities arising from collecting data from tags from persons shopping but unknown to the shop owner. However, the final step could be expressed more clearly.

In this example the shop owner is collecting data from RFID tags a customer carries into his/her shop. He/she does not know about the customer yet. On the next visit a RFID tag is recognised again and used as key reference. The customer avoids using card payment and feels safe from being identified by the shop that openly shows its RFID equipment. But one day, e.g. because he/she does not have enough cash in his purse, the customer needs to use his/her credit card. He/she would most likely assume that only data from his/her visit when he used his credit card could and would be collected. The arising problem is, that the shop owner can link the identity to not only the last visit where the customer revealed his identity but also to all the earlier visits, forming a huge personal profile. The customer does not know about this. He/she probably would and could not even imagine that a single card payment would have such consequences and therefore not intervene or make use of his/her rights to be informed about the data stored about him. This possibility of delayed data linking goes against the principle of utmost good faith: a usual customer would only assume that his/her actual actions (card payment) would lead to data collection linkable to him/her.

g) Currency

There is a passing mention on RFID tags to be embedded into currency. We are of the opinion that this involves many problems already addressed of the points stated above, e.g. a thief could pick the most valuable pocket after learning about its contents wirelessly. The loss of the anonymity of cash transactions is a major privacy implication on its own. We suggest that the WP105 could be updated to mention these problems.

h) Hiding

The problems arising from hidden tags and readers are - in our opinion - not expressed strong enough. Law alone does not protect the citizen's privacy if it is made as easy as with RFID to read information without the citizen being able to notice it. RFID technology increases the temptation to do hidden data collection. Only few, complex and active means exist to monitor data collection. Ordinary citizens will not be able to use those means. Without knowledge the law won't be applied. We consider this a shortcoming of current law and therefore kindly suggest within the WP105 next version to demand law extension to prevent RFID products to be produced without means for privacy protection, e.g. PETs, scientifically proven to be working. Because of the experience in other areas we do not think that industry

self-regulation would suffice for RFID.

i) Main components

The WP105 describes the main components of RFID technology to be a tag and a reader device. There is a third part: The unique identification number (UID) is the "ID" part in "RFID" and, thus, part of the whole system by definition. With this all RFID applications include the potential for data protection concerns. The caption of section 3.1 and the following text are about "information linked to personal data". Because of the UID and implications as described in f) we would kindly suggest to rethink the section to deal with information that is "linkable" to personal data.

j) Demands from civil rights and data protection groups

Last but not least, there is the outstanding demand by several privacy organisations [7] to perform a technology assessment. "RFID must be subject to a formal technology assessment process, sponsored by a neutral entity [...]. The process must be multi-disciplinary, involving all stakeholders, including consumers." Perhaps the EU commission could be motivated to address this open and yet unanswered demand and act as a neutral entity for within Europe including the provision of resources.

[0]

<http://www.rvs.uni-bielefeld.de/>

[1]

http://europa.eu.int/comm/internal_market/privacy/workinggroup/consultations/consultation_en.htm

[2]

http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf

[3]

http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_de.pdf

[4]

c't magazin, issue 5/2005, Heise Zeitschriften Verlag, Hannover, Germany, ISSN 0721-8679

[5]

<http://www.obivision.com>

[6]

http://www.rvs.uni-bielefeld.de/publications/Reports/PETC_RFID_Scrutinised.pdf

[7]

http://www.spychips.com/jointrfid_position_paper.html