Pervasive computing – IT security and privacy

1 List of Contents

2 Summary

The protection of privacy is often described as the greatest obstacle to the average consumer's confidence and trust in the technology of pervasive computing when it comes to IT security. It is natural to ask whether this fear is justified, and if so, to what extent; and indeed also what other IT security problems pervasive computing may produce. For this reason, the report "Things That Think" from Technological Foresight in the Danish Ministry of Science, Technology and Innovation recommends that the Danish Council for IT Security carry out an analysis to reveal the *real* IT security problems with pervasive computing.

This report contains an analysis and a mapping of the most important problem areas with IT security in the field of pervasive computing, and an investigation of whether the Danish Act on the Processing of Personal Data ensures a reasonable balance between the possibility of registering information and the necessary protection of personal rights and privacy.

The main conclusions of the report are that the primary IT security problems in the short-term relate to the safeguarding of privacy and usability. The legal analysis concludes that the Danish Act for the Processing of Personal Data is a suitable tool for protecting the right to privacy, provided that the practical elucidation of the rules of the law is continuously updated such that they are realistic in the technologised reality.

In the longer-term, improved technology is expected to help solve some of these problems, and also to form the basis for more advanced uses of personal agents. This introduces new security problems related to the conclusion of binding agreements between agents, and how to deal with trust in other people's agents.

A number of recommendations for dealing with the key problems are given on the basis of this analysis:

- A code should be drawn up for the use of RFID in the retail trade.
- The need for strong encryption of sensitive personal data should be clarified – particularly in connection with the use of units with limited communication ranges.
- Recognised security protocols should be used.
- A "proof-of-concept" project should be implemented to illustrate how some of the problems that have been identified can be dealt with.
- The legal status of agreements concluded by personal agents should be investigated.
- A group of experts should be appointed to follow the development of IT security in the field of pervasive computing.
- The Danish tradition for research in the fields of IT security and usability should be continued and combined.

3 Introduction

3.1 Background

This report has been prepared for the Danish Council for IT Security as a follow-up to the report "Things That Think"[1], which recommends the implementation of an analysis of the security problems linked to pervasive computing.

According to "Things That Think", this report should help to give consumers confidence and trust in the use of pervasive computing, as the report should assess which security-related problems are real, in order to thereby enable a qualified discussion whereby confidence and trust can be created on a solid foundation. Thus, the report does not aim to provide a fully-comprehensive technical or legal presentation of the field, but to form a serious, professional contribution to the technical and legal discussion of the IT security aspects of pervasive computing. This should, in particular, be seen in the light of the fact that the area is undergoing rapid development, both industrially and in terms of research.

The future use of pervasive computing can be described by a number of scenarios, of which some are already a reality, whilst others are unlikely to be seen in the immediate future – and may never be realised. The assessment of the security aspects of pervasive computing will be based on these specific scenarios, as it will in this way approximate the expected use of pervasive computing.

3.2 Pervasive computing

Pervasive computing means that there are computers everywhere[2]. We choose to use the informal definition given in "Things That Think" when we use the term pervasive computing.

In brief, pervasive computing deals with the fact that there are computers everywhere, which is made possible by the technological development whereby chips are becoming smaller and cheaper all the time. "Things That Think" lists various examples of pervasive computing:

- Interactive spaces. In addition to consumer electronics in private homes, this also includes things such as swivel chairs in offices that remember height settings, intelligent fridges that know whether or not the milk is too old, and under-floor heating that is automatically turned on when the forecast is for cold weather.
- Clothes. This includes jackets with in-built mp3 players, sports clothing with in-built heart rate monitors, and glasses with an inbuilt screen. Other examples include intelligent work clothes for groups such as firemen[3].
- Healthcare. Includes intelligent bandages that can report how the injury is doing, and video conferences with doctors, so patients can be treated at home. Another example is doors that open automatically, so the rescue services can come in to a patient with insulin shock.
- The retail trade and production. There are a large number of examples in the retail trade, such as shoplifting prevention systems that work by the product triggering an alarm when it

[1] [TDT].

[2] Related concepts include ubiquitous computing and ambient intelligence. Ubiquitous computing deals with computers that disappear, i.e. they are everywhere, but they are invisible, and ambient intelligence goes one step further and looks at how this can be utilised by "intelligent" applications. In this report we attempt to encompass all three concepts under one hat.

[3] See, for example [IpFireFighter].

leaves the shop, automatic stock-taking, and checkouts without cashiers, where the shopping trolley is pushed through a scanner that registers the products. Researchers are also working on ideas of using RFID to provide warnings to people with allergies, for food safety, for sorting waste, and much more.

- Cars. Computer-controlled brakes, and DVD films and games for passengers are already widespread, as is the use of GPS and direction guides. Solutions offering automatic alarms in places where the road is slippery by means of communication with other cars, and traffic safety initiatives are also underway.
- IT. In this sector pervasive computing offers new solutions such as public printers that can be used via mobile phones, and the automatic storing of personal data such as digital photos. The use of chips in passports is another example.
- Defence. Lastly, there are a number of defence applications such as unmanned planes, tanks and operating rooms, weapons that can only be fired by the rightful owner, etc.

All these applications are based on the many new units with inbuilt computers and communication possibilities, of which we have probably only seen the tip of the iceberg. Pervasive computing typically involves units with a limited IT capacity, i.e. limited resources in terms of CPU power, memory, bandwidth and battery. The most prominent representatives of this include the so-called RFID tags (also called electronic bar codes), but the list of pervasive computing technologies that is in the public domain is already long, and includes such things as mobile phones, PDAs, BlueTooth and much more.

A few supplements to this include examples of modern IT that hover on the periphery of pervasive computing[4]: Normal services on the Internet where information can be accessed from a central database, such as various Internet banking solutions, the use of traditional PC-based programmes for accounts, graphic design, games, etc. This kind of solution does not fall within the scope of this report.

“Things That Think” presents a distinction inspired by Forrester’s[5] definition of ‘the executable Internet’: “*Intelligent applications that execute code near the user to create rich, engaging conversation via the net*”, which we will call *services-in-everything,* and of “the extended Internet”: “*Internet devices and applications that sense, analyse, and control the real world*”, which we will call *agents-in-everything.* A fundamental assumption for this is that units (including clothes, lamps, etc.) are on the Internet, so these definitions can suitably be supplemented with *ID-in-everything*: where all the objects and units we can think of are on the Internet, and can therefore communicate electronically with other units. This also means that each individual unit will be able to be identified[6]. The following list is in order of increasing technological complexity:

- ID-in-everything is characterised by the use of passive units, by which we mean that the units can only report their ID, and possibly raw sensor input. All calculations that do not have anything to do with the reporting of ID are placed in the infrastructure that is used to communicate with. Examples of this include the use of RFID to prevent the shoplifting of clothes, online thermometers and web cams, and a number of other “passive” units.

[4] In practice it can be difficult to give a precise delimitation of the concept of pervasive computing. More traditional solutions will often be closely integrated with pervasive computing solutions. In the same way, it is not obvious whether a traditional computer game played on a mobile phone falls under the category of pervasive computing, either.

[5] See [Forrester].

[6] Not necessarily a unique identification in a global sense. We will deal with this matter in more detail below.

- Services-in-everything is characterised by the use of more active units that can perform calculations and influence their surroundings themselves. Examples of this include a large number of services accessible via electronic communication, such as fridges, heat meters and car engines.
- Agents-in-everything is characterised by units that are not only active, they are also autonomous, i.e. they send data and influence their surroundings on their own initiative. Examples of this include software agents that automatically look for your favourite wine, and automatically order and pay for it (after having asked the bottle – which is also on the Internet – directly about its temperature throughout its lifetime, for example).

3.3 IT security

The following three fundamental properties shall be considered in connection with IT security[7].

Integrity
Integrity is confirmation that no changes have been made to data that has been sent, received or saved. The protection of integrity requires that only users/units with the right of access to data/systems are able to change data. In this way, the authenticity of data that guarantees that this information originates from the source stated will also be of importance.

Confidentiality
Confidentiality means protection from unauthorised third parties gaining access to confidential information.

Availability
Systems and data should be available, and should function in spite of any disruptions. Such disruptions include things such as attacks, accidents, power cuts and natural catastrophes.

An implicit requirement for building secure IT systems in relation to these concepts is that a secure access control can be carried out on the systems – both physically and logically. In connection with integrity, access to the writing/changing of data needs to be controlled, and in connection with confidentiality, access to the reading of data needs to be controlled.

This access control includes both identification (authentication) of the users/units wanting access, and authorisation to get through to the desired data. Identification should here be understood in the broad sense, as it may involve unique physical identification, recognition in a specific context (e.g. using pseudonyms), or proof that the user possesses the rights required to achieve the desired access. The concept of identification as used in this report is therefore not necessarily identification in a unique sense, but is instead *purpose-related*.

A person is often identified by means of PIN codes (or passwords), biometric methods or one-time passwords (e.g. with the help of special tokens). This identification can either be made directly to the system to which the user wants access, or by means of a two-step process where the user first identifies him/herself to a local unit, which then identifies itself to the system on the user's behalf. This is typically done with the help of cryptographic mechanisms such as digital signatures or

[7] See [RFITS].

special identification protocols intended for this purpose. In this second step the unit will thus behave like a trusted unit, where it is implicitly assumed that it will only complete step two if step one was successful. The advantage with this two-step process is that the identification protocol used by the unit can be very secure, and the unit can also potentially be set up so that it only identifies the user to the extent required to obtain the desired access.

User identification implicitly assumes that the user behaves (more or less) as expected. If this is not the case, it can have serious consequences for maintaining the desired security properties. If we put a piece of paper with a password on our monitor, for example, then the value of the access control is already drastically reduced. An important element of security is therefore that the parts that require interaction with the user are usable, which means that the user is able to use them in a natural way, so that normal procedures, etc., are not changed. Usability also means that the user has an understanding of problems related to security, such as the password being personal, etc.

Integrity and confidentiality are guaranteed by a number of mechanisms varying from physical access control to security procedures to the use of cryptography. Mechanisms based on the use of cryptography will often be used in connection with pervasive computing, where physical protection will often only be able to be used to a limited extent.

With regards to confidentiality, it should be mentioned that there has already been a great deal of discussion concerning conditions for safeguarding privacy, and privacy problems have been reported in the media as being the Achilles heal of pervasive computing[8]. Three levels of privacy shall be considered here:

- Anonymity (or confidentiality of identity)
- Protection against location tracking, which provides confidentiality of where we have been
- Linking or data aggregation, which is the linking of different pieces of data that are innocent enough in themselves, but that reveal things when pieced together[9].

Location tracking is a special form of linking. In many cases it cannot be ruled out that a successful tracking attack can lead to the identification of the person, as the linking of a number of events will characterise the person uniquely.

It should be noted here that the installation of systems that improve the safeguarding of aspects such as integrity and confidentiality often lead to a risk of poorer access. If data are encrypted for reasons of confidentiality, for example, they will not be accessible if the key is lost. In the same way, access to data can be lost if a required password is forgotten. In practice such problems are solved by suitable procedures, such as the back up of key material and the possibility of getting a new password. Another example is the use of PUK codes in mobile phones to open up the telephone if we forget the PIN code.

[8] See [IEEEPervasive].

[9] An article in [SPC] explains, for example, how tracking can be carried out using the wireless network card in a laptop computer: assuming that the computer is seen at a particular postal address every evening, and at a certain workplace every day, the identity of the owner can be established with great certainty; if the same laptop computer is now regularly seen at a psychologist’s, for example, then we can draw conclusions – and all this from three pieces of information that are, in themselves, quite innocent.

3.4 Legal regulation

Law and security are connected in the sense that they are both means of achieving certain goals, such as the protection of identity (anonymity). Legal regulation can, however, also make requirements of the technology, and the security connected with this. Legal requirements to pervasive computing may require the availability of certain forms of security.

The legal requirements are, first and foremost, linked to the protection of privacy, and the personal integrity of the individual. These legal requirements include a number of sub-requirements. There must be openness/transparency about the use of the technology. In this respect, openness does not refer to the technical details, but to information about the use of the technology, such as RFID tags. Another requirement is that the individual should have the opportunity to exercise control over the technology. This right to control must, however, be weighed up in relation to other legitimate concerns that may be required by law[10]. A third requirement is that the technology should only be used when it is fair to do so, and in accordance with good practice. The assessment of this will vary from context to context, but important factors include the purpose, and the fact that the data that has been collected is not spread around in all directions, which security can help to prevent. A fourth requirement is that information should not be used to create profiles that can be used to monitor people, for example. Requirements of this kind can be met in various ways, cf. appendices 2 and 3.

It should be added that there may be legal requirements that are not linked to the use of the technology in relation to identifiable individuals, but these requirements will often be able to be met without special security requirements being made.

[10] If it is decided that bank notes should be fitted with RFID, the individual will not be able to have so much control that he/she can choose to use notes without RFID. Another example is passports fitted with RFID.

4 Scenarios and cases

The concept of pervasive computing is broad, and stretches from pure science fiction to everyday things such as mobile phones. A security analysis is a very specific assessment of values and the threats to such values, and in order to bring the concept of pervasive computing "down to earth", so specific values and threats can be identified, the analysis in this report is based on specific scenarios and cases. These are gathered from various research projects, think tanks and industrial applications in the field of pervasive computing.

Scenarios and cases fall into the three groups described in section 3.2:

- ID-in-everything
- Services-in-everything
- Agents-in-everything

The complete scenarios and cases are presented in appendix 4. This section describes the essence of them.

A recurrent element in the scenarios and cases that are described is that IT security is rarely explicitly included. This does not mean that security is not important in these scenarios. On the contrary, the ISTAG scenarios (that are of the agents-in-everything type) stipulate security as being an important element, for example[11], so it is an implicit assumption in the cases and scenarios described that security can be maintained at a desirable level, in a way that does not materially alter the use. In other words, the introduction of security must not reduce the usability.

4.1 ID-in-everything

This level is already commercially widespread. Basically, a facility is offered whereby a unit can identify itself passively (be read by scanners) or actively (by transmitting a signal – possibly controlled by the user). The example that has been commented on most in the press is the use of RFID tags in the retail trade and in production management. Cases with specific applications include:

- Shoplifting prevention systems, see, for example: [electronics.howstuffworks.com/question601.htm].
- Logistics. The idea is basically to put an RFID tag on a product, or, for example, just a pallet with products, so as to be able to control the logistics concerning the shop's stock. This kind of application at Walmart has caused a great deal of comment in the press, but the English supermarket chain, Tesco [www.rfidjournal.com/article/articleview/658/1/1/], and the Danish snacks firm Kims have entertained similar thoughts.
- Tracking of people. KidSpotter [www.kidspotter.com], which is used in Legoland, is a good example of this. Here, children are given an armband with a tag, and if a child gets lost, the parents can find out where in Legoland they are via a text message service.
- Identification of people. The Mexican legal system offers a more exotic example, where employees in the Mexican Public Prosecutor's office have had a chip implanted that is in fact a normal RFID tag from the company VeriChip, which is used to identify employees in connection with their access to confidential documents [www.nytimes.com/2004/10/14/technology/14implant.html]. A less ambitious example is the use of chips in cards that give access to lifts in ski resorts.

[11] See the "socio-political issues" in connection with the "Maria – road warrior" scenario, for example.

In addition to these examples, there are already others, and research is also being carried out on many other applications such as automatic checkout lines where all products are scanned automatically when a shopping trolley is pushed past the checkout, and where the total may even be deducted automatically from the purchaser's credit card.

Although the selection of cases named above focuses on the use of RFID technology, this is far from the only representative of this field. A large number of other technologies are, like RFID, bearers of information about identity, such as magnetic cards, smart cards (such as the new Visa cards), and the SIM cards (which are technically also smart cards) that sit in mobile phones and BlueTooth units. These technologies have a broader application that is dealt with as part of the section on services-in-everything below.

With regards to privacy, the technologies and applications named have the immediate weakness that they all involve unique identification, which could lead to the incorrect conclusion that unique identification is a necessary element. Which it is not. There are numerous proposals for solutions that do not involve unique information, but their commercial application is less widespread.

The key element in ID-in-everything is that units can be identified by being read, i.e. a depiction of physical objects – whether this be objects or people, or objects that represent or that are associated with people, such as a train ticket – in the virtual space.

4.2 Services-in-everything

On this level, units are not just on the Internet, they are also fitted with sensors, actuators and various applications whereby the units are able to offer various forms of services via the Internet. Basically, we can say that systems on this level assist the user in his/her actions. This technology is already partly realised, for example via PDAs, digital cameras and many more things that can communicate, and that are thereby on the Internet in one form or another.

Three scenarios with services-in-everything from current research projects can be listed here:

- EPCiR. Deals with the treatment of diabetic patients with foot wounds at home[12]. The patient is given an "intelligent" bandage that sends various data to a database, and video consultations are also carried out by a chief physician at a hospital, with the assistance of a visiting nurse.
- The European Service Network (ESN) from eu-DOMAIN[13] deals with plumbers who are online via their vans (that automatically pay for parking, road/bridge tolls, etc.), who use virtual reality glasses to study heat pumps (that send data on their condition to the glasses, the plumber's PDA, etc.), and that are able to localise the nearest dealer or colleague who is able to sell him/her any spare parts he/she may need, and can electronically conclude a contract of sale here and now.
- Healthcare for tomorrow (also from eu-DOMAIN): like the ESN scenario, this deals with a mobile worker, but in this case a nurse, which is a bit similar to the EPCiR scenario. Here

[12] This is a serious problem, because the diabetic is unable to feel the wound, which means that there are often complications in the form of infections, for example. In Denmark there are many – potentially unnecessary – amputations for this reason every year.

[13] eu-DOMAIN is the name of the research project sponsored by the EU from which the ESN and Healthcare for tomorrow scenarios originate. In addition to the scenarios themselves, appendix 4 also contains a reference to the homepage for this project.

RFID is, for example, used to keep a check on the patient’s insulin stock, and the nurse is automatically given access to the patient’s home if the patient does not respond when the nurse rings on the door (and if the patient is at home, of course).

The common feature in all these scenarios is that we have three types of units in action. Sensors (on the heat pump, for example) that send data. Actuators that receive instructions (e.g. to unlock the door or turn on the light). (Partially) central units, such as a PDA, or a so-called gateway[14] in the plumber’s van. Different units can have one, two or all three properties, and can communicate via central points or decentrally (i.e. directly with one another). Most units can be accessed by the user either directly or via other units. Moreover, there is great dynamism in relation to which units have to talk to one another, e.g. when the nurse connects a video camera in the patient’s home. In general, however, the systems are relatively closed, so it is known in advance what (types of) units will be involved, and these units will be able to be set up to be able to take part in the system. A slightly old-fashioned, but very widespread, example that is not mentioned in the scenarios, is remote controls for all kinds of electronic equipment. Remote controls are typically part of a closed system, as they are constructed specifically to communicate with a certain type of unit.

It should be noted that usability is seldom mentioned in these scenarios, if at all. This does not mean, however, that it is not important. On the contrary, because the interface between the system and the user is assumed (implicitly) to be of such a quality that the procedures described can take place without further problems. In particular, this means that the parts of the system that can be attributed to security requirements are also expected to be natural in their use, such as user authentication, and the mechanisms required to support the connection of the video camera brought by the nurse, for example.

From a technological perspective, this collection of scenarios has the limitation that it focuses on gateway-based solutions, i.e. communication via a *central* unit. This may be due to the fact that the projects from which the scenarios are taken have a relatively short time horizon, and in the short-term it would appear that solutions based on gateways are those that are closest to commercial realisation. In contrast, the agents-in-everything scenarios described below also deal with decentralised solutions.

Gateways and a large number of other current technologies that can, and will, help to form the technical platform for pervasive computing are described in the book “Pervasive Computing”[15].

4.3 Agents-in-everything

This last group is described in four scenarios drawn up by a think tank under the auspices of the EU. These scenarios are intended as a possible peek into the future, in line with the EU’s vision of ambient intelligence.

- Maria – road warrior. Maria does not need to show her passport when she travels, the system carries out automatic ID checks via her intelligent armband. Her rental car is automatically waiting for her at an assigned place when she arrives. Maria saves an encrypted version of a presentation on a foreign company’s network. It is decrypted when she needs it, and 1½

[14] A gateway is, in layman’s terms, a computer that understands a large number of communication protocols, both short and long range, i.e. it can function as a link between units with a short range and the rest of the world.

[15] [PC].

minutes after her presentation is over, the encrypted version is deleted. During the presentation her telephone is closed down, so that only very important calls are sent through.

- Dimitrios – Digital Me. Dimitrios has an agent, Digital Me, which handles a number of decisions for him. It supplies data about the nearest chemists to another person's agent, because the other person needs the same type of medicine that Dimitrios uses, for example. In this situation, the agent decides that it will not supply information about who Dimitrios really is to the other person's agent; on the one hand this will safeguard Dimitrios' anonymity, but on the other hand it also prevents a personal (human) conversation to clarify any questions. Dimitrios' agent also answers telephone calls in a voice that sounds like Dimitrios', and only lets through calls that it knows that Dimitrios wants.
- Carmen – traffic, sustainability & commerce. Carmen's agent finds a lift for Carmen by contacting other drivers' agents. Whilst Carmen is being driven to work, her agent finds the products she noted down in the morning, orders them and pays for them, and organises delivery to her local corner shop, so that Carmen can just pick them up on her way home. The agent finds a good offer for Carmen's favourite wine, and presents it to Carmen, who decides to buy that as well.
- Annette and Solomon – the Ambient for social learning. "The Ambient" is everywhere in the room where Annette and Solomon follow a training course. The Ambient communicates by means of speech synthesis, and passes on communication between different participants on the course with the help of something similar to video conferences; this involves communication over distances from a few metres to several thousand kilometres.

With the exception of the last one, these scenarios are similar to the services-in-everything scenarios. The major difference – for the first three scenarios – lies in their scope, both globally and locally, and in the fundamental difference that a great deal of the responsibility for decisions is handed over to technology. Globally, in the sense that the technology is found wherever we travel in the world, and locally in the sense that the technology is found everywhere: in armbands, in the local corner shop, in food, in cars, etc. True pervasive computing! The transfer of responsibility consists of a great number of decisions in these scenarios being made by so-called agents. This includes simple tasks such as the answering of telephone calls and calendar functions, and also financial transactions and evaluations about supplying personal data.

From a technological perspective, a number of the functionalities described here will be able to be solved using the same technologies as for services-in-everything. However, the systems described are no longer "closed" in the same sense, i.e. we can no longer restrict ourselves to having to communicate with units that are connected to a "local" system, as is the case in the EPCiR scenario, for example. Moreover, the future may also involve greater use of ad-hoc networks that, unlike gateways, etc., are decentralised network structures.

5 Analysis of current law and the legal considerations and requirements

In order to ensure that pervasive computing is used in a manner that is socially and appropriately beneficial to both individuals and companies, legal regulation is required to support this objective, in addition to good security solutions. This legal regulation can take many forms, but primarily concerns the question of privacy, on which the following and the more detailed account in appendix 2 are therefore centred. The need to ensure adequate privacy is important for people's acceptance, and reception, of the new technologies, and thus also for the commercial utilisation of these technologies.

One of the main questions for the legal analysis in this context is how can we ensure that the individual can avoid becoming transparent, or informationally naked, when pervasive computing spreads, for example by data about the online person becoming accessible to everyone? How can we safeguard autonomy and a socially acceptable right of self-determination for the individual? It is this problem that is considered to be central from the legal perspective, and that is thus linked to the basic right to privacy as stated in article 8 of the European Convention on Human Rights.

When assessing this problem, it is important to distinguish between two situations. The first use of pervasive computing leads to the acquisition of knowledge about, or the surveillance of, people whose identity is not known, whilst the other involves the processing of information about identifiable people. Regardless of the continued spread of identification technology, the first situation will continue to take place, so in order to prevent a general experience of being monitored, it is desirable for rules to be laid down, in both the public and the private sector, imposing a general duty to provide information that such forms of pervasive computing are being used. The second situation is, however, of greater interest, so it is this that is dealt with in the following.

The problem is currently regulated by the Danish Act on the Processing of Personal Data (and a number of sector laws), and the question is whether this regulation, that is primarily based on directive 95/46 EF will continue to suffice when there is IT in everything. In other words, is the Act future-proof[16]? The Act does not commit itself to who owns personal data, but rather to the manner in which they may be processed by the person who has them in his/her possession. Although it may, at first glance, be tempting to assume that the individual owns his/her own data, this is in fact a complex problem that is in no way exclusive to pervasive computing. The consequences of a rule whereby a person owns his/her own data are almost impossible to fathom, so it is best to base the legal analysis on the approach taken by the Act in this context.

One of the key questions is thus whether, in a situation where IT is everywhere, including increasingly in an online world, it will still be possible to determine with certitude who is the data controller who has to observe the legal requirements in specific situations. The increasing flow of data is likely to create difficulties on this point, and may also in some cases make it less reasonable to hold an original data controller responsible for the data. The elucidation of this concept in practice ought therefore to be considered in the future.

A change in practice may also be a good response in relation to other rules of the Act, without thereby implying that they should be formally amended, as described below. The reason for this is

[16] The assessment of this problem does not take into account the somewhat distant future with "agents-in-everything".

that the current rules are formulated in a technologically neutral manner, and that they, in many cases, take the form of legal standards that can be adapted to a changed technological reality.

This is true of the general principles, including those of fairness/good practice, purposefulness, proportionality, data quality and time limits. These principles, which constitute the status of data protection, are well suited to the phenomenon of pervasive computing, but they are also put under pressure by this development. It may, for example, become more difficult to ensure that the original purpose of the collection dictates the actual use of the data, so as to achieve the desired transparency, or to ensure that personal data is not used in new contexts, such that they give a misleading picture of the person. Pervasive computing requires increased awareness in connection with the observance of these principles.

The principle of security will be of key importance in the future. The Act lays down a general requirement for security. It can be established that there is a ministerial order and guidelines clarifying the situation for the public administration, but that there is no such legislation for the private sector, which may give cause for some astonishment. In practice, however, it is assumed that these rules also apply to the private sector. It should be emphasised that data controllers are obliged to lay down adequate rules for security, which must be regularly updated, to pay particular attention when transmitting the information, because sensitive data, such as data about a person's health, have to undergo strong encryption based on a recognised algorithm, and also to pay particular attention when processing personal data outside of a professional environment, e.g. at home. It would be preferable for the statutory security requirements to be continuously adapted to the technological situation, and for them to be communicated as effectively as possible.

In general, it is desirable for the individual to be informed that his/her personal data are being processed with the help of IT. The Act stipulates that information must be provided when data is collected either directly or indirectly. When there is IT in everything, it may be difficult to ensure that this duty is always observed in the case of indirect collection, which will become more and more commonplace. The rule may appear to place a burden on resources, but it is, on the whole, adequate, although an increasing need for supervision of its observance should be expected.

One of the key questions is whether the individual's opportunities for controlling the use of personal data are adequately safeguarded by law. It can be established that the Act enables personal data to be processed on the basis of consent, but that such consent is only obligatory in a few cases. It is difficult to assess this access by consent, because on the one hand consent is an expression of the right of self-determination, but on the other hand it can throw the weak to the wolves. In this context, the consensual right should not stand alone, as the state must still have a duty to protect its subjects' privacy.

All in all, the conclusion of the legal analysis is that the legal task consists of ensuring that pervasive computing becomes a reality in such a way that it continues to ensure the protection of privacy. The Danish Act on the Processing of Personal Data is a suitable instrument for this purpose, but the practical elucidation of the rules of the Act will need to be updated on a regular basis, so that they are realistic in the technologised reality.

6 Analysis of IT security problems

As mentioned in the introduction, the analysis of the security aspects connected with the use of pervasive computing is based on the scenarios outlined in section 4. The potential security threats to these scenarios will be described, and possible methods of protection from some of these will be outlined.

The purpose of a traditional security analysis is to identify threats, and to prioritise them on the basis of the risk they constitute. This kind of risk assessment can be based on two dimensions: 1) how serious will the consequences of realisation of a specific threat be? And 2), how often is the realisation of the threat likely to occur? The more serious, and the more often, the greater the risk is said to be. Such assessments will often depend to a great extent on the technology used, and on empirical studies, but as this report is investigating future technologies and imagined applications, no such inputs are available. This risk assessment will therefore be based on extrapolations of current IT applications, and on evaluations of how difficult the realisation of a specific threat is assessed to be.

The potential threats will be assessed on the basis of existing methods of analysing IT security in organisations and specific IT systems. As described in Octave[17], a threat can be characterised by:

- The asset that is threatened (e.g. personal information)
- The access to this asset (physical or logical)
- The actor threatening the asset
- The actor’s motive
- The outcome of the threat (which may be the compromising of integrity, confidentiality or availability).

It would be too complicated to characterise each and every threat by means of these characteristics here, but they will be used as guidelines in assessing the scenarios. The following description focuses on the outcome of the threats that have been identified, as this gives the most homogenous presentation. A summary of the threats that have been identified is given in section 6.4.

One type of actor does, however, deserve particular attention, and that is the average user, because threats of this origin are not clearly described in the scenarios named. Users who do not behave reasonably in relation to IT security can cause an otherwise well thought-out security policy to break down[18]. Inexpedient user behaviour is thus a recurrent threat that is prevented in a traditional manner, i.e. by training users, and by developing systems with good usability.

6.1 Analysis of ID-in-everything

ID-in-everything cases primarily concern the communication of a sequence of bits (ID code) that identify a unit, such as a mobile phone or an RFID tag. If this unit is closely linked to a person (such as a mobile phone the person always has on them, or a chip implant), the ID code will also act

[17] [Octave].

[18] A good example is the story from [Bardram] about how personnel in a Danish hospital found it too time-consuming to log in personally every time they had to register data in the IT system, so as a consequence one member of staff logged in to all the machines every morning, and then everyone had free access to the system. This made the work much easier for the personnel, but makes meaningful logging on a user basis impossible, and this is one of the requirements in Danish hospitals [The Danish National Board of Health].

as personal identification[19]. If the unit is more loosely connected to a person (in the case of a ski lift card, for example), then the ID code is not necessarily a personal identification, but serves to identify the person in a specific context (in this case in the use of ski lifts).

The overshadowing security problem with this type of pervasive computing is therefore rooted in problems related to identification. The security problem that has been discussed the most in this context so far has been related to privacy, because this is obviously a question of how we can guarantee that personal information remains private, as the use of these units (see section 4.1) becomes more and more widespread. Other relevant problems are related to integrity and availability.

6.1.1 Threats to confidentiality with ID-in-everything

The threats to confidentiality in connection with ID-in-everything are all linked to privacy. The legal analysis in appendix 2 assumes that the current legislation is able to deal with these questions, apart from the fact that access by consent may constitute a certain risk, but that there is a need for regulation in relation to the surveillance of non-identifiable individuals. Regardless of this conclusion, there is a potential threat to privacy from a technical perspective, and this is described in more detail in the following.

Systems that use ID codes to depict physical objects in the virtual space can work in the following way: each object is given an ID code, and a database is maintained with a list of which objects have which ID codes. When a scanner (with a specific geographical location) “sees” an ID code, the system can conclude from this that the object with the ID code that has been seen is close to the reader. RFID works in this way. In addition to a database with the depiction from ID codes to physical objects, it is naturally possible for the system to build up a database of the observations registered about a specific ID code.

On the basis of this, there are three types of threat to privacy: the reading of ID codes, the misuse of existing databases with registered ID codes, and lastly, a combination of the two.

As ID codes are most often sent wirelessly, it will be possible to intercept them without being noticed, as a receiver can often be hidden very easily. This threat is basically more serious the greater the distance from which ID codes can be intercepted, as this increases the attacker’s options. For example, a GSM telephone now transmits an ID code that can be read at a distance of several kilometres, a laptop computer that is set up for wireless communication sends out a unique address (when it discovers a wireless network) that can also be intercepted over great distances, whilst a small (passive) RFID tag often requires the ID code scanner to be relatively close to the tag (less than a metre). An attacker wanting to intercept the ID code from an RFID tag therefore has to be in the immediate vicinity of the tag.

However, there are aspects other than the physical technology that are also relevant for how great a distance an ID code can be read from. If we take the RFID tag as an example, it should be noted that certain protocols[20] for reading the code from such a tag work by the scanner transmitting a known prefix of the code, whereupon the tag sends the next bit[21]. This process is repeated until the

[19] Biometric identification, which simply comprises a biometrical characterisation of a person converted into a sequence of bits, is another example of personal identification.
[20] E.g. EPC – Electronic Product Code [EPC].
[21] See [AutoID].

entire code has been read (this method makes it possible to differentiate between codes from many tags that react to the scanner at the same time). More specifically, this means that it will be possible to read the tag's identity code from the signals transmitted by the scanner. The transmitter normally transmits its signals with considerably greater strength than the tag, and it is not uncommon for them to be able to be read at great distances (up to 100 m).

In general, then, the reading of ID codes is possible from a purely technical perspective, but it will naturally require an attacker to be in possession of a scanner that is fairly close to the unit that is being scanned. A distinction can be made here between attackers who purposefully set up scanners to register units in a specific area, and scanners that are set up with a legitimate purpose, and that read and register units that are not otherwise relevant to this purpose. An example of the latter could be access points to wireless networks that register which PCs move through the area covered by the network, even though these PCs do not want to use the network, or similarly, RFID scanners in shops that read tags on all products, including products bought elsewhere. Although we would not expect legitimate scanners to actually be misused, the key point for the assessment of this threat is that they can very easily be misused.

The ability to read an ID code from things such as a mobile phone or an RFID tag basically discloses *nothing* about the unit or user associated with this ID code. This would usually require access to the database that associates the ID codes with the unit and/or user. Thus, the examples given above do not provide information about what a user has bought in other shops, for example, but it does, however, provide the opportunity to follow a product, and thereby an (anonymous) user's movements in a shopping centre, for example.

Please note that the possibility of carrying out surveillance is neither new nor particular to pervasive computing. It has also been possible in the past, with the help of video surveillance, for example, but with ID-in-everything it will be very easy to automate the collection and processing of these data. As seen above, the increased spread of IT equipment that communicates wirelessly, and the fact that the equipment can relatively easily be made to transmit a unique ID code, helps to make it easier to trace the bearer of the equipment. As ID codes are already given in electronic form, and as each individual acquires more and more equipment containing IT, the possibilities of carrying out an exact tracking of the user will be improved. Such tracking is, however, conditional on ID codes being read and analysed. So databases will need to be maintained with ID codes and the context in which they are read.

This leads us on to the next threat, which is the misuse of databases containing ID codes that can be traced to a particular person, either directly or indirectly, by linking different pieces of information together. Such analyses are commonplace for detecting credit card fraud, and identifying consumption patterns, amongst other things[22], and in the same way it is easy to imagine the value of analyses of consumption patterns on the basis of information from the use of RFID in the retail trade, for example. In connection with attacks on databases, it is important to understand that an attacker must have access to the database, and will therefore often be an insider. The threat to privacy in connection with tracking therefore comes, to a great extent, from the organisations and their employees who control these databases. In comparison with the more direct and tangible threat of a breach of anonymity by reading what a person on the street has in their shopping bag, for

[22] See, for example [CreditCardFraud].

example, this threat is less obvious, because it is based on an analysis of a quantity of data that has been collected, where each individual case of scanning can appear innocent.

The last threat is the combination of a scanning of ID codes and the (mis)use of databases. If we look at the use of RFID tags to prevent shoplifting, for example: a product with an RFID tag bought in one shop will also be able to read in our shopping bag by another shop that also uses RFID. The new factor here is thus that as well as being able to follow a certain ID code, there is also access to the database that links this ID code to more interesting data. Depending on what data material is available, the second shop will have an idea of what products we may be interested in, and possibly who we are, or even what we have previously bought in various shops. This type of attack on privacy will generally be more complex than attacks that merely analyse a single database, both because they require (online) access to the relevant databases, and because the attack will probably either involve several organisations that are working together, or else an organisation that has to obtain unauthorised access to another organisation's database.

6.1.2 Threats to integrity with ID-in-everything

Attacks on the integrity of an identification mechanism will often have the nature of attempts on making false identification. The scenarios mentioned provide a number of motives to do this. Here are just two of them:

- In the example from Mexico, where RFID tags are implanted in connection with access control to confidential documents, a person may be interested in pretending to be another person specifically in order to gain access to certain documents.
- If an RFID tag is used to identify a product in connection with payment for the product, a (dishonest) customer (who has physical control over the tag) may be interested in the product being identified as a much cheaper product.

In all the scenarios, identification is carried out by means of transmission of a constant ID code. As mentioned above when dealing with confidentiality, this code can easily be intercepted, and then it is easy to assume this identification. If the unit is used to identify a person, we can now pretend to be that person ("identify theft").

As long as there is a (financial) benefit from such attacks, the threat will be real. There are numerous examples of this, such as the first generation of mobile phones, where the telephone's identity could be intercepted with the help of a simple radio receiver, and then copied to another telephone.

It should be underlined that it is far from all forms of identification that are as unsafe as those described here. This is dealt with in more detail in section 6.1.5.

6.1.3 Threats to availability with ID-in-everything

In addition to the above, three types of threat to availability can be identified. These are threats that aim to prevent a unit from transmitting its ID code, threats that aim to prevent the system that receives and uses the ID codes from working, and lastly the prevention of access in the event of power cuts, i.e. if a unit's battery runs out.

The first will be a particularly relevant threat in the shopping scenario, as it is possible to imagine a dishonest customer avoiding payment for a product when there is a fully automatic checkout[23], if the product's RFID tag is prevented from transmitting its ID code. Again, the chance of this happening depends on the type of communication technology used, and on the logical protocols used. In practice, such an attack can be carried out by screening the tag (the product) so that it is unable to respond to the receiver's signals (e.g. by putting the product in a bag lined with a material that acts as a suitable screen). Other systems operate with the possibility of turning a tag off (in order to limit the threat to privacy, amongst other things). This creates a risk that a customer can turn the tag off before the product has been bought.

Threats to the availability of systems using the ID codes will often be denial-of-service attacks, where the receiver system is flooded with more codes than it is able to handle. This kind of attack can naturally have disastrous consequences for shops that base payment on ID codes from RFID tags, for example, or companies whose infrastructure is based on wireless networks. This form of attack is technically more demanding than the first, but the Blocker tag (see below) is an example of a technological aid that can inundate a scanner.

Both these types of threat appear very probable in connection with the retail trade, simply because shoplifting is a widespread phenomenon.

The last type of threat to availability, where the unit runs out of battery, could be realised with the type of attack that Stajano[24] calls "sleep deprivation torture", which basically means sending signals to a unit to which it is expected to respond, whereby it will run out of battery in time. In day-to-day applications, this form of attack is not particularly realistic, however, apart from in the case of alarms (e.g. for protection against shoplifting), where it could obviously be in the thief's interest.

Threats to availability are caused by hardware and software errors that are also found in ID-in-everything. These are dealt with in connection with the analysis of services-in-everything in sections 6.2.3 and 6.2.6.

6.1.4 The protection of confidentiality with ID-in-everything

The above analysis of threats to confidentiality – i.e. privacy – in connection with ID-in-everything works with a number of implicit assumptions, for example that RFID is tantamount to unique identification, and thus, that RFID tagged products in the retail trade are allocated a unique ID that follows the product throughout its life cycle, which in particular means even after it has left the shop. As mentioned earlier, there are no a priori reasons for identification solutions to require systems that use unique identification. This not only applies to RFID, but also to other identification technologies such as WiFi and mobile phones. We will discuss this in more detail below.

A system used for identification can be characterised by the four properties listed below:

- The use of databases – does the unit contain an ID code that can be linked to logical information via a database (as described in section 6.1.1), or is the logical information also on the unit (including if the only information is the ID code)? RFID as described here is of the first type.

[23] If the checkout is not fully automatic, there will naturally still be a threat, but then the situation will be no different to the one in shops today.

[24] [Stajano].

- Unique identification or context-dependent recognition – does the unit have a fixed, unique ID code, or can it have several different ID codes for use in different contexts?
- Authorisation to read the ID code – does another unit, such as an RFID scanner, have to be authorised by the unit before the unit transmits its ID code, or is the ID code given to everyone who asks for it?
- User control – is the user involved in deciding who gets what information from the unit?

RFID, such as in the case of EPC, uses unique identification, no authorisation, and basically no control. In this situation there are technical and non-technical mechanisms that can protect privacy. The legal analysis in section 5 describes a number of non-technical measures that can be used. These include openness, consent and clear definitions of who is the data controller for a specific database with ID codes, for example. This involves legal regulation with the purpose of protecting data from the threats described in section 6.1.1. Such non-technical solutions are based on legal regulation in the form of legislation and/or voluntary agreements. Appendix 3 presents just this kind of voluntary agreement in the form of a proposed code for the use of RFID technology in the retail trade, for example.

If we maintain the technological assumptions that apply to RFID (see above), then the primary technical method of providing security is the proper protection of the databases involved, which underlines the need for clarification of the data controller, as also mentioned in the legal analysis in chapter 5.

There are several ways in which the user can be given control over the reading of ID codes. Basically, these are the same as the threats to availability described in section 6.1.3 (which means that these threats can, strangely enough, be considered as security mechanisms in this context!) A mobile phone can, for example, be prevented from transmitting its ID code if we turn it off. There is no such possibility for RFID tags, but here we can suggest methods such as the “kill mode”[25] and Blocker tags[26]. In general, these solutions have the restriction that they reduce the functionality, as a mobile phone that has been turned off is of less use than its intended application, for example.

As also mentioned in section 5, control over our own data is generally desirable – in one form or another. This can either be a form of control over which data are transmitted by a unit in a specific situation, or control over data that have already been collected, e.g. control over which data have been saved and/or disclosed by a certain shop with regards to our purchases.

In cases where RFID tags are used to mark a product, for example, the shop has control over the tag for as long as the product has not been sold. Once the product has been sold, the purchaser may be interested in turning the tag off, so that others cannot read the tag to see what products the purchaser has in his/her shopping bag. Later, however, the purchaser may be interested in turning the tag back on again (if our freezer is able to keep a check on the contents of the freezer, for example). The important thing here then, is that the purchaser must not be able to gain control over the RFID tag on the product before it has been bought, but that after the purchase, he/she will be interested in having full control. In the case of RFID, it is also conceivable that after buying a product, the user is able to obtain full control over the ID code transmitted by the unit. In particular, this option gives us

[25] The kill mode allows an RFID tag to be turned off by sending a specific “kill code” to the tag. Once this has been done, the tag cannot be resurrected.

[26] A Blocker tag (see [Blocker]) transmits several different ID codes at a time, thus confusing the RFID scanner, so it is blocked from reading the code in other tags.

the opportunity to set our own ID code, i.e. the opportunity to give a unit a new ID code, for example, so as to thereby render it impossible to combine data about a person’s private units with data from the shops selling the units, for example[27]. In principle, this can be done with units with a small IT capacity, but this is not possible with normal RFID tags, and, as mentioned above, methods are required to deal with, and transfer, control over the unit[28].

If we consider units with greater IT capacity, such as more advanced RFID tags, smart cards (and thereby mobile phones), etc., it will be possible to ensure that units only supply their identity to other units that are authorised in advance, e.g. with the help of cryptography. This would prevent foreign systems from being able to follow the unit, but it would not prevent tracking with the help of authorised units. It should also be noted here that a number of units and protocols, such as BlueTooth and GSM that actually support cryptography, tell their ID code to everyone who asks for it anyway. The use of cryptography is thus not in itself a guarantee that data such as ID codes are protected.

All in all, the primary method of safeguarding privacy when using global identification, is to regulate the use of – and thus protect – databases containing ID codes and associated data, and to control which units are authorised to read an ID code. Moreover, there are certain technical measures that prevent the unit from being read, but these are all irksome for the average user.

As mentioned above, there are no a priori reasons to use unique identification. This can be avoided either by hiding the ID code entirely, with the help of cryptography[29] as described below, or by using solutions where the ID codes are replaced (automatically or under user control) during the unit’s life cycle.

There are technical solutions that ensure anonymity whilst being able to uphold properties such as non-repudiation. These include solutions for the anonymous handling of privileges, where the anonymity is only granted as long as no attempt is made to cheat, in which case the user’s identity is revealed, so that he/she can be called to account[30]. The use of such techniques requires the underlying technology to support advanced cryptographic mechanisms, however, which may be a technological challenge. Besides, anonymity in practical solutions will probably also often be dismissed, because the need for anonymity does not match the cost involved.

The basic idea in this form of protection of privacy is to reduce the value of ID codes saved in databases. This leads us to the possibility that exists for using solutions that do not use a database, such as in certain network protocols, where a unit merely reports an address (an ID code) that is used to send it the response in the current communication; an example of this is MAC codes, which are mentioned in connection with WiFi. In this context, it should be noted that just because a database is not part of the infrastructure, does not mean that a database cannot be constructed from scanned ID codes, so tracking is still a threat.

Thus, there are several good ideas as to how privacy can be safeguarded by technical means, and this is an area in which a great deal of research is being carried out. The thing that all these

[27] See, for example [Engberg].

[28] Anderson and Stajano's “Resurrecting Duckling” described in [Stajano] is a proposed solution to this problem.

[29] A technical pitfall with this is that the encrypted value that is sent out must be different from one time to the next; otherwise the encrypted ID code will act like the ID code itself, for all practical purposes.

[30] See, for example [Chaum].

solutions have in common is that they demand more: both of the unit and of the user, due to the increased technical complexity. On the other hand, these solutions do not change the basic functionality that is offered, i.e. the cases and scenarios described in section 4.1 can be realised without their use being materially altered. The case with the use of RFID in the retail trade and the like will, for example, require cheap RFID tags that can perform the required calculations (otherwise these solutions will be too expensive), and it will require the solution to be designed so that it can easily be used by the average consumer.

6.1.5 The protection of integrity with ID-in-everything

In this context, the primary objective is to achieve the secure identification of units. The threats described in section 6.1.2 are, in fact, all forms of spoofing, in the form of identity theft, for example.

If we again base our assessment on the RFID technology, then the cheap and widespread passive tags provide very poor security. For many of the applications described, it can, however, be argued that the security is suitable *for the purpose concerned*. Either because the security requirements are not so high (who would think of spoofing a litre of milk in the fridge?), or because RFID can be used in connection with other technologies: in the example with implanted RFID tags, one might imagine a combination with physical access control, for example, where the possession of the RFID is merely one of several elements of identification: having read it, the ID code could be used to automatically call up a picture on the guard’s screen, whereby the value of spoofing a tag is reduced to almost zero.

A large number of other identification technologies, such as BlueTooth and WiFi, are criticised as being unsafe. In reality, however, they have to be considered some of the best proposals for secure identification in practice. A pronounced strength of these protocols is that they are standardised and widespread, which is precisely why they are subject to heavy criticism. It is this that is their strength, under the key assumption that the weaknesses that are identified in these standards are addressed as they arise, because any weaknesses can then be found and corrected. If a non-standard protocol is used, there will be a risk that it has weaknesses that are not brought to the public’s attention. A good example of this is GSM, which uses its own protocol that has proved to have more major weaknesses[31].

6.1.6 The protection of availability with ID-in-everything

Availability is often the hardest thing to protect. Denial-of-service attacks in the form of jamming an RFID scanner, for example, can be hard to prevent with purely technical solutions. A typical solution would be to identify an attack when it takes place – and preferably where it comes from – and then subsequently stop the attack. The misuse of Blocker tags (described above) by shoplifters illustrates the problem. As mentioned in section 6.1.3, Blocker tags transmit a number of codes. However, the scanner can easily discover this, as the codes that are transmitted include irrelevant or invalid codes (such as codes for products that are not stocked in the shop).

The guaranteeing of battery life is a central element in the construction of units, so it must be assumed that the most common problems are, or will be, countered automatically. An interesting solution is naturally passive RFID tags that do not have a battery at all. However, such units are only able to offer very limited functionality.

[31] Described in [Anderson].

6.2 Analysis of services-in-everything

6.2.1 Threats to confidentiality with services-in-everything

The threats to confidentiality identified in the three services-in-everything scenarios fall into two groups: threats to privacy and threats to the confidentiality of data that is communicated or stored.

As with ID-in-everything, the identification of units is a very important element. Units do not just have to send an ID code to a scanner, they also have to be identified as belonging to a certain person, and acting in various networks, for example. This is the case in the ESN scenario, where the service person’s unit is part of a network with a number of units in the building he/she is servicing. This gives rise to a number of privacy-related threats concerning the monitoring of where he/she is, and when. However, it should be noted that this is monitoring in connection with the performance of a job, so there may be reasons for the monitoring actually being considered desirable. Another situation where monitoring may be desirable is in the Healthcare for tomorrow scenario, where a diabetic patient is monitored if certain criteria are met – e.g. it is monitored whether he/she has taken insulin from the fridge within 10 minutes of his/her blood sugar becoming too low. Moreover, the healthcare scenarios in general are different in that the database in which the sensitive monitoring data are stored will often be located in the patient’s home. This drastically reduces the risk of attacks by insiders.

On aggregate, services-in-everything gives rise to a number of threats related to privacy, just like ID-in-everything. However, in some of the suggested applications the actual threat would appear to be lower, such as in the cases where the sensitive database is under the control of the person who is being monitored, so to speak.

In addition to threats related to privacy with services-in-everything, we meet a requirement for the protection of confidential information. This is particularly true in connection with the “healthcare” scenarios, where the patient is typically not interested in his/her healthcare information being able to be read by people other than the relevant doctors and nurses. The selected scenarios focus on visiting nurses, but the problem is no less relevant in hospitals and the like (for example in connection with electronic patient records). There are specific security requirements for hospitals stipulating which data must be kept confidential, for example[32]. These rules originate partly from more general security rules for the treatment of sensitive personal data[33]. Thus, there is not merely a threat to the confidentiality of the data that is communicated and stored in these scenarios; in a number of cases rules are laid down specifically demanding that this threat be met.

The threats to confidentiality in this group of scenarios thus include threats to privacy (such as in ID-in-everything), threats to the confidentiality of the data that is communicated (internally in the home and externally between the gateway and a central system), and threats to the confidentiality of data in connection with storage and use.

6.2.2 Threats to integrity with services-in-everything

The scenarios point to three types of threat: the modification of data in connection with communication, unauthorised access and the repudiation of agreements.

[32] See [The Danish National Board of Health].

[33] See [The Danish Data Protection Agency].

The integrity of data communication is essential in all the services-in-everything scenarios, and in this context it is usually also important to be sure of the origin of data. For example, the doctor wants to be sure that health information comes from the right patient, and that it is in fact the measured data that get through from the sensor to the doctor. If this is not the case, it is conceivable that the patient could be given the wrong treatment. Similar problems are met in the ESN scenario, where information is downloaded about the buildings that have to be maintained. These threats are very serious, not necessarily because the chance of data actually being modified is high, but because the consequences are unacceptable, for example in the form of incorrect treatment. It should be noted here that the threat to the integrity of data can either be directed at the communication from the sensor to the gateway (including the introduction of false sensors), or at the communication from the gateway to the communications centre.

In the eu-DOMAIN scenarios, the identification of a unit (or the person who owns the unit) is used to gain access to information and buildings (so the service technician can gain access to the buildings that have to be maintained, and the nurse can gain access to the patient, if alarms are triggered). A threat to the security (integrity) of the identification protocol could therefore lead to unauthorised physical access. In general, the identification in these scenarios is also used to obtain access to networks, to information or to buildings, as this access is reserved for specific people in the scenarios referred to here. There are thus threats of both physically and logically unauthorised access. Again, this threat must be taken very seriously in order for the solutions to be accepted. It is, for example, on the one hand important for the patient’s sense of security that the nurse is able to come in if required, but on the other hand the patient naturally does not want the system to give other people access.

Unauthorised logical access to closed systems is already a well-known problem. A popular technique amongst burglars has been to use remote controls for expensive television and stereo equipment to find out whether it will be “profitable” to break into a specific house. The burglar uses his/her own remote control to determine whether there are “desired” machines in the home. If the machines are not turned off properly, they will react to the remote control (e.g. play high music), and the burglar can thus decide whether there is equipment he is interested in without entering the house.

The last type of threat is the repudiation of agreements that have been concluded, as seen in the ESN scenario, for example, where agreements are concluded with subcontractors. It is normally desirable for such agreements to be non-repudiatable, i.e. so that the service technician is not able to conclude binding agreements about a spare part with two different suppliers in order to be sure to get the spare part, and then go back on the agreement that is delivered last. The security problem related to this is also important for scenarios of the agents-in-everything type, and will be discussed in more detail in this context.

6.2.3 Threats to availability with services-in-everything

In all three scenarios, availability is essential for the systems to be able to be used in practice. The threats fall into three groups, of which two concern errors, and one concerns the possibility of running “foreign” software, i.e. hardware errors, software errors and malevolent software.

In the “healthcare” scenarios it is naturally unacceptable if a patient cannot be treated because one of the units is not working, regardless of whether this is due to an error in the hardware or the software. The same is true, but is perhaps less serious (after all, it does not concern human lives), in the ESN scenario, where it is unacceptable for a building to be without heat or electricity for a few days because the system is not working properly.

The problem with faulty software is made worse by the desire to be able to download new software to a unit, either automatically or manually (see both the ESN and EPCiR scenarios). This is already a well-known security problem in connection with applications downloaded from the Internet, and it naturally increases the threat to the availability of the units used in the services-in-everything scenarios.

The possibility of installing modified or additional software also opens the system up to malevolent software – viruses, worms, etc. – that is able to penetrate the systems "of its own volition". This is one of the most common problems in the "PC world", and the trend is for many of the small units to start using operating systems based on the same basic ideas as PCs, so there is no reason to believe anything other than that viruses, etc., will also become a big problem in the field of pervasive computing. Indeed, the first viruses on mobile phones have already been reported[34].

6.2.4 The protection of confidentiality with services-in-everything

The protection of privacy with services-in-everything does not include anything new in relation to ID-in-everything as discussed above. The need for protection may vary, depending on how serious the threats are considered to be, but the protective mechanisms that are available are, in principle, the same.

The confidentiality of stored data is basically safeguarded with the help of encryption, and with the help of access controls that manage which users have access to which data. When it comes to access control, the identification of users is important, as mentioned in connection with the threats to integrity in section 6.2.2, as the assumption of other people's identity in a specific situation can give that person unauthorised access, and thus compromise confidentiality. Access control is discussed in more detail below, under the protection of integrity (section 6.2.5).

Access control does not, however, address the aspect of the communication of data over "open" networks,[35] or even the placement of data on a unit that is easily accessible, such as a PDA or a laptop computer. Cryptography is used to safeguard confidentiality here. In closed systems, which are characteristic for services-in-everything, it will often be possible to configure the cryptographic infrastructure that allows the communication of encrypted data in connection with the conclusion of the agreement that forms the basis for the closed system. It should be emphasised here that secure solutions ought to be based on recognised standards for the use of cryptography, such as RSA or AES – as well as standards for the infrastructure.

An open problem in connection with pervasive computing is whether the fact that many units have a limited IT capacity means that traditional cryptographic algorithms can no longer be used, simply because they take too long, or use too much memory, for example. However, there are examples of solutions that use RSA for scenarios similar to services-in-everything[36], and if this is not sufficient, consideration could be given to using other cryptographic systems that are more performance

[34] See [MobileViruses].

[35] Such as WiFi and other forms of wireless communication, and also communication over the Internet in a broad sense.

[36] See [MicrosoftResearch].

“friendly”, such as public key[37]solutions based on so-called elliptic curves (that have already been standardised) instead of RSA, which is the most widespread today. Lastly, it should be noted that the use of gateways, i.e. solutions where there is a central unit with a large IT capacity, could facilitate the work, because, in some cases, the cryptographic algorithms can be adapted so that the most difficult calculations are performed here.

Communication from a small unit (such as a sensor in a bandage) to a gateway will also, in a number of cases, probably not require such a high level of cryptographic security, provided that this communication is not able to be listened to from outside the home. If it is not possible to guarantee this (depending on the technology), additional security will naturally be required, which may pose a challenge, due to the limited computing power in the sensor.

The confidentiality of data must therefore be guaranteed in the traditional manner. The primary challenge, as can be seen here, is to get small units with limited IT capacity to encrypt data. At the end of the day, the solution of this depends on a cost-benefit analysis, as such units are often relatively expensive (compared to similar units that do not support cryptography). Moreover, there are challenges in connection with the infrastructures that are necessary for exchanging and handling cryptographic keys and access control in cryptography, as described below under the protection of integrity. However, there are no principal obstacles to the use of cryptography in guaranteeing confidentiality (or integrity – see below) in connection with services-in-everything.

6.2.5 The protection of integrity with services-in-everything

The integrity of the data that is communicated in connection with these scenarios can, in most cases, be safeguarded by traditional techniques. This is true of data that is sent from a central gateway in a building to a central server (or another gateway) for example, as the units involved here will have adequate computing power to be able to support standardised cryptographic methods. Otherwise, the comments made above about cryptography in units with small IT capacities naturally also apply here.

The second main threat to integrity in these scenarios is directed at access control (physical access to buildings and logical access to IT systems and data). The protection of this involves the secure identification of the user, as mentioned in section 6.2.4, and a secure system for authorising users requesting access. In addition to the three traditional elements: something we know (e.g. a password), something we have (e.g. a token with a digital signature), and something we are (biometry), access control in connection with pervasive computing will, in some cases, draw on a fourth element: where we are – i.e. our physical, geographic location (this should obviously also be considered from a privacy perspective, because tracking is implicitly involved in such solutions).

The last type of threat is directed at the non-repudiation of agreements, i.e. the fact that agreements are binding. Systems that ensure non-repudiation may comprise a digital signature together with a set of rules for the use of this digital signature, i.e. how agreements should be dealt with electronically in order to be binding, for example. In those cases where the agreements are concluded by participants in a closed network – which is the case in the three services-in-everything scenarios, the set of rules will often be laid down in connection with the configuration of the network. In situations where agreements are not made within a closed network, it will be more

[37] Public key cryptography is the form of cryptography used in digital signatures, and is the form of cryptography requiring most IT capacity. RSA is the most widespread type of public key cryptography.

difficult to lay down such a set of rules, as we shall see in section 6.3.5. Lastly, it should be noted that digital signatures are based on public key cryptography, which is why the problems mentioned above concerning the limited IT capacity of the units also apply here. On aggregate, however, it would not appear unrealistic to have both cryptography and agreements in place in connection with the services-in-everything scenarios, because they are closed systems where there is often a central unit with greater IT capacity available.

6.2.6 The protection of availability with services-in-everything

The threats to availability that are described can be directly addressed by two mechanisms: guarantees that the hardware and the software are correct, by means of certification, for example, and the use of secure operating systems.

It will probably always be the case that the use of pervasive computing will push technology to its limits, which is why it will always be reasonable to imagine the use of units with specialised software. These units ought to be certified in one way or another – depending on their application – so that the user can be fairly sure that they will behave properly. Such certification is expected to be able to take place on the background of existing methods such as the Common Criteria[38].

Such certification may soon become worthless, however, if it is possible to change (parts of) the software that is being run on the unit. There are now several “secure” operating systems for this purpose that run foreign programs in strictly controlled surroundings, and that use measures such as digital signatures to guarantee the origin of the programs. This will reduce the risk for units that have sufficient IT capacity to use such operating systems. In certain cases it may be necessary to restrict the possibility of installing foreign programs in order to eliminate this threat.

6.3 Analysis of agents-in-everything

The values and threats in these scenarios are generally covered by the analyses of ID and services-in-everything. Compared to the solutions that can be used in these scenarios, there are now a number of new problems as a result of the even greater number of units, the openness of the systems, and the use of intelligent agents that autonomously carry out actions on behalf of their “owners”.

The scenario of Maria – road warrior describes how Maria’s armband automatically identifies her in connection with what can be compared to old-fashioned passport control. The security of this authentication is implicitly dependent on the armband (and the system with which the armband communicates) being convinced that it actually is Maria who is in possession of the armband (user authentication), and on Maria *wanting* (control) to be identified by the system (in this specific case, it appears obvious, but in general this is not necessarily the case).

6.3.1 Threats to confidentiality with agents-in-everything

The increased amount of interaction between agents will in itself give rise to a number of threats to the confidentiality of personal data, and it will, to a great extent, be up to the agents to control this. This includes the storage, communication and processing of these data in the agent. On the basis of the agents-in-everything scenarios, it is to be expected that these agents will control, and process and communicate, a large quantity of personal data (such as medical data), so the protection of this will be important for the user’s acceptance of such systems.

[38] [CommonCriteria].

With regards to privacy, we are now dealing with applications where the users use units that transmit ID codes to “foreign” systems. On this face of it, this would appear to increase the risk of the ID codes being registered in databases, because the legal regulation of this across national borders will not necessarily be unambiguous.

6.3.2 Threats to integrity with agents-in-everything

In addition to the threats that have already been mentioned, the primary problems related to integrity are directed at non-repudiation, and at a form of unauthorised access. The latter may not be so much of a threat as a problem, due to the need for interaction with foreign agents, units and users.

In these scenarios a number of agreements are concluded in connection with the lift and the purchase of goods, for example. These are binding – i.e. non-repudiatable – in the sense that they will subsequently give rise to payment. If these agreements cannot be used to collect payments that are due after all, then their use in these scenarios will fall to the ground. This problem is related to the existing problem with the legal validity of digital signatures. Please note that there is the additional challenge here that, whereas a digital signature today is typically generated on the basis of the user’s explicit acceptance (e.g. in a browser or e-mail program), an agent in these scenarios will be configured to be able to make such an agreement on behalf of its owner more or less independently.

As can be seen in the description above, agents-in-everything involves constant identification, and typically to “foreign” units, i.e. units we do not really know whether we can trust or not. Children’s use of the Internet is already a big problem for parents’ sense of security, with regards to the fact that it is possible for strangers to contact their children electronically. If children are given agents that are as investigative as in the example with Carmen, where her agent takes responsibility for finding a lift, then there is a great risk of “unauthorised access”, i.e. the foreign unit gaining access to more information than we would like, such as our name and address. In order to avoid the subsequent sense of insecurity, it is important that agents can be configured and controlled so that not only children, but everyone, is only in contact with agents belonging to people with whom we want to have contact. This may, however, appear to conflict with the ideas behind agents-in-everything, where it is this electronic interaction with strangers or their agents that we want. The problem is basically how, and how much, we can trust people, units and agents we may never have met before.

6.3.3 Threats to availability with agents-in-everything

The threats to availability are no different to those in the cases with ID and services-in-everything. The main difference is that the technology is expected to be much more widespread. Thus, the individual’s day-to-day life will probably also be much more dependent on technology, and problems with availability may have much more serious consequences.

6.3.4 The protection of confidentiality with agents-in-everything

As mentioned above, these scenarios do not involve any new features of note. However, it should be noted that personal agents, for example, can be assumed to have sufficient computing power to be able to encrypt data using traditional, strong encryption methods, because the capacity required to be able to run a sophisticated agent will be much greater than that required for cryptography. Thus, it will be possible to protect personal data by using advanced cryptographic methods.

In the same way, it is also expected to be possible to implement good identification protocols (at least on units that run agents) that do not immediately disclose the identity of the owner, but maybe just a pseudonym or, more generally, the fact that the owner has the privileges required in a specific situation (whether or not such solutions can be used will, however, depend on whether such anonymous access can be permitted at all). Given the increased risk that this poses to privacy, in particular, as described above, it would appear sensible to devote extra effort to the technical front.

6.3.5 The protection of integrity with agents-in-everything

As mentioned in section 6.3.2, the protection of integrity requires the support of non-repudiatable agreements, and control over which foreign agents we want to "have a relationship with".

If we want to use the most common cryptographic infrastructures to deal with non- repudiatable agreements, these scenarios require international cooperation, e.g. an international digital signature. This has been on many people's wish list for the past 10-15 years, but is as yet a long way from becoming a reality, and it is questionable whether such a global infrastructure will be able to be established. In order to support the scenarios stated, all agents must be certified. In addition to these, certificates should be issued for all other (relevant) units on a global level where we want certificates and the associated cryptographic techniques to be used. Certificates that are used perfectly transparently by various units are already being issued today in connection with the production of chips for these units (e.g. credit cards and chips for PCs with inbuilt keys). So it is technically possible, but it needs to be raised onto a larger scale in order to be able to support these scenarios. Apart from the purely practical aspect of issuing certificates, it must be a minimum requirement that better solutions be used to revoke certificates – the lists of blocked cards that are used today are not feasible, simply because they will become too long. In general, it can be said that the technology for this exists already, in the main, but it is in no way implemented sufficiently.

Although solutions such as digital signatures are escalating, there are still problems. The idea with a digital signature system is that we trust the statement about who owns a specific cryptographic key, based on the fact that a CA "approves" this link between the individual/unit and the key[39]. The crux of the matter here is that because we trust the CA, we also trust the CA's statement, i.e. certificates. The question is whether the average Danish user without a great insight into IT will trust a Japanese national CA, for example, or perhaps a CA run by a private person (e.g. for certification of the person's own units)?

Moreover, there is a further complication concerning precisely this problem of trust or unauthorised access. As mentioned earlier, access control comprises identification and authorisation. If we assume that a foreign unit is safely identified, what privileges should we attribute to it? This means that even if we have safely determined a unit's, an agent's or a person's identity, do we then trust that person? Do we want to conclude agreements involving money, for example? In general, trust is described in the literature as being one of the fundamental research problems with regards to security and pervasive computing, and there are a number of research activities in this field, including the SECURE project,[40] which has Danish participation.

[39] The Danish public digital signature [DigitalSignature] is a good example of this kind of infrastructure, and there are a number of popular infrastructures and recognised cryptographic standards that may be able to used directly. TDC, the Danish telecommunications company, has the role of CA in the case of the Danish digital signature.

[40] See [Secure].

6.3.6 The protection of availability with agents-in-everything

There is nothing new to add here in relation to the analyses of ID and services-in-everything.

6.4 Summary of potential technical security problems

In summary, the analysis carried out above has identified a number of potential security problems related to the use of pervasive computing. In many areas, they do not differ significantly from well-known problems concerning the use of IT. The main ways in which they differ from the current IT solutions is in the use of units with very limited computing power, and in the great popularity that it is expected to enjoy.

The table below provides an overview of the threats that have been identified in the previous section. Please note that the threats in the ID-in-everything scenarios are also found in services-in-everything, and in the same way the threats in these scenarios are also found in agents-in-everything. In the table below it is only the first type of scenario in which these threats are described above that is included.

The table below should naturally not be interpreted such that the threats described in services-in-everything scenarios will not be able to arise in ID-in-everything, for example, but it does reflect a general tendency in possible threats to pervasive computing.

Outcome	**Description**	**Type of scenario**
Confidentiality is compromised	Tracking or identification of a person in connection with the registration of ID codes	ID-in-everything
	The misuse of databases containing registered ID codes	ID-in-everything
	The compromising of data used in the system (such as personal data)	Services-in-everything
Integrity is compromised	The falsification of ID codes (the assumption of identity)	ID-in-everything
	Unauthorised access (physical or logical)	Services-in-everything
	The modification of data used in the system (such as personal data)	Services-in-everything
	Binding agreements in a *closed* system	Services-in-everything
	Binding agreements in an *open* system	Agents-in-everything
	Trust of foreign agents (and their owners)	Agents-in-everything
Availability is compromised	Power failure	ID-in-everything
	Preventing the unit from transmitting an ID code	ID-in-everything
	Denial-of-service attack against the scanner	ID-in-everything
	Hardware error	Services-in-everything
	Software error	Services-in-everything
	Installation (download) of unsafe software	Services-in-everything
	Virus attacks on units	Services-in-everything

7 Discussion and recommendations

This section discusses the most important challenges to IT security on the basis of the threats and possible solutions identified above. We will divide the discussion up into time-wise perspectives, as a number of problems differ in character between the short and the long-term. This is due to the fact that expectations of, and the specific knowledge about, the technology used differ considerably, and that a number of solutions that will not be able to be realised in the short-term, may be realised in the long-term.

7.1 Short-term perspective

In the light of the legal analysis and the analysis of ID-in-everything and services-in-everything, the most important problems in the short-term are assessed to be:

- Privacy
- The practical use of mechanisms that ensure traditional confidentiality
- Usability

The analysis also mentions problems in connection with integrity, primarily in the form of secure identification, and availability. Section 7.1.4 below, discusses why these problems are considered to be less important.

7.1.1 Privacy

Both the technical and the legal analysis point to privacy being a problem in connection with pervasive computing. The main conclusion in this matter is that the challenge lies in ensuring that pervasive computing is realised in such a way that guarantees privacy. The use of RFID, for example, is vulnerable from a technical viewpoint (see section 6.1), but the Danish Act on the Processing of Personal Data can deal with these vulnerabilities, provided that the practical elucidation of the Act is updated on a regular basis (see chapter 5).

The problems concerning privacy, i.e. anonymity and tracking, are not new to pervasive computing. The new factor is, however, the scale, and thereby presumably also the financial gain from implementing such threats. At the same time, the consumer’s fear may hamper the spread of pervasive computing, and thereby potentially reduce a large gain for society. The most topical example of these problems is the use of RFID, particularly in the retail trade, where the consumer perceives the risk as being great. Just how great the actual risk of future intrusions of privacy is will, to some extent, depend on clear legal rules being drawn up, as the threat of legal, and possibly financial consequences may serve to counterbalance whatever motives there may be for such intrusions. However, it should be noted that the risk of discovery may be small, in which case the overall risk of punishment will naturally diminish correspondingly.

In addition to the laying down of rules, the privacy problem can also be addressed from a technical perspective, by using solutions that make it harder – or impossible – to carry out tracking, for example (see section 6.1.4). In the case of RFID, however, this will require brand new solutions based on RFID tags with increased functionality, which can thereby be expected to be more expensive. In the short-term, the best solution put forward is thus that based on sound, understandable, widely accepted rules and agreements to control the use of pervasive computing. One specific initiative on this front could, for example, be the definition of an industry code for the use of RFID in the retail trade.

It is recommended that an industry code be drawn up for the use of RFID in the retail trade.

A draft of such a code is included in appendix 3.

It is uncertain whether or not such rules are sufficient, in practice, to give the average user the required sense of security, so the practical relevance of various potential technical solutions should be continually taken up for revision. The question is, however, whether the technical solutions we know of will find commercial application in the short-term, so consideration should be given to implementing initiatives that can promote the use of solutions that remove or reduce the threat to privacy by technical means. See more details on this matter in section 7.1.5.

It is underlined that the threat to privacy is not limited to the use of RFID in the retail trade. It also applies to other sectors such as the health sector[41], and also to other technologies such as mobile phones and old-fashioned credit cards. The use of RFID in the retail trade is somewhat special, however, because the scale on which the technology is used is much greater than has been seen to date.

Please note that tracking is not necessarily a bad thing. In some applications, such as in a number of workplaces, it may well be that the personnel are happy to use location tracking because it facilitates their work, for example, in the same way as the tracking of patients can lead to help being administered more quickly. Thus, the same technology can give rise to different threats and risks when used for different applications.

7.1.2 Confidentiality

As described in sections 6.2.1 and 6.1.4, another related problem is the confidentiality of sensitive personal data. According to the Danish Data Protection Agency[42] sensitive personal data, such as data about a person’s health, which is transmitted over an open network or on a portable medium (such as a PDA or a laptop computer) should be strongly encrypted[43]. This requirement is also explicit in the Danish National Board of Health’s IT security policy for hospitals[44]. However, it is probably not always common practice to follow these rules, partly because it often makes it more difficult to access data.

When units with very limited computing resources, such as wireless sphygmomanometers, start transmitting sensitive personal data in the form of measurement data, they should basically also be treated in the same way. The problem here is not necessarily a lack of motivation to follow the rules, but the mere fact that the unit may not be able to carry out strong encryption (although this is often a question of finance rather than technology, cf. section 6.2.4). Another problem may be that the standard configuration does not use the required level of security. BlueTooth[45] guarantees confidentiality, for example, with the help of a key of between 8 and 128 bits – and the maximum

[41] See, for example [Anderson].
[42] See [The Danish Data Protection Agency].
[43] The Danish Data Protection Agency writes in [Strong Encryption] that this means at least 128-bit keys for symmetric encryption.
[44] See [The Danish National Board of Health].
[45] BlueTooth units have started being authorised in the USA (by the FDA) for use in the health sector [FdaApproval].

security should be chosen here for transmission of sensitive data, which also requires the units to actually support this key size.

There is thus somewhat of a span between the rules for the confidential communication of sensitive data that can be traced back to a specific person, and what is done in practice, both with regards to the use and the technical possibilities. In appendix 2 it can be seen that the choice of technology does not affect the legal requirements for security, but is it realistic to require that sensitive data that can be traced back to a particular person, and that is transmitted wirelessly from a very small unit with very short range, should be strongly encrypted? In order to avoid misunderstandings about where and when demands are made of the use of strong encryption in units with limited IT capacity, these requirements should be clarified.

It is recommended that the need for the strong encryption of sensitive data in connection with the use of pervasive computing be clarified.

As stated above, this recommendation is particularly relevant for wireless communication from units with a short range.

7.1.3 Usability

The last problem is usability. The key point here is that if the users do not use the system as it is intended, then there is a great risk that the entire security policy will collapse like a house of cards.

Section 7.1.1 mentions the problem with usable methods for controlling units that transmit ID codes, but as more and more daily chores gradually become electronified with the spread of pervasive computing, it becomes more important for the user and the system to “understand” one another. This means that the mechanisms related to IT security, such as user authentication and the management of certificates, must be better implemented in a number of applications.

It is not evident how this problem is best dealt with, but it is clear that the understanding between system and user can be improved by making the users more proficient. Here we are not just thinking of their IT skills in the traditional sense being improved, but of the average user’s operational understanding of problems related to IT security being increased, so they choose a sensible password and do not tell strangers their password.

7.1.4 Minor problems

It may appear remarkable that two problems, in particular, are ignored in our analysis here:

- Secure identification, i.e. threats to integrity
- Availability, including viruses, etc.

Secure identification may appear to be a major IT security problem in connection with pervasive computing, if we were to measure the size of the problems on the basis of media coverage. A number of widespread protocols such as WiFi and BlueTooth appear to have been given a thrashing, but for many practical purposes, these protocols provide reasonable security. This is due to the fact that these protocols are often improved when weaknesses are identified. This is a particularly weighty argument for using these protocols for secure identification.

Another argument is that secure identification will, in many situations, be a requirement for the commercial spread of pervasive computing solutions, particularly in connection with services-in-everything, so it is reasonable to believe that secure identification will automatically be placed high on the list of priorities when these systems are developed.

Moreover, experience shows that problems related to the identification of users are often due to factors other than attacks on the cryptographic protocols. For example, a number of people have gained unauthorised access to IT systems by luring passwords out of users (also called “social engineering”), and many banks all over the world are now facing security problems due to “phishing” where the bank customer is lured to a site that closely resembles the bank’s, but that is fake, and where passwords and the like are lured out of the customer. These problems are important, but are considered here to be a part of the problem of usability (see above).

It is a recognised principle in the field of IT security that thoroughly tested security methods ought to be used (i.e. recognised cryptographic algorithms and protocols, for example). This not only applies to secure identification, but also to protecting integrity in a broader sense, and naturally to protecting confidentiality.

It is recommended that recognised protocols be used for secure communication.
A list of recommended security mechanisms for pervasive computing could be kept by an official body.

The threats to availability that have been identified, such as viruses, battery life and preventing an RFID tag from transmitting its ID code, are also assessed to be less important in the context of this report. The reason for this is simply that the problems are not peculiar to pervasive computing, and they will probably have to be solved with standard techniques known from the world of PCs. Viruses – in connection with pervasive computing – are, for example, facilitated to a great extent by small units starting to use the same types of operating system as PCs, so it would also appear obvious to use the same methods for protection. The same applies to the screening of RFID tags used to prevent shoplifting, for example, where the best solution would appear to be keeping an eye on the problem to ensure that it does not happen; it is no different, in principle, to normal shoplifting.

7.1.5 General recommendations

If we leave out the legal mechanisms described above, good pervasive computing solutions have a number of desirable technical properties from a security perspective:

- The protection of privacy, including minimal or no registration of data that can be traced back to a specific person
- The use of standard security mechanisms
- They support requirements for the use of strong encryption, if required
- Good usability.

One recommendation that has been considered concerns a security declaration for the units and systems used in pervasive computing. This kind of declaration could, for example, state which mechanisms are used to protect identification, the observance of any rules for the protection of sensitive and personal data, and information related to privacy (such as which data a system registers, or whether or not a unit “voluntarily” transmits ID codes). However, it does seem difficult to quantify this in a good way (e.g. there may be great disagreement as to whether a specific protocol actually provides secure identification).

An entirely different perspective on how these desirable properties can be communicated is to demonstrate their worth in practice. It may be interesting to implement a national project as a lever for the use of pervasive computing technologies, such as RFID, in order to demonstrate that these properties can be realised in a commercial solution, and that, in particular, the obvious vulnerable spots that are identified in section 6.1 can be countered by technical means. This kind of RFID project could focus on an area in the retail trade, or similar public areas, such as libraries[46].

It is recommended that a project be implemented to demonstrate the use of RFID in the retail trade, or a similar area, in such a way that privacy is safeguarded by technical means.

The first step that ought to be taken in this kind of project is to provide a more detailed definition of the desired security requirements[47] and specific ideas for their realisation[48]. It is naturally also important to carry out an economic assessment, to ensure that the project is relevant.

7.2 Long-term perspective

The major new problems in a long-term perspective are assessed to be:

- Integrity, and specifically
  - Non-repudiation
  - Trust
- Privacy
- Usability

7.2.1 Non-repudiation

A number of practical problems arise when agents conclude agreements that have to be non-repudiatable. There are already uncertainties about the legal validity of the “normal” Danish digital signature. It is evident that this problem will only be made worse by the fact that agents should now be able to conclude agreements on behalf of users as well. On the other hand, Denmark is one of the leading nations when it comes to the use of digital signatures, so it would obviously be a good idea to investigate the problem in more detail.

It is recommended that an investigation be carried out into the extent to which it is legally feasible to allow agents to conclude valid agreements on behalf of their owners.

[46] In fact the Danish National Library Authority is waiting before recommending the use of RFID, because of concerns about privacy, amongst other things [The Danish National Library Authority].

[47] These requirements could include a book’s tag only being able to be read by the library and the borrower, but not by other borrowers or other RFID systems, for example; or, a bit more extreme, perhaps the library should not even be able to scan books that are out, as long as they have not been returned, even when they are physically in the library. Moreover, the users should naturally be able to scan the books at home themselves.

[48] A need may arise for more sophisticated RFID tags that can perform certain calculations.

It may appear unrealistic that agents should be able to do this at all, but it is a key element in agents-in-everything. For this reason, it would seem reasonable to adapt our conceptions of the future use of pervasive computing to the requirements the law makes of the technology, if it is to be used in practice.

One possible conclusion is that the user should always be involved in the final consummation of the agreement, but this kind of conclusion questions the whole value of agents – at least in the way they are described in the agents-in-everything scenarios.

7.2.2 Trust

As mentioned earlier, it is unlikely to be realistic to expect a single global infrastructure for digital signatures or the like. However, a number of regional infrastructures can be expected to be established, and we might also expect some of these to be able to be linked together. This would, for the most part, be sufficient for advanced cryptographic techniques to be able to ensure communication between different agents – including the conclusion of binding agreements. The establishment of such an infrastructure will not, however, solve the "human aspect of the problem": how we establish trust between people, units and agents who do not already know one another. As mentioned in section 6.3.5, this is an area in which a great deal of research is being carried out, but no glittering solution has, as yet, been found.

7.2.3 Privacy

There are two things to add here, in relation to the short-term discussion. In the long-term, pervasive computing can naturally be expected to be more widespread than in the short-term, which may in itself give rise to an escalation of the problems. On the other hand, the technology can also be expected to be further developed: RFID tags that can carry out cryptography are, for example, already underway, and in the long-term it is generally to be expected that even very small units will be able to perform calculations that can help to secure privacy. This may make it easier to realise some of the technical solutions that are already known (see section 6.1.4).

As already mentioned, the determination of which technical solutions that secure privacy are of practical use should be subject to continuous appraisal. The use of more technically-oriented solutions to secure privacy will always be a balancing act between different factors, including the capabilities of the technology, and what it costs. This kind of appraisal could be ensured by appointing a group of experts responsible for following the development in technical methods aimed at protecting privacy.

It is recommended that a group of experts be appointed to follow the development in technical methods for protecting privacy.

One of the first tasks for this group of experts could be to help to lay down the requirements for the project described in section 7.1.5.

Please note that, just because there are technical solutions to protect privacy, it does not necessarily mean that they will be used, unless the parties who invest in the solution can see a commercial advantage in it[49] - or unless it is required by law. Thus, it cannot be ruled out that public initiatives, such as in the form of projects as described in section 7.1.5, will be required to get these solutions off the ground.

7.2.4 Usability

In extension of the short-term discussion, it can be added that in the long-term it is probably more realistic, and more necessary, to do something about the problem of usability, due to the more widespread use of pervasive computing.

As mentioned above, usability can be improved by increasing the user’s understanding of the system. The opposite perspective is naturally that the system’s understanding of the user be improved, i.e. where the system is constructed so that it fits naturally into its intended application[50]. This poses a challenge to a number of technical solutions, including solutions intended to give the user increased control over the ID code on an RFID tag, for example. A large number of these kinds of solution suffer from the weakness that they typically impose a burden on the user, in the form of managing a key, because they are based on various forms of cryptography. Thus, it is often the case that technically smart solutions require technically “smart” thinking users, and when the technology becomes common property, this will not be the case.

The development of security solutions with good usability could be based on knowledge of sophisticated technical security (such as cryptography), as well as knowledge of usability. Denmark has a good tradition for technical security, and for developing IT with good usability. This would appear to be an obvious opportunity to try to combine these areas of research in order to address some of the problems identified here.

It is recommended that resources be put into Danish research and development that integrates usability and technical security.

[49] Various systems for anonymous payment have been developed, for example, but they have never caught on.
[50] Jakob Nielsen argues for this approach rather than the education of users [Nielsen].

8 Appendices

The following appendices are attached to this report:

- Appendix 1: References
- Appendix 2: Detailed legal analysis
- Appendix 3: Proposed industry code
- Appendix 4: Scenarios

9 Preparation of the report

This report has been prepared by the Alexandra Institute's Centre for IT Security, in collaboration with Peter Blume, Professor LL.D., from the University of Copenhagen.

The following have taken part in the project group on behalf of the Alexandra Institute's Centre for IT Security:

- Michael Østergaard Pedersen, PhD student at the University of Aarhus
- Jakob Illeborg Pagter, Assistant Professor at the University of Aarhus, and Project Manager at the Alexandra Institute's Centre for IT Security, and
- Torben Pryds Pedersen, CTO, Cryptomathic A/S