Privacy Checklist for Privacy Enhancing Technology Concepts for RFID Technology Revisited

Bernd Sieker, Peter B. Ladkin, Jan E. Hennig
RVS Group, University of Bielefeld
{bsieker|ladkin|jhennig}@rvs.uni-bielefeld.de
in cooperation with FoeBuD e.V. and Causalis Limited

13 October 2005

Contents

1 Abstract

In [1] we proposed a checklist with which privacy-enhancing technologies for the deployment of Radio Frequency Identification (*RFID*) can be evaluated. The main focus lies in the reliably guaranteed protection of the privacy of citizens. The list has since found resonance in the community, e.g. it has been cited by Ziekow and Spiekermann (forthcoming), see also [2].
We have updated our list to clarify certain checkpoints. Because of the increasing public interest in RFID technology and associated risks in German-speaking countries we also provide a German translation.

2 Updated Privacy checklist (English version)

This is the English version of our updated checklist for privacy-enhancing technologies.

The Privacy Enhancing Technology (PET) concept ...

a. enforces making sparing use of data?
b. makes privacy the default?
c. transfers control to citizens?
d. sends tags to a secure mode automatically?[1]
e. can prove that automatic activation of secure mode always works?
f. prevents eavesdropping of tag-reader-communication?
g. protects citizens from producer?
h. protects citizens from retailer?
i. protection includes in-store problem?
j. protects tag in secure mode against presence-spotting?
k. does not require citizens to take active protection measures?
l. does not interfere with active protection measures?[2]
m. avoids creation and use of central database(s)?
n. avoids creation and use of databases at all?[3]
o. enables functionality after point-of-sale in a secure way?[4]
p. can be achieved without changing RFID physical technology?
q. does not make tags much more expensive?
r. does not make tags more expensive?
s. does not introduce additional threats to privacy?
t. introduces additional benefits for privacy?
u. provides benefits for the retailer?

[1] unsafe tags are disabled forever („killed“) automatically
[2] e.g. using blocker tags. Active protection measures are controversial but there should be no loss in privacy protection through interference with other privacy protection
[3] databases allowing to create associations between objects and people either directly or indirectly
[4] e.g. intelligent fridges or washing machines

We changed the sense of some items to make a consistent checklist in which a checked mark means “good”. In the original list some points had to be checked and some left unchecked to denote the positive sense.

a. Making sparing use of data shall not just be a nice-to-have, but shall be enforced by the design of the PET concept.

b. It is not sufficient only to demand certain default settings; citizens’ privacy protection must be the fundamental principle of the PET concept.

   In particular, applications that might affect a citizen’s privacy must require explicit permission and activity from the citizen. If no action is taken there must not be any privacy violation.

c. In particular citizens must be given complete and exclusive control of every tag that they carry, or that can otherwise be related to them, where today the manufacturer and retailer have this control.

e. We changed the wording slightly to make it less ambiguous. It must be possible to prove rigorously that the system used for deactivating the tags will *always* deactivate *every* tag and that this system cannot be circumvented by the producer or the retailer.

i. The "in-store problem" describes the situation inside the store where citizens may carry RFID-tags and may be tracked, before any tags will be decativated at the point-of-sale.

j. We made it clearer that only disabled tags (tags in "secure mode") shall be undetectable.

k. Since there has been some discussion about the meaning of "active" measures, we rephrased this item to state the intended meaning more clearly.

Certain kinds of protective measures force citizens to take action in order to protect their privacy. These measures might be called "defensive". Although this reflects a valid angle, we decided to emphasise the aspect of avoiding the necessity of active protection measures, i.e. measures that require action in order not to have one's privacy invaded.

l. We changed the wording to make it consistent with item k. It should be noted that it is not enough only to demand that the technology not inhibit the use of existing active protection measures but the technology must not interfere with such active measures to a lesser degree.

m.–n. It is neccessary to mention both the creation and the use of central as well as locally constrained databases.

Because it is hard to control what happens to the data after the creation of a database, it appears unwise to allow creation of databases and subsequently try to restrict their use. On the other hand it is not sufficient only to prohibit the creation of databases because that would permit the use of already existing databases.

Distinguishing between central and local databases may prove useful in cases where local databases cannot be avoided but a central database is not necessary to allow a more fine-grained evaluation of the concept.

p. If a concept cannot be implemented technically it becomes irrelevant. Although this point is not in itself related to the protection of privacy it is important because otherwise all other aspects are moot.

t. We changed the wording to keep the grammar consistent

u. as with item t. A concept that does not gain acceptance with the retail industry will most likely not be successful.

3 Aktualisierte Pivatsphärenschutz-Checkliste (Deutsche Version)

Dies ist die offizielle Übersetzung der privacy checklist (siehe [1]) durch die Autoren und sollte bei Verwendung in deutschen Veröffentlichungen als autoritativ angesehen werden.

Ist das Privacy-Enhancing-Technology-Konzept (PET-Konzept) so geartet, dass ...

a. es Datensparsamkeit erzwingt?
b. es auf der Durchsetzung des Daten- und Privatsphärenschutzes als Grundsatz basiert?
c. es dem Bürger die Kontrolle über die Technik überträgt?
d. es das Tag automatisch in einen gesicherten Modus versetzt?[1]
e. es nachweisbar sicherstellt, dass das automatische Versetzen in den gesicherten Modus immer stattfindet?
f. die Kommunikation zwischen Tag und Lesegerät abhörsicher ist?
g. es den Bürger vor dem Hersteller schützt?
h. es den Bürger vor dem Handel schützt?
i. es den Schutz des Bürgers im Laden einschließt?
j. die Anwesenheit eines Tags im gesicherten Modus nicht erkannt werden kann?
k. es keine aktiven Schutzmaßnahmen vom Bürger erfordert?
l. es aktive Schutzmaßnahmen nicht behindert?[2]
m. es die Entstehung und Nutzung zentraler Datenbanken vermeidet?
n. es generell die Entstehung und Nutzung von Datenbanken vermeidet?[3]
o. es die Nutzung von Funktionalität nach dem Kauf in sicherer Weise ermöglicht?[4]
p. es mit bestehender RFID-Technologie umgesetzt werden kann?
q. dadurch die Tag-Kosten nicht erheblich steigen?
r. dadurch die Tag-Kosten gar nicht steigen?
s. dadurch kein weiterer Nachteil für die Privatsphäre entsteht?
t. dadurch eine weiterreichende Verbesserung der Privatsphäre erfolgt?
u. davon der Handel profitiert?

[1] Tags ohne sicheren Modus werden automatisch endgültig deaktiviert („zerstört“)
[2] z.B. Benutzung von Blocker-Tags. Aktive Schutzmaßnahmen sind umstritten, dennoch sollte sich aus ihrer Benutzung keine Beeinträchtigung der Schutzwirkung anderer Schutzmaßnahmen ergeben
[3] Datenbanken, die eine Zuordnung zwischen Objekten und Personen, auch indirekt, ermöglichen
[4] z.B. intelligente Kühlschränke und Waschmaschinen

Wie auch bei der Englischen Version werden wir hier auf einige der Punkte eingehen, und erläutern, warum wir gerade diese deutsche Übersetzung für die passende halten, insbesondere auch in einigen Fällen, warum bestimmte alternative Übersetzungen unpassend sind.

a. Datensparsamkeit sollte nicht nur ein wünschenswertes Ziel sein, und möglicherweise durchgesetzt werden, sondern das Grundkonzept so ausgelegt sein, dass die sparsame Erhebung und Verwendung von Daten erzwungen wird.

b. Das Englische Wort *privacy* impliziert mehr als nur Datenschutz, daher ist es zu schwach, nur datenschutzfreundliche Voreinstellungen zu forden; vielmehr soll der Grundsatz des

Schutzes der Privatsphäre der Bürger die Basis des gesamten Konzepts sein. Dies bedeutet insbesondere, dass Anwendungen, die die Privatsphäre beeinträchtigen können, explizites Einverständnis und besondere Aktivität seitens des Bürgers erfordern müssen. Wenn er sich gar nicht darum kümmert, darf keine Beeinträchtigung der Privatsphäre stattfinden.

c. Die Wortwahl *überträgt* (statt *gibt*) betont die Mündigkeit des Bürgers, und unterstreicht die Tatsache, dass bei bestehenden Anwendungen die Kontrolle noch voll in der Hand der Hersteller und Anwender (z. B. Einzelhandel) liegt, diese aber für ein funktionierendes Konzept zum Schutz der Privatsphäre an den Bürger übertragen werden muss.

e. Gemeint ist hier nicht, dass jeweils im Einzelfall nachgewiesen werden soll (oder kann), dass ein individuelles Tag deaktiviert wurde, sondern dass ein rigoroser Nachweis geführt werden kann, dass das zum Deaktivieren der Tags verwendete System *immer alle* Tags deaktiviert und insbesondere nicht vom Hersteller oder Handel unterlaufen werden kann.

k. Man kann bestimmte Arten von Schutzmaßnahmen, bei denen die Bürger selbst für die Abwehr der Gefahren sorgen müssen, als „defensiv“ bezeichnen. Obwohl dies im Prinzip einen richtigen Aspekt widerspiegelt, haben wir uns entschieden, das Vermeiden der Notwendigkeit aktiver Schutzmaßnahmen hervorzuheben, also jener Maßnahmen, bei der der Bürger etwas unternehmen *muss*, um nicht in seiner Privatsphäre eingeschränkt zu werden.

l. Die Forderung nach Störungsfreiheit reicht noch etwas weiter als die Forderung, das anzuwendende Konzept dürfe nicht solche aktiven Schutzmaßnahmen ganz unterbinden.

m.–n. Es erscheint notwendig, sowohl auf die Entstehung (bzw. Erzeugung) als auch auf die Benutzung, sowohl zentraler, als auch lokaler oder regional beschränkter Datenbanken hinzuweisen. Wenn nur die Benutzung solcher Datenbanken verhindert werden soll, kann nach der Erzeugung einer solchen Datenbank kaum noch kontrolliert werden, was mit den Daten geschieht. Die Versuchung einer Nutzung erscheint zu groß. Andererseits reicht es nicht aus, nur die Erzeugung zu verhindern, denn das lässt die Möglichkeit offen, bestehende Datenbanken zu verwenden.

Die Aufteilung in zwei Punkte für zentrale und dezentrale Datenbanken kann sinnvoll sein, wenn sich im Einzelfall herausstellt, dass nur der Einsatz von zentralen Datenbanken vermieden werden kann, nicht aber der von lokalen. So kann die Qualität des Konzeptes detaillierter evaluiert werden.

p. Ein Konzept zum Schutz der Privatsphäre ist hinfällig, wenn es nicht technisch machbar ist. Obwohl dieser Punkt nicht unmittelbar zum Schutz der Privatsphäre beiträgt, ist er wichtig, da andernfalls alle anderen Punkte nur noch von akademischem Interesse sind.

u. Hier gilt sinngemäß das gleiche wie für Punkt p., dass ein Konzept, das keine Akzeptanz beim Handel findet, in der Praxis nicht durchsetzbar sein wird.

4 The real Checklist

We will now present the checklists, once in English and once in German, to be used as actual lists for ticking off the individual items that make up a good privacy-enhancing technology concept.

How to use

- Print the checklist and add the name of the concept at the top
- Carefully check if your concept really fulfills each individual point listed in the checklist, and check the circle if appropriate
- Carefully consider what (if any) additional threats and benefits for privacy your concept may introduce and list them on the lines below the checklist proper

The Privacy Enhancing Technology (PET) concept _____ ...

- ◯ enforces making sparing use of data?
- ◯ makes privacy the default?
- ◯ transfers control to citizens?
- ◯ sends tags to a secure mode automatically?[1]
- ◯ can prove that automatic activation of secure mode always works?
- ◯ prevents eavesdropping of tag-reader-communication?
- ◯ protects citizens from producer?
- ◯ protects citizens from retailer?
- ◯ protection includes in-store problem?
- ◯ protects tag in secure mode against presence-spotting?
- ◯ does not require citizens to take active protection measures?
- ◯ does not interfere with active protection measures?[2]
- ◯ avoids creation and use of central database(s)?
- ◯ avoids creation and use of databases at all?[3]
- ◯ enables functionality after point-of-sale in a secure way?[4]
- ◯ can be achieved without changing RFID physical technology?
- ◯ does not make tags much more expensive?
- ◯ does not make tags more expensive?
- ◯ does not introduce additional threats to privacy?
- ◯ introduces additional benefits for privacy?
- ◯ provides benefits for the retailer?

- Additional threats to privacy
  - a. _____
  - b. _____
  - c. _____
  - d. _____
- Additional benefits for privacy
  - a. _____
  - b. _____
  - c. _____
  - d. _____

[1] unsafe tags are disabled forever („killed“) automatically
[2] e.g. using blocker tags. Active protection measures are controversial but there should be no loss in privacy protection through interference with other privacy protection
[3] databases allowing to create associations between objects and people either directly or indirectly
[4] e.g. intelligent fridges or washing machines

Ist das Privacy-Enhancing-Technology-Konzept (PET-Konzept) _____ so geartet, dass ...

- ◯ es Datensparsamkeit erzwingt?
- ◯ es auf der Durchsetzung des Daten- und Privatsphärenschutzes als Grundsatz basiert?
- ◯ es dem Bürger die Kontrolle über die Technik überträgt?
- ◯ es das Tag automatisch in einen gesicherten Modus versetzt?[5]
- ◯ es nachweisbar sicherstellt, dass das automatische Versetzen in den gesicherten Modus immer stattfindet?
- ◯ die Kommunikation zwischen Tag und Lesegerät abhörsicher ist?
- ◯ es den Bürger vor dem Hersteller schützt?
- ◯ es den Bürger vor dem Handel schützt?
- ◯ es den Schutz des Bürgers im Laden einschließt?
- ◯ die Anwesenheit eines Tags im gesicherten Modus nicht erkannt werden kann?
- ◯ es keine aktiven Schutzmaßnahmen vom Bürger erfordert?
- ◯ es aktive Schutzmaßnahmen nicht behindert?[6]
- ◯ es die Entstehung und Nutzung zentraler Datenbanken vermeidet?
- ◯ es generell die Entstehung und Nutzung von Datenbanken vermeidet?[7]
- ◯ es die Nutzung von Funktionalität nach dem Kauf in sicherer Weise ermöglicht?[8]
- ◯ es mit bestehender RFID-Technologie umgesetzt werden kann?
- ◯ dadurch die Tag-Kosten nicht erheblich steigen?
- ◯ dadurch die Tag-Kosten gar nicht steigen?
- ◯ dadurch kein weiterer Nachteil für die Privatsphäre entsteht?
- ◯ dadurch eine weiterreichende Verbesserung der Privatsphäre erfolgt?
- ◯ davon der Handel profitiert?

- Zusätzliche Nachteile fuer die Privatsphäre
  - a. _____
  - b. _____
  - c. _____
  - d. _____
- Weiterreichende Verbesserungen für die Privatsphäre
  - a. _____
  - b. _____
  - c. _____
  - d. _____

[5] Tags ohne sicheren Modus werden automatisch endgültig deaktiviert („zerstört“)

[6] z.B. Benutzung von Blocker-Tags. Aktive Schutzmaßnahmen sind umstritten, dennoch sollte sich aus ihrer Benutzung keine Beeinträchtigung der Schutzwirkung anderer Schutzmaßnahmen ergeben

[7] Datenbanken, die eine Zuordnung zwischen Objekten und Personen, auch indirekt, ermöglichen

[8] z.B. intelligente Kühlschränke und Waschmaschinen

References

[1] *Hennig, Jan; Ladkin, Peter; Sieker, Bernd*: Privacy Enhancing Technology Concepts for RFID Technology Scrutinised, 2004, RVS Group, University of Bielefeld, Bielefeld, Germany, RVS-RR-04-02, available through
`http://www.rvs.uni-bielefeld.de` → Publications → Research Reports.

[2] *Spiekermann, Sarah; Ziekow, Holger*: RFID Technologie und Implikationen, 2004, Project InterVal, Berliner Forschungszentrum Internetökonomie, Humboldt Universität zu Berlin
`http://www.ccc.de/congress/2004/fahrplan/files/482-rfid-slides.pdf`