Pervasive Computing: Trends and Impacts

www.bsi.bund.de
The present study was prepared for, and in cooperation with, the German Federal Office for Information Security (BSI) in an interdisciplinary collaborative arrangement between VDI/VDE Innovation und Technik GmbH, Fraunhofer Institute for Secure Information Technology und Sun Microsystems GmbH.

The expert survey upon which this study is based was carried out in the summer of 2006. The present study reflects exclusively the opinions of the experts who worked on it, the ones who were surveyed and the literature referred to. Any trademarks, product names or product illustrations or logos are being shown only to identify the products, and may be registered trademarks of the respective manufacturers. Trademarks, registered trademarks and product names are trademarks or product names of the respective holders.
Pervasive Computing:
Trends and Impacts
Federal Office for Information Security

Pervasive Computing:
Trends and Impacts

SecuMedia
1 Foreword
2 Summary – Pervasive Computing: Developments and Impact
  2.1 The two stages of pervasive computing development
  2.2 Characteristics of pervasive computing
  2.3 The technological foundations of pervasive computing
  2.4 Drivers and hurdles in pervasive computing
  2.5 The impact of pervasive computing
    2.5.1 Impact on privacy
    2.5.2 Economic impact
    2.5.3 Social impact
    2.5.4 Winners and losers in pervasive computing
  2.6 Pervasive computing safety
  2.7 Study overview
3 Methodology
  3.1 International online survey
  3.2 Qualitative in-depth interviews
4 Areas of Pervasive Computing Application
  4.1 Logistics and production
  4.2 Motor traffic
  4.3 Inner and external security
  4.4 Identification systems
  4.5 Smart homes
  4.6 Electronic commerce
  4.7 Medical technology
5 The Technology of Pervasive Computing
  5.1 Microelectronics
  5.2 Power supply
  5.3 Sensor technology
  5.4 Communication technology
  5.5 Localisation technology
  5.6 Security technologies
  5.7 Machine-machine communication
  5.8 Human-machine interface
6 Pervasive Computing: Socio-economic Requirements and Impact
  6.1 Pervasive computing drivers
  6.2 Limiting factors in pervasive computing
  6.3 Anticipated impacts of pervasive computing
    6.3.1 Impact on privacy
    6.3.2 Economic impact
    6.3.3 Social impact
    6.4 Winners and losers in pervasive computing
  6.5 Pervasive computing: assessment of technology effects—conclusions and consequences
7 Security in Pervasive Computing
  7.1 Scenario 1: Object identification with TPM
    7.1.2 Security of object identification via TPM
    7.1.3 Opportunities and risks of object identification with a TPM
  7.2 Scenario 2: The universal ID
    7.2.1 The biometric identification system of UID according to ICAO
    7.2.2 The security of a universal ID
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.3</td>
<td>Universal ID: opportunities and risks</td>
<td>74</td>
</tr>
<tr>
<td>7.3</td>
<td>Scenario 3: Distributed telematics systems</td>
<td>75</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Security in decentralised telematics systems</td>
<td>76</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Opportunities and risks in distributed telematics systems</td>
<td>80</td>
</tr>
<tr>
<td>7.4</td>
<td>Outlook Security requirements for future pervasive computing</td>
<td>81</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Privacy in pervasive computing</td>
<td>81</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Security</td>
<td>83</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Safety</td>
<td>83</td>
</tr>
<tr>
<td>7.4.4</td>
<td>First steps toward a privacy-compliant pervasive computing</td>
<td>84</td>
</tr>
<tr>
<td>8</td>
<td><strong>Future Outlook</strong></td>
<td>86</td>
</tr>
</tbody>
</table>

List of abbreviations

Index

Bibliography
Authors and Experts

Authors

This study was authored by

VDI/VDE Innovation + Technik GmbH

• Peter Gabriel
• Dr. Marc Bovenschulte
• Dr. Ernst Hartmann

assisted by:

• Wolfram Groß
• Dr. Hartmut Strese

Fraunhofer Institute for Secure Information Technology SIT

• Dr. Kpatcha M. Bayarou
• Michael Haisch
• Manuel Mattheß

Sun Microsystems GmbH

• Dr. Christoph Brune
• Heinz Strauss

Federal Office for Information Security (BSI)

• Harald Kelter
• Rainer Oberweis

Experts

We would like to thank the experts who participated in the in-depth interviews:

• Prof. Dr. Lorenz Hilty,
  Swiss Federal Laboratories for Materials Testing and Research EMPA, St. Gallen

• Dr. Hartmut Raffler, Siemens AG, München

• Dr. Sarah Spiekermann, Humboldt-University, Berlin

• Dr. Reinhold Eberhardt
  Dr. Matthias Stümpfle,
  DaimlerChrysler AG, Ulm

• Dr. Werner Weber, Infineon AG, München

In addition to the experts mentioned above we would like to thank all experts who participated in the empirical online survey
Dear Reader,

The dissemination and use of modern information and communication technologies (ICT) are considered to be preconditions today for dynamic economic growth and future viability in global competition. At the same time, the processes of change triggered, enabled and accelerated by ICT are enormous. The new technologies have an ever-expanding ripple effect on the economy, public administration, science, scholarship and private life. They exert influence on social and individual life. The development of mobile telephony and Internet technology during the past ten years exemplifies the transformative potential of ICT.

Digital information and services are going mobile and can be called up from any location. A trend toward pervasive computing is emerging – that is, the ubiquitous and invisible use, creation, processing, transmission and storage of information. The “computerisation of the world” is being accelerated by technological and economic developments. Everyday objects are becoming “smart objects”, which are linked together into networks, react to their environment, and interact with their users.

Along with serving the German federal government as its IT security provider, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) also deals with future perspectives in ICT. Current examples from the BSI’s research programme are the study “Communication and Information Technology 2010+3” and the RIKCHA study on the opportunities and risks posed by the use of RFID systems. The present study on the development and impact of pervasive computing carries on this fine tradition.

The study’s findings underscore the fundamental potential of pervasive computing. They also show, however, that different application areas and sectors will profit from this potential at different speeds and with qualitative idiosyncrasies. In addition, the study makes clear that pervasive computing not only poses technical problems, it also comprises serious social, economic and judicial challenges that require active solutions and management. As has often been the case with technical innovations and advances, pervasive computing raises the question of what sort of future we want. The study should, on the one hand, contribute to greater objectivity in this discussion. On the other hand, it is intended to outline enough different issues so that a multitude of social groups and actors will be drawn to participate actively in the discussion on pervasive computing.

I thank the consortium that prepared the study for its successful work. I especially want to thank the experts who made their knowledge available to us in interviews and the online survey. They helped us greatly to get a preview of the exciting future of information and communication technology.

Dr. Udo Helmbrecht
President of the Federal Office for Information Security
2 Summary – Pervasive Computing: Trends and Impacts

Pervasive computing is about making computers invisible to people.

Henk Muller, University of Bristol, Great Britain

For more than 30 years, microprocessor performance has doubled approximately every 18 months. Similar progress in performance has been made in other technology parameters, such as data transfer rates in both wired and wireless networks. This trend is shaping a future in which computers will become increasingly smaller and inexpensive, and therefore abundant. In recent years, smaller personal devices such as PDAs, smart phones, palmtops and subnotebooks have begun supplementing and to some extent replacing traditional computer platforms such as workstations, PCs and servers. Computers are integrated increasingly into everyday devices and expand their operational capacities. These so-called embedded systems, such as driver assistance systems in cars or flexible software-driven boiler regulation can be controlled using a PC in the office or via mobile telephone.

As early as 1991, Mark Weiser, the former Scientific Director of the Xerox Palo Alto Research Center, shaped the vision of Ubiquitous Computing as an omnipresent infrastructure for information and communication technologies (ICTs). His work on ubiquitous computing continues to define all technological and socio-political considerations inherent to the field. According to Weiser, we can speak of ubiquitous computing once the following four criteria have been met:

- Microcomputers are integrated into physical objects of any shape and displace services heretofore performed by desktop systems.
- These embedded systems are characterised by their small size and by their near invisibility to the user.
- Embedded microcomputers thus augment a physical object’s original use-value with a new array of digital applications.
- The ubiquitous availability of services lies at the centre of communication between device and application—not the device itself. This last point is what distinguishes ubiquitous computing from the familiar mobile networks of today. Ubiquitous computing is characterised by the omnipresent and mobile availability of services themselves, regardless of the target platform. Services will be tailored to the physical capacity of a specific device, whether a mobile telephone, PDA or other value-added communications device. [Weis 91]

Advances in microelectronics and communications technology have moved the technical vision of ubiquitous computing into the realm of the possible. Early examples of ubiquitous computing in use include processor module integration into identification documents and the integration of transponders into cargo pallets that send ID numbers to a reader automatically. In professional circles, the term Pervasive Computing is used commonly to describe the ubiquitous ICT infrastructure aimed at feasible short and medium-term solutions.

Pervasive computing is viewed less as a discrete field of technology, but rather as an emerging application of information and communications technology that is integrated into the everyday world more than ever before. The goal is to meet the claim of “everything, always, everywhere” for data processing and transmission through the ubiquity of ICT systems. The following characteristics define this application paradigm:

- Miniaturisation: ICT components are becoming smaller and more mobile.
- Embedding: As ICT components are integrated into everyday objects, they transform them into smart objects.
- Networking: ICT components are linked to each other and communicate generally via radio. They are therefore not part of a fixed environment or application, but are instead designed to form networks spontaneously. To prevent human attention from being overwhelmed, people are intentionally not integrated into many machine-to-machine interactions.
Ubiquity: While embedded ICT components are increasingly ubiquitous, they are at the same time increasingly less noticeable – or even invisible – to most people. Most components will interface with their surrounding environment in several ways but will not be visible.

Context awareness: ICT components use sensors and communication to collect information about their users and environment and adjust their behaviour accordingly. [Hilt 03]

Pervasive computing is thus a complementary paradigm to virtual reality. Rather than reproduce and simulate the world with a computer, pervasive computing turns all objects in the real world into part of an information and communications system. Overlapping each other, the real and virtual worlds are joined.

Pervasive computing will change the ways in which we use computers drastically. Whereas today’s ICT products and services are generally used consciously, this will change with pervasive computing. As computers are integrated into everyday objects, they will no longer be perceived as such and their usage will recede largely from our conscious perception. In pervasive computing, a variety of processes run automatically in the background and interact on behalf of the user. The user does not have to provide explicit instructions or make decisions. Pervasive computing involves smart environments that are envisioned as an individual’s cooperative partner. However, the seeming disappearance of the computer together with the delegation of complex processes or tasks to a ubiquitous ICT infrastructure raises serious questions. How secure are these systems? How can one determine whether they act truly on behalf of their respective users? How will the enormous amounts of data generated by these processes be handled? Can the individual user exercise the right of privacy and prevent his or her data from being passed on, stored, compared and analysed? Doesn’t the vision of pervasive computing permeating our everyday environment entail an immeasurable increase in resource and energy consumption? How can a potentially fatal dependence on technology be prevented? As the majority of commercial, administration, trade and recreation transactions become impossible without pervasive computing support or are provided in the form of pervasive computing only, will this not lead to a forced usage thereof? How will pervasive computing develop and what impact will it have?

May 12, 2018

It’s nearly 7 a.m. and the sun is shining. As the Sleep Manager gently wakes Lukas up from his deep sleep with a soothing massage, he notes that his soreness from yesterday’s ambitious water squash game has, for the most part, vanished. The first thing he reaches for is his identification wristband – a few moments later, he stands with a satisfied expression before the mirror as it takes a few important vital signs. Everything looks good. Feeling “made of iron”, Lukas chuckles over how archaic language can be in comparison to all the new materials now available. But then, who wants to be made of a polymer? Ugh. While eating breakfast on the terrace, Lukas watches the latest news from work on the terrace wall; the report from Hong Kong captures his full attention. “Let me guess – you have to leave today because everything is moving along faster than expected?” asks Anna. A short nod of confirmation, meant as much for his wife as for the projection on the wall, and the Planning Routine is already checking possible connections, synchronising them with the current schedule in Hong Kong, loading the necessary meeting and travel documents, determining the local weather data and, working with the Event Tab, it creates a clothing list, reserves a room in a hotel near the event site and suggests three options for the little free time Lukas will have. Lukas quickly scans the schedule in full-security mode; he chooses the Frisbee quarter-finals for the evening and authorises the entire process. He opted out of the boring standard translator module. Lukas has just discovered a new agency offering an “emotional translator”, which will help him translate moods and allow him not only to understand Chinese irony, but be ironic in Chinese as well. “Did you stay out late?” he asks his wife. “Not really – it’s the Cerveza that’s still coursing through my veins. Cerberus warned me, but of course I ignored him.” Cerberus is Anna’s nickname for her Wellness Monitor, which suggests healthy behaviour tailored to her fitness level on any given day. “I’m sure he’s set the treadmill for 45 minutes instead of 30 again.”
It’s half-past eight and pouring rain. Anna jumps out of bed, startled. This is the first time she has overslept since owning a Sleep Manager, and she still isn’t certain whether yesterday’s news of a new computer virus was a dream or not. Feeling somewhat rushed and grumpy, Anna steps into the shower. It is still set to her youngest daughter’s height. The ruddy thing doesn’t react to her ID wristband, and she can’t adjust the showerhead by hand. Following a much-too-hot shower, Anna stands before the mirror looking as red as a lobster. The mirror begins the morning health check as Anna thinks about the good-morning greeting from Hong Kong. “Why is it so cold in here?” she grumbles to herself as Cerberus urgently advises her to go back to bed and sleep off her fever. “What fever?” Anna asks herself, “can’t the sensor tell the difference between a hot shower and a fever? I just hope the thing hasn’t already called in sick for me!” But her employer has in fact already been informed – having registered her oversleeping, bad mood and elevated body temperature from the hot shower, Cerberus has reached the conclusion that Anna is sick and therefore unable to work. Then Lukas appears on the InterCom. “Would you believe my luck, all systems are down here in Hong Kong, and at the moment we can’t even leave the hotel because the whole building was mistakenly set to ‘quarantine mode.’ Well, at least I can still take part in the meeting over the InterCom. But now I’ll have to watch the test run of the new plant remotely. I could have done that just as easily from home.” Anna is annoyed enough as it is. And to make matters worse, the FullSec security agent is now showing that some data from the last context update were intercepted. This means that in all likelihood, they will be used by obnoxious sales people to waste her time with profile spamming. To prevent this from happening, yesterday’s status will have to be re-established on her security provider Personality Online, which unfortunately means that the nice new Shopping Routing in her car will be lost. “Qué mala suerte – unbelievable that one still has to take care of these things oneself these days,” she thinks, “and then you get slammed with a hefty fee too, just because someone at P-Online presses the button!”

No one knows whether pervasive computing will actually develop in ways similar to these two intentionally opposite scenarios. Clearly, however, similar applications and elements – with both negative and positive characteristics – will emerge in upcoming years and have far-reaching socio-economic effects.

This study examines the projected technological development of pervasive computing, its socio-economic impact and the potential dangers to security, privacy and safety. An online survey and in-depth interviews were conducted with national and international experts alike to gather their assessments of trends in technology as well as the social and economic impact of pervasive computing. In addition, the study includes a close examination of the security issues in pervasive computing, which is based on three scenarios. This study is intended to provide a differentiated perspective on the opportunities presented by and impact of pervasive computing. It aims to provide decision-makers in politics and industry with a foundation for future action in a networked world. The study thus ends by identifying the fields of action in which pervasive computing will be shaped in the future. For those interested in pervasive computing, it seeks to demonstrate which uses for smart objects can be expected, and how they will influence our lives in the future. The following sections of this chapter introduce the study’s key results. An overview of the rest of the study can be found at the end of this chapter in section 2.7.

2.1 The two stages of pervasive computing development

Responses provided by the surveyed experts suggest that current views on pervasive computing are shaped heavily by short-term considerations. Highly developed pervasive computing capacities – such as application autonomy – are not mentioned, for the most part. The study’s findings indicate that pervasive computing will develop in at least two stages: The first stage, PvC-1, will see numerous products and applications characterised by the goals of mobility and ad-hoc networking becoming established within the next five years. This will essentially be a continuation of current trends, such as the
miniaturisation and integration of various functions in an electronic device to the point of creating smart objects. During this stage we can expect to see context awareness realised in a simplified form, e.g., in the form of user profiles. Despite their permanent linkage to communications and data networks, these smart objects will remain largely isolated solutions that join together a great number of capabilities, especially those relating to communications and data processing. In a parallel process, more and more everyday technical objects will be increasingly outfitted with microcontrollers, sensors, etc., and thus upgraded to smart objects. Their capabilities will be tailored to specific tasks and provide simple forms of networking. As these parallel trends converge, they will lead to isolated applications that are defined by specific use models or manufacturers. During this transition phase, media ruptures among isolated applications will be overcome; their barriers to other solutions/applications will remain. The second stage, PvC-2, will take hold only in the wake of this interim stage of isolated applications. We will then see the emergence of a truly open networking structure without media ruptures. The experts surveyed estimate that PvC-2 will establish itself in roughly 10 years (see figure 1).

During the PvC-1 phase, pervasive computing’s characteristics and capabilities will increase in number and make qualitative gains. The ability to perform operations in the background without receiving explicit commands is a central characteristic of the seemingly invisible ICT structure. In PvC-1, this kind of context awareness will at first be based on user profiles, much in the same way many Internet services are today. It is expected with some degree of certainty that these profiles will be Internet-based and then accessed and used by the individual smart objects. This profile-based context awareness will be extended significantly in PvC-2. In PvC-2, smart objects will be able to respond intelligently and on a case-by-case basis to the situational needs and/or environment of the user. Smart objects will therefore require well-functioning software agent technology that is based on artificial intelligence and knowledge management paradigms. These agents’ flexible world models permit a functional, adaptive logic. User-defined action is therefore made possible in different – even unfamiliar – contexts.

Qualitative leaps similar to those expected in the transition from PvC-1 to PvC-2 are expected in pervasive computing’s impact as well. The embedding of pervasive computing components into a vast number of everyday objects will pose new challenges to recycling. The integration of pervasive computing components will turn those objects, which are currently relatively homogeneous, into mixed-material objects. They will no longer be compatible with current recycling methods, which are based on unmixed materials. Labourious pre-treatment and/or entirely new procedures will be required, even for some of today’s ordinary consumer materials.

The number of components in pervasive computing will grow significantly during the transition to PvC-2 as media ruptures will have been overcome, the technology will have matured, and the cost-effective mass production of products and applications will have begun. The number of smart objects will increase rapidly. On the one hand, this means recycling will constantly face new qualitative challenges; on the other hand, the cumulative impact of these changes will push the existing recycling infrastructure to its limits.

Figure 2 illustrates the key development trends and cross-linkages in pervasive computing. It provides a highly condensed illustration of the prospects for pervasive computing development. The following overview is therefore intended to introduce the study’s key findings for individual dimensions of
pervasive computing. These findings are based upon the survey of experts conducted and the professional literature on pervasive computing.

2.2 Characteristics of pervasive computing

Pervasive computing can be characterised by a set of attributes and capabilities that describe the extent of its functionality. Mobility and ad-hoc networking capabilities are expected to emerge relatively soon, that is within the next one to two years. Characteristics such as autonomy, context awareness and energy autarky are not expected until later, taking anywhere from five to ten years. Context awareness and embedment in everyday objects are viewed as pervasive computing’s definitive and formative characteristics. Energy autarky and the autonomy of components and systems, in contrast, are considered secondary characteristics.

It therefore stands to reason that pervasive computing will establish itself gradually as its individual characteristics develop step-by-step. Although market-ready pervasive computing applications are anticipated in the next four to eight years, the characteristic of autonomy is not expected for another ten years. Also, the individual characteristics vary in relevance depending on the field of application. For example, the autarkic power supply of pervasive computing components and their mobility are relatively unimportant for the smart home, whereas these characteristics are key to communications applications.

2.3 The technological foundations of pervasive computing

Communications technologies and microelectronics in particular are key requirements for almost all pervasive computing applications. Although energy autarky is certainly not an important characteristic of all pervasive computing applications, supplying energy is clearly a central task. Maturation and availability of pervasive computing-relevant technologies is expected soon, within the next one to four years; nearly all of the technological requirements needed for pervasive computing should be met in the foreseeable future. Unresolved problems with power supplies, an inadequate human-machine interface and a lack of well-functioning security technology pose particularly serious bottlenecks to the development of pervasive computing. Further differentiation reveals the following as potential technological bottlenecks:

- There are two aspects worth noting in power supply: Batteries and accumulators are important requirements for pervasive computing, and – despite their high availability – should be regarded as a technological bottleneck. Considerable development is needed on this point, despite the availability of current solutions. Energy harvesting – the extraction of energy from a device’s surroundings – is seen as an alternative technology of the future. Micro fuel cells are not of key interest.

- Regarding human-to-machine interfaces, processing natural speech is given high priority. It is considered a comparatively mature technology that could nonetheless represent a technological bottleneck.

- In the field of security technology, biometric identification technologies are considered less relevant for pervasive computing and are therefore rated as a less critical bottleneck, especially when compared to other security technologies such as trust management and identity management.

2.4 Drivers and hurdles in pervasive computing

The realisation of new products and services are the primary driving forces behind the development and establishment of pervasive computing. Depending on the area of application, the importance of cost savings and increases in energy efficiency or comfort can vary significantly. In production and logistics, for example, reducing costs via pervasive computing is considered very important. In military applications, however, cost savings functions as a weak motivation. Using pervasive computing to improve safety is considered important for motor traffic as well as the security, military and medical sectors. However, improving safety is not a motiva-
tation in other application areas for using and developing pervasive computing. Enhanced comfort and improved usability are seen as significant driving forces in the automotive and household industries. Potential cost savings and improved energy efficiency play only minor roles in these two areas. In medical technology, however, there is a broad spectrum of motivations for using pervasive computing, which is seen as a key strategy in solving several different problems in this sector.

Analogous to the driving forces behind pervasive computing’s development and application, there are identifiable limiting factors that could – whether directly or indirectly – influence pervasive computing. These include shortcomings in human-machine interfaces and data protection as well as technical hurdles to availability and reliability. These limiting factors are real, despite the fact that the core technologies of pervasive computing are expected to be market-ready within the next one to four years.

According to the experts surveyed, environmental sustainability, resource consumption and legal regulation are minor limiting factors in pervasive computing’s successful development. They assign a great degree of importance to standardisation, however, as the functional interplay of individual components is a key requirement of pervasive computing. The relevance of individual data protection and privacy varies depending on the specific application. Whereas privacy is not a primary concern in production and military applications, it is an important limiting factor in security, communications and medicine. The relative weight given to privacy varies among the various professional groups surveyed. Across the board, experts working in industry assign less importance to this limiting factor than experts outside industry do.

---

*Fig. 2:* Key trends, developments and dependencies in pervasive computing. (Arrows within the category describe evolutionary processes, arrows reaching across categories represent influences.)
2.5 The impact of pervasive computing

Pervasive computing will permeate everyday life – both private and working – and is therefore expected to have far-reaching consequences that will be reflected in a variety of socio-economic contexts. Both positive and negative effects are likely in equal measure at several levels. Safety versus privacy, for example, make up two ends of one key pole. The following overview presents the pervasive computing’s impact in terms of privacy, economics, society and the digital divide.

2.5.1 Impact on privacy

In terms of privacy, slightly positive effects are expected for the application fields of security, medicine and production; moderately negative effects are expected in other application contexts. A pervasive computing design for privacy that conforms to data protection standards is regarded as a requirement for ensuring privacy and is preferred to the downstream concept of context-dependent data protection filters (digital bubbles). Only a system architecture that protects privacy from the outset can prevent serious conflicts in data protection from developing. In the use and processing of data, rendering all steps in the process visible and logically comprehensible seems to be of less importance. Far more crucial is a user’s explicit trust in a particular pervasive computing system that the service provider will handle personal data responsibly. Apart from this concern, there is the danger that frequent use of a pervasive computing application could potentially lead to the inattentive handling of personal data. This means that the premature availability of a groundbreaking pervasive computing application could result in limited public attention being given to the protection of privacy during its crucial phase of implementation.

2.5.2 Economic impact

Among the economic effects associated with pervasive computing, work efficiency in particular is expected to improve. This will become most apparent in the key economic areas of production, logistics and commerce. This will not, however, play a role in smart homes. It is worth noting that no significant efficiency gains from pervasive computing are expected for housework, professionals working at home, and homecare of the elderly and/or ill. The motivation for introducing pervasive computing into the smart home is to increase personal comfort, which is not quantifiable in economic terms. Experts apparently anticipate effects similar to those resulting from the introduction of modern household appliances during industrialisation. Back then, the time saved by the use of new appliances was counteracted by increased demands in hygiene and cleanliness, which resulted in extra work. Moderately positive effects are anticipated for increasing energy and resource efficiency in all areas of application. Significant increases are expected, however, in production and especially logistics. Indeed, pervasive computing’s potential for commerce and production is immense because of its ability to self-organise and control industrial processes. Such self-organisation depends on several things, including the availability of fully developed knowledge-based systems. Developing these systems in turn, however, poses a significant challenge. Finally, newly adapted recycling procedures will be needed to allow for the re-use of pervasive computing components that have been integrated and embedded into everyday objects.

2.5.3 Social impact

Clear positive effects are predicted for pervasive computing’s support of personal activities in medicine, the home, communications and automobiles, while moderately positive effects are expected in inner and external security, and in production, logistics and commerce. Improvements in safety are anticipated primarily in military and security-related applications, but especially in medical applications. The automotive branch will also profit somewhat, according to expert opinion.

On balance, pervasive computing is not expected to produce any negative “rebound effects”, which would offset or even negate pervasive computing’s positive effects. This is true for work and attention efficiency, resource consumption and for man’s ability to orient and locate himself in his environment. In Germany, this view is held primarily by
those employed in the industry. Experts elsewhere, who are employed in the industry, expect instead a disproportionate increase in resource consumption resulting from pervasive computing.

2.5.4 Winners and losers in pervasive computing

The experts identify several social groups as winners and losers in pervasive computing. The elderly and persons with little experience with technology stand out as groups that could benefit from pervasive computing and be disadvantaged by it as well. How might this paradox come about? The first generation of pervasive computing applications in particular are likely to demand a certain level of knowledge and requirements that will result in a temporary division between pervasive computing’s winners and losers. However, this divide should subside as the functional logic of later pervasive computing generations is automated and cost-effective mass production sets in. According to one of the experts, “Once the technology has matured and becomes publicly available, the less educated will begin to profit from it. If this does not happen, they will continue to fall behind.”

It is therefore imperative that a pervasive computing infrastructure offers accordingly easy access, whether in technical, financial or intellectual terms. Otherwise, a digital divide between those with and those without access to pervasive computing will emerge. Other groups that experts believe could suffer disadvantages as a result of pervasive computing include small businesses and retail, political minorities, critics or sceptics, marginal groups and persons with “unusual” backgrounds. Also mentioned in this context are persons who intentionally avoid participation in a pervasive computing-based system or those who cannot participate. There are two dimensions to the potential disadvantages resulting from pervasive computing: those associated with surveillance and those associated with an inadequate access to pervasive computing-based infrastructures and services. Pointing to entire countries lacking a pervasive computing infrastructure, some experts also speak of a digital divide on the global level.

2.6 Pervasive computing security

In pervasive computing, a large number of smart objects communicate with one another or with the user. Many of these interactions should be as inconspicuous and situationally dependent as possible, and thus occur semi-automatically. The user will often no longer take conscious note of the smart objects’ actions. To some extent, the user will neither want nor be able to do so. The usual means of control and correction within IT systems will not apply here. Protecting system security in pervasive computing is therefore very important. This includes security, privacy and safety. Security involves preventing unauthorised persons from viewing and therefore potentially manipulating confidential data. Likewise, communication must remain confidential and may not be interfered with. The meeting of digital identities must be at least as trustworthy as meeting in person. Known and tested security technologies and methods are already available. However, they need to be adapted to pervasive computing’s peculiarities – especially the frequent limited performance of smart object hardware and to the marked decentralisation of infrastructure, services and objects. There is an inherent conflict between pervasive computing’s goal of accurately identifying persons, objects and messages (authenticity), and the desire for anonymity – to prevent data trails from the outset. This problem can be addressed through digital pseudonym technology—somewhat. In the end, the competing security goals of authenticity and anonymity must be considered individually for each application.

Pervasive computing will see the accumulation of vast amounts of data that can provide a comprehensive overview of an individual, his or her behaviour, finances and health. These huge sets of data and the spontaneous networking of smart objects will make it impossible for the pervasive computing user to trace where one’s personal data are stored, how they are used and how they might be combined with one another. In pervasive computing, data protection is therefore an essential requirement for protecting privacy – even more so than in other IT systems. Today’s principles and rules for protecting privacy also apply to pervasive computing.
The networking of pervasive computing is not limited to individual states because several services will not fully evolve until they are made available across borders. This internationalisation requires standardised international regulations guaranteeing privacy protection. Currently, however, there are still highly disparate approaches to preserving the private sphere in the digital world. These differences are illustrated clearly by the gap between Europe’s strict legal regulations and the comparatively open, self-regulatory approach in the United States. The global networking of smart objects and services, which is anticipated in the long run, will necessitate the creation of a standardised international regulatory regime for data protection in pervasive computing.

Pervasive computing’s invisibility and the complexity of its networking could mean that system failures and malicious interference go unnoticed, or are noticed much later. In some pervasive computing applications – such as medicine, traffic system control or in self-organised production lines – this could put human lives in danger and lead to extensive property damage. In applications where safety is crucial, the reliability of pervasive computing is essential. It must be guaranteed, for example, with system redundancy or a backup system.

2.7 Study overview

The in-depth interviews with six selected pervasive computing experts and the online survey of international and national experts make up one of the central pillars of this study. The methodology underlying the interviews and the online survey is presented in Chapter 3. Although pervasive computing currently represents a rather technological vision, its introduction is nevertheless being pushed forward by several areas of application, which are examined in Chapter 4. Pervasive computing is not a discrete technology; it is based rather on the interplay of an array of technology fields that are introduced in Chapter 5. Chapter 6 summarises the experts’ statements on the socio-economic aspects of pervasive computing: What are the driving forces and limiting factors? What impacts are anticipated? Who are the winners and losers when smart objects are introduced? The invisibility and ubiquity of pervasive computing make its safety a central question. This issue is addressed in Chapter 7 with three scenarios. As it is still far too early for a final word on pervasive computing, Chapter 8 identifies key areas where action is needed in the coming years to ensure that the variety of groups and actors in society, politics and industry are able to profit equally from pervasive computing.
3 Methodology

3.1 International online survey

A central foundation of this study is an international survey of experts. The survey was conducted with an online questionnaire from August 15 through September 26, 2005. Invitations to participate in the survey were sent by letter and email to 298 experts. One hundred of them signed up online for the survey, and 83 of them actually completed the questionnaire. Engineers and natural scientists were heavily overrepresented among the respondents, while social scientists and economists were underrepresented (see Figure 3).

Scholars were definitely represented more heavily than were experts working in industry. Other fields, such as the public sector and NGOs, were weakly represented (see Figure 4). This distribution was predetermined by the selection of experts, and it reflects the fact that pervasive computing remains mostly a topic for technological research.

The largest share of the participants came from Germany, as is only to be expected from a survey carried out by a German consortium on behalf of a German institution. However, the United States and Japan – countries vital to pervasive computing – were also represented by good-sized contingents (see Figure 5).

The online questionnaire used scales for evaluating relationships and statements. Space was provided for open-ended comments or in-depth responses. All scales in the online questionnaire were rating scales and were evaluated statistically. As is customary in the human and social sciences, the rating scale scores were regarded as interval-level measurements and analysed accordingly.

3.2 Qualitative in-depth interviews

In preparation for the international expert survey, six experts were asked about the development and impact of pervasive computing. A modified structure-formation technique was used here [Sche 88]. This method was intended to produce a sketch of the development of pervasive computing over time.
from today until 2015. The individual aspects of pervasive computing were then visualised in a grid structure comprising four categories on the vertical axis and change over time along the horizontal axis. The visualisation depicts evolutive processes as well as cross-linkages with arrows (see Figure 6).

Especially meaningful cross-linkages were identified in the visualisations, and ten incisive hypotheses on the socio-economic and technical impact of pervasive computing were derived from them. In the sample visualisation shown in Figure 6, an incisive linkage was identified across all four categories of the grid (highlighted in colour) and the following hypothesis derived:

“Context-awareness requires pervasive computing components with a perception of their environment that relies on an ‘internal model of the world’. Knowledge-based systems and/or software agents are a key precondition for such models and could thus represent a serious technological bottleneck. Therefore, every effort must be made to find top-quality pervasive computing solutions in this area.”

The hypotheses were evaluated by the international experts using a preset rating scale in the online questionnaire.
Areas of Pervasive Computing

Application

Pervasive computing compares to a traditional PC like batteries to a power plant: not as powerful, but available everywhere, in different shapes, for many different applications.

Prof. Dr. Jochen Schiller, Freie Universität Berlin, Germany

Pervasive computing aims to permeate and interconnect all areas of life, and thus to enable a ubiquitous flow of data, information, and – by integrating cognitive capabilities in the future – even knowledge. Mark Weiser, one of the fathers of pervasive computing, described this vision of a continual and ubiquitous exchange transcending the borders of applications, media, and countries as “everything, always, everywhere.” This sketch offers a strongly future-oriented perspective on pervasive computing that is still far removed from today’s reality.

Although wireless Internet access, email via mobile phone, handheld computers and the like may give the impression that constant, unimpeded exchange of information is already routine, in the future the special performance characteristics of pervasive computing will enable an entirely new quality in the exchange and processing of data, information and knowledge. With pervasive computing, many of these processes will recede into the background, and most will occur partially or wholly automatically. But this new form of pervasive computing will not develop uniformly and synchronously in all economic and social areas. Rather, applications will be defined and implemented at different speeds in different contexts. For this study, nine application areas were selected in which pervasive computing is already recognisable and is very likely to play a decisive role in the future:

Communications: As a cross-application, the communications area affects all forms of exchange and transmission of data, information, and knowledge. Communications thus represents a precondition for all information technology, as well as one of its key domains.

Logistics: Tracking logistical goods along the entire transport chain of raw materials, semi-finished articles, and finished products (including their eventual disposal) closes the gap in IT control systems between the physical flow and the information flow. This offers opportunities for optimising and automating logistics that are already apparent today.

Motor traffic: Automobiles already contain several assistance systems that support the driver invisibly. Networking vehicles with each other and with surrounding telematics systems is anticipated for the future.

Military: The military sector requires the provision of information on averting and fighting external threats that is as close-meshed, multidimensional, and interrelated as possible. This comprises the collection and processing of information. It also includes the development of new weapons systems.

Production: In the smart factory, the flow and processing of components within manufacturing are controlled by the components and by the processing and transport stations themselves. Pervasive computing facilitates a decentralised production system that independently configures, controls and monitors itself.

Smart homes: In the smart home, a large number of home technology devices such as heating, lighting, ventilation and communication equipment become smart objects that automatically adjust to the needs of residents.

E-commerce: The smart objects of pervasive computing allow for new business models with a variety of digital services to be implemented. These include location-based services, a shift from selling products to renting them, and software agents that will instruct components in pervasive computing to initiate and carry out services and business transactions independently.

Inner security: Identification systems, such as the newly introduced electronic passport and the already abundant smart cards, are an essential application of pervasive computing in inner security. In the future, monitoring systems will become

---

1 This quotation and all others at the beginning of chapters come from respondents to the online survey. At the end of the questionnaire, they were asked to give a concise definition of the term “pervasive computing.”
increasingly important – for instance, in protecting the environment or surveillance of key infrastructure such as airports and the power grid.

Medical technology: Increasingly autarkic, multifunctional, miniaturised and networked medical applications in pervasive computing offer a wide range of possibilities for monitoring the health of the ill and the elderly in their own homes, as well as for intelligent implants.

Identifying each application area’s potential and estimating when we can expect applications to be established is essential to a well-founded prognosis of pervasive computing development. Because any such assessment is based on various definitions of pervasive computing and depends on variable contexts, we must first describe the performance features and characteristics of pervasive computing and then relate them to the selected application areas. In the online survey carried out for this study, pervasive computing was defined on the basis of six characteristics and correlated with the application areas (see Figure 7).

Expert opinion, on average, clearly places the general time horizon for pervasive computing realisation in the near future. According to expert opinion, no area will require ten years or more for the breakthrough of pervasive computing applications. However, it must be borne in mind that pervasive computing is characterised by a set of characteristics that range from mobility and embedding to ad-hoc network capability, and finally to energy autarky, context awareness and autonomy. These characteristics will not all become available simultaneously. They will reach full maturity asynchronously, as can be seen in the experts’ assessment (see Figure 8).

The experts anticipate that mobility and ad-hoc networks will be available imminently, with autonomy and energy autarky following considerably later. Notably, those surveyed expect the availability of essential pervasive computing characteristics of context awareness and autonomy to take significantly longer than five years.

In line with this expectation, it is not possible to foresee the identifiable – much less full – realisation of all of these characteristics for pervasive computing applications within the time horizons shown in Figure 7. Clear features of pervasive computing are, however, already emerging. According to the survey, autonomy will not become reality for about
another ten years, although pervasive computing applications are predicted in all nine application areas within the next four to eight years.

Due to the asynchronous development of pervasive computing, these characteristics are not equally relevant to the different application areas (see Figure 9). For example, mobility and power supplies for pervasive computing components are relatively unimportant for the smart home, whereas they are key to communications applications.

Mobility is generally regarded as an especially important characteristic, whereas autonomy is judged to be less crucial across all application areas. The two application areas that place the highest demands on pervasive computing are the military and mobile communications. Overall, it is notable that no single pervasive computing characteristic is crucial in all application areas. This suggests that the experts do not believe there is a universal pervasive computing application.

This assessment is supported by an open-ended query on milestones in the development of pervasive computing products and services. The experts’ responses indicate that there is no single application unanimously expected to produce a breakthrough. Several experts consider the products and services of mobile communications in particular as short-term milestone products. Many of them mentioned they expect to see milestones in mobile applications and location-based services during the next year or two – especially in applications for personal use. A handful of the experts also anticipate pervasive computing milestones in the fields of medicine, automobiles, home automation, and logistics within the next one to two years, but the majority expect this to take three to four years or longer. Demanding applications such as sensor networks, smart textiles, and car-to-car communication are expected in three to four years, at the earliest. Characteristics more specific to pervasive computing – such as context sensitivity and autonomy – will play an important role in these applications.

We can conclude from these responses that the contemporary international discussion on pervasive computing remains powerfully shaped by visions of the immediate future. Highly developed capabilities – such as application autonomy – have been largely neglected. This suggests that current trends do not yet represent full-blown pervasive computing, which may well need another ten years to become established. The present study’s findings indicate that pervasive computing will develop in at least two stages: The first stage, PvC-1, will see numerous products and applications characterised by the goals of mobility and ad-hoc networking becoming established within the next five years. This will essentially be a continuation of current trends, such as the miniaturisation and integration of various electronic functions in a single chip. During this stage we can expect to see more ambitious characteristics realised, too, such as context awareness in simplified form, e.g., in the form of user profiles. Truly pervasive computing, however, will emerge only in practical applications in the second stage, PvC-2, which will also reveal its novel characteristics. Context awareness will then actually mean intelligent, case-by-case reactions to the user’s needs and to the environment.

In order to sketch the possibilities of pervasive computing in central fields and sectors, this chapter introduces the relevant application areas and describes in detail their potential for pervasive computing. Logistics and production are discussed together because the two fields deal with related concerns. Similarly, the closely linked fields of inner and external security are combined. Public identification systems, such as the newly introduced electronic passport and the health ID card that are currently being tested in pilot projects, comprise a key area within inner security. Due to their current importance, identification systems are treated separately.

### 4.1 Logistics and production

Pervasive computing is already well developed in PvC-1 terms when it comes to RFID systems in logistics. Practically all logistical systems today – be they the in-plant flow of components, or the transport of consumer goods by truck, air, or rail between the producer and the market – are controlled and monitored by IT systems. These IT systems are based on identification systems in which a data carrier is affixed to an object, which can then be recognised...
by a reader. Such systems allow physical streams of goods to be tracked throughout the logistics supply chain and generate tracking data for the IT systems. Most identification systems in logistics today still rely on inexpensive barcode labels. However, these have a number of disadvantages. Reading a barcode requires a direct sightline to the scanner and as a result is usually a manual – and thus expensive – process. A barcode label can be dirtied or suffer surface damage easily. In addition, the barcode’s data cannot be altered. In RFID systems, by contrast, the data carrier is a transponder with a microchip that communicates with the reader by means of an electromagnetic field. RFID already has a long history of use in chip cards for access systems, in car keys, and in other applications.

Falling production costs and miniaturisation of transponders have allowed RFID systems to be used increasingly in tracking objects in logistical identification systems. These objects can be either goods or circular flowing logistics assets such as containers, pallets, or gas cylinders:

- Logistical objects can be automatically tracked and traced as they move along the supply chain. This allows closer, more precise tracking than is possible with barcode systems. One result of this is that warehouse stock reserves can be reduced. Manufacturers can reduce their inventory of logistics assets, which are often expensive. For foodstuffs, RFID offers a way to implement EU rules mandating traceability (EU Regulation 178/2002) from their sale through the entire supply chain back to their producers.

- A transponder is rewritable, in principle. It can thus carry product and process data for the manufacture, usage, maintenance, and disposal of a product, for instance. In industrial manufacturing, this can be used to create a “smart factory” where control functions are decentralised and production processes are therefore less error-prone.

- If cryptographic functions are integrated within a transponder, the authenticity of an object can be verified along the entire logistics supply chain. These functions are applied primarily in products requiring special protection from tampering or counterfeiting, such as medications and replacement parts for airplanes.

- Transponders with sensors can take on active control functions, such as monitoring the seamlessness of the cold chain for frozen products or for medications.

The use of RFID systems in logistics is a topic of intense discussion in many sectors. The retail area has received special emphasis, since the goal here is to implement RFID systems across companies and sectors. Because retail margins are very narrow and the leeway for cutting production costs has often already been exhausted, many retail companies and producers of consumer goods are thinking about new, cost-saving logistics concepts that allow products to be manufactured and delivered according to demand on a just-in-time basis. This should largely eliminate the need to maintain expensive reserve stocks in a variety of interim storage sites. In the salesroom, continuous monitoring of shelf inventory should prevent merchandise from being out of stock. The checkout process is to be sped up with automatic recognition of all products in the shopping cart. Large retail chains such as Metro, Wal-Mart and Tesco have begun applied testing of RFID technology at the pallet level with selected major suppliers. Pilot projects such as the Metro Future Store are also testing RFID-enabled labelling of boxes and individual products. Here, however, a number of technical problems remain unsolved. For example, the water and metal in products, packaging, shelves and shopping carts disrupt data transfer between an RFID chip and the reader. At least in the medium run, the high cost of transponders also stands in the way of RFID-enabled tags for individual products.

Other sectors have begun to experiment with RFID applications in production control and intralogistics. Automobile makers are currently concentrating primarily on projects in container management and the tracking of large workpieces (for example, car bodies as they move through the paint shop). More ambitious scenarios envision transferring some control functions from production planning and control systems to the workpiece itself, with the goal of decentralised, workpiece-related control of materials flow. This will enable real-time control of
the production system according to parameters such as current machine utilisation, production disruptions, and changes in job order prioritisation. Pilot projects are now underway at virtually all major car makers, including VW, BMW and Volvo. The major airplane manufacturers, Airbus and Boeing, are planning to implement RFID systems in conjunction with their main suppliers in order to improve the reliability of parts identification (which is mandated in aviation). The pharmaceutical industry is considering the use of smart labels in drug packaging in order to prevent counterfeiting of medications. For instance, in early 2005 Merck, Novartis, Schering, and Solvay conducted an RFID pilot project in 50 sales outlets in Great Britain. Pfizer has announced it will use RFID tags on Viagra packages to protect against counterfeiting.

A number of national and international activities are underway to standardise RFID. Of particular importance is EPCGlobal, the user-oriented joint venture launched by the industrial boards EAN and UCC, which recently merged into a single organization called GS1. The European organisation EAN (European Article Numbering) and its American counterpart, the UCC (Uniform Code Council), are supported by retailing and the consumer goods industry. In the 1980s, they introduced the EAN (European Article Number) and its American equivalent, the UPC (Uniform Product Code), for consumer goods, along with their corresponding barcode systems Building upon work done at MIT’s Auto-ID Lab, EPCGlobal has defined a standard for RFID systems with the EPC (Electronic Product Code), which is being adopted increasingly by other industries as well. EPC uses a simple transponder to store each object’s ID number – each of which is unique worldwide – while the data on each object are held ready in a backend database.

The experts in the online survey see pervasive computing in logistics and production as motivated primarily by cost savings and by the emergence of new products and services. This would seem well founded; for one thing, efficiency gains result from optimised logistical and production processes. For another, new product functions can be realised with pervasive computing, such as counterfeit-proof products, or product life-cycle data recording, which enables new, individual maintenance and disposal processes. Accordingly, efficiency gains are the main effect expected from pervasive computing in this application area.

So far, public discussion has paid little attention to the fact that pervasive computing offers an opportunity to monitor employees’ behaviour and performance more effectively. Employees, unions and employers will need to grapple with this matter in the future.

4.2 Motor traffic

The automobile is one of the first everyday products in which pervasive computing is put to use. Today’s cars contain a multitude of driver assistance systems that are intended to support the driver in guiding the vehicle - without calling attention to themselves, as a rule. The car itself thus becomes a smart object, reacting flexibly to the driving situation as well as the condition of the vehicle and the driver.

The driver assistance systems commonly found today – at least in luxury-class automobiles and in some trucks – can be divided roughly into three groups [BrSe 03]:

- Assistance systems for vehicle operation that do not directly intervene in control of the vehicle. These include rain sensors that automatically turn wipers on or off, navigation systems, and spring and shock absorber systems to improve passenger comfort.

- Assistance systems for driving tasks that the driver can override or switch off. Adaptive cruise control is just one typical example of such systems. Other examples include four-wheel drive or warning functions for which activation is situationally dependent – for instance, if seat belts are not fastened, the driver is tired, or the vehicle drifts out of its lane.

- Assistance systems for driving tasks that independently override driver decisions. Among these are the Electronic Stability Program (ESP), which prevents skidding by intervening in the car’s braking system and powertrain, or the Pre-Safe System, which reacts to full braking by auto-
matically tightening the seatbelt or adjusting seats and headrests to their safety positions.

One goal of driver assistance systems is thus to enhance convenience for the driver by supporting him or her in everyday traffic. Another is to take over safety functions in exceptional circumstances. However, many functions of driver assistance systems currently encounter little acceptance among drivers. Intervention by the assistance system is perceived not as support but as an annoyance (e.g., provision of unnecessary tips) or even as a restriction of one’s own freedom of action (e.g., maintenance of a minimum following distance). (See [Bize 06] for an empirical study of user acceptance of a telematics scenario.)

More ambitious approaches to driver assistance systems depend primarily on more powerfully integrating information on the car’s surroundings into the system (sensor fusion). Collision warning and avoidance systems use image recognition, radar, or other sensors to capture data on the car’s immediate surroundings and interpret the situation. They then transmit a warning to the driver or even initiate braking or an evasive manoeuvre. The industry has already developed prototypes, including Mitsubishi’s Advanced Safety Car and Daimler-Chrysler’s VITA II [Ulme 94].

Co-operative assistance systems exchange data between vehicles in order to give drivers information on the traffic situation in their vicinity. The car of the future will become an intelligent, adaptive swarm-object within a decentralised communication and sensor network; it will both supply and gather information that allows it to process and analyse its own guidance system’s decision-making, as well as that of external systems. Compared to conventional traffic warning systems, this will enable warnings to be issued that are directly related to the traffic surrounding the vehicle (e.g., fog bank, freezing rain, rear-end collision, etc.). Any disturbance is forwarded from one vehicle system to the next within a fraction of a second. Depending on the device-specific communication, processing and visualisation possibilities, communication is established with the nearest swarm-object and the driver or a subordinate system is informed. For example, driving data such as brake applications or ESP interventions are exchanged among multiple vehicles in order to give the driver early warning of hazardous situations that he or she cannot see directly, such as accidents or traffic jams. Such systems underwent close analysis by DaimlerChrysler, Fiat and Bosch as part of the European Union’s CarTalk2000 project. This application area will be discussed in greater depth in section 7.3 under the rubric of security considerations in pervasive computing.

According to the experts, the expectation of new products and services, enhanced convenience and improved traffic safety constitute the main motivations for pervasive computing in this application area. Technical challenges in implementation and an inadequate human-machine interface are regarded as possible limiting factors. Along with greater traffic safety, a loss in privacy is seen as a further (albeit relatively minor) effect of pervasive computing in cars.

### 4.3 Inner and external security

On the basis of applicable law, the goal of inner and external security is to assure the integrity of public life and to protect the state as an organisational and functional unit. The main application areas in external security are the armed forces and the secret services. The actors in inner security include disaster control, fire departments, the police, the health sector, flood control, the judicial system and penal institutions. Surveillance and networking play a key role here. Along with personal identification and related measures such as access control, etc. (see also the description of the identification system application area in section 4.6), property surveillance and monitoring are centrally important.

In the military context, Network Centric Warfare has become an essential concept. Network Centric Warfare uses comprehensive information exchange over networks that bridge the different branches of the armed forces to enable efficient communication among all elements involved in command as well as sensors and weapons. This extends down to the level of individual soldiers, who – equipped with various sensors to capture their vital signs and environmental parameters – themselves become part of an ad-
hoc sensor network and thus supply information on conditions in individual sectors [Bove 04].

Such pervasive computing systems can also be used to monitor infrastructure such as the electric grid, roads and airports. At present it remains unclear whether this would really require nationwide distribution of tiny sensors that together would form a decentralised sensor network, or whether this could be accomplished with intelligent selection of parameters and the combination of various signals, data, cross-measurements and interpolations. Since these kinds of sensor systems ought to be almost universally applicable, they have great practical potential. It is likely that such systems will also be used in industry for comprehensive control of complex processes and factories, such as large-scale chemical plants. Monitoring systems in industry could control air quality, recognise fires on an ad-hoc basis, register strains and malfunctions in the infrastructure, etc. A major challenge is the development of robust, small-sized, distributed and inexpensive multi-signal sensors that measure various parameters such as temperature, pressure, acceleration, chemical signals, etc.

The organisational and technical co-operation of various partners from industry and government represents a special challenge for many monitoring systems. Such co-operative arrangements exist already in the field of disaster preparedness – for example, the Rhine Alarm system in Switzerland, Germany and the Netherlands, or the Baltic Marine Environment Protection Commission (aka the Helsinki Commission), which monitors, contains and combats threats to the Baltic Sea. Pervasive computing – and in particular innovative sensor networks – offer previously unimagined opportunities for large-scale monitoring systems, which for instance could enforce the polluter-pays principle in environmental crime.

Monitoring systems that keep entire regions under surveillance fundamentally have the potential to monitor and collect data on people, too: Vehicles driving through thinly populated areas would be easily detectable by means of their exhaust fumes and heat generation. Used in this way, such a system would also be suitable for police and military purposes. This is all the more true if it is capable of functioning transnationally, as does the Brazilian monitoring system for the Amazon rainforest, SIVAM (Sistema de Vigilância da Amazônia). Dedicated surveillance systems are not always necessary for gathering security-related data on individuals. Much of the information that accrues in pervasive computing applications can also be used in the work of inner and external security. For example, monitoring data from telematics systems can be used in fighting crime.

When using monitoring systems to conduct surveillance of persons, the gain in public safety must be weighed against the individual’s claim to privacy in each case. An early example of this balancing act was the discussion of whether data from the German autobahn toll system could be used in criminal prosecutions. The specific case that provoked this debate was the “car park murder”, where a truck driver ran over and fatally injured a parking attendant in order to avoid paying a parking fee [BaWü 05].

According to the opinion of the experts in the online survey, the driving force behind pervasive computing in applications for inner and external security is – as one would expect – first and foremost increasing the level of security. For military applications, more efficient use of resources is also an essential motivation. The main barrier here is technical feasibility, especially with regard to security. For inner security applications, the threat to privacy is also ranked as a limiting factor.

### 4.4 Identification systems

Many electronic administrative and business processes require the secure identification of persons. In the past, this has usually taken the form of state-issued identification papers. Progress in smart card and RFID technologies and improved biometric and cryptographic methods now allow digital systems to satisfy strict security requirements in personal identification. The increased need for security after the attacks on the World Trade Center on September 11, 2001, and the desire for more efficient administrative processes have motivated many state institutions and some private ones to expedite projects in this area.
On November 1, 2005, Germany began introducing new passports with biometric data stored on RFID chips [BMI 05, Schi 05]. The passport will initially include only a digital passport photo, which requires that a frontal view photo be presented when applying. A fingerprint will be added later as a second biometric characteristic. An iris scan could also be incorporated into the chip as a third characteristic. The biometric data will not be stored in a federal or EU-wide central database, so that it will be impossible to use the biometric passport data for other purposes. By 2008, every border crossing-point is to be equipped with digital passport readers [BSI 04].

According to a decision by the European Union’s heads of state, passports must include a digital photo by the end of 2006, and a digitised fingerprint by the end of 2008 [Rae 04]. For visa-free entry into the United States, passports issued after October 26, 2005, must contain a digital photo. After October 26, 2006, a digital fingerprint will also be required [UDHS 05]. During 2005, the United States issued a million digital passports based on smart cards produced by Axalto. Only after October 2006 will American passports also contain RFID chips [Prin 05].

In its fight against crime, the Mexican government founded a national information centre that plans to collect all information on “criminal activities” in a single database. To protect the centre, its employees have had a chip implanted in their arms [Veri 04].

Automated and Biometrics-supported Border Controls (Automatisierte und biometriegestützte Grenzkontrolle, or ABG) at the Frankfurt airport is a pilot project of the German Federal Police. It allows registered air travellers to enter and leave the country via special auto-control lanes. During its test run, the passport data and iris characteristics of 4000 passengers have been registered with the Federal Police to date. Passengers entering and leaving through the special auto-control lanes at Concourse B need only scan their travel documents and look into an iris camera. This largely eliminates the necessity for the standard manual check by border officials. One official does still need to be on hand in case the system malfunctions [BGS 04].

The German Federal Ministry for Health and Social Security (Bundesministerium für Gesundheit und Soziale Sicherung, or BMGS) plans to introduce an Electronic Health Card in the form of a smart card. The interoperable solution architecture for its telematics infrastructure was developed by institutes of the Fraunhofer-Gesellschaft. This infrastructure should allow the existing IT systems of doctors’ offices, pharmacies and hospitals to be integrated into the system and enable smooth communication among all involved parties. In addition, the solution architecture encompasses security solutions and mechanisms such as encryption and digital signatures to guarantee the security of sensitive data. Most importantly, insured patients will retain control over their own data – that is, patients will determine whether and how their data will be used. Patients’ Electronic Health Cards and health workers’ medical ID cards are readable by card terminals (e-kiosks). Patients can view the data stored on their cards at these terminals. Access to the communications infrastructure is limited to registered users connected at access points [BMGS 05]. The German federal cabinet has decided to use the Electronic Health Card – with its digital signature and insurance ID that is valid for life – for other administrative functions of e-government, such as tax returns [BMWA 05].

Alanco Technologies has developed an RFID-based surveillance technology called TSI PRISM. At the behest of the Los Angeles County Sheriff’s Department, the prison in Castaic, California, which houses 1800 inmates, will conduct a pilot project with TSI PRISM. The system consists of wristwatch-sized transmitters for the prisoners and additional transmitters for the guards that attach to their belts. Receivers connected to a central computer are placed in the prison. Each wristband or belt transmitter emits a signal every two seconds and the computer analyses these signals, allowing each person’s location and movements to be followed in real time. With the help of a database, it is also possible to use motion profiles to analyse past incidents. The software triggers an alarm if anyone tries to remove the transmitter. If faced with a threat, guards can manually activate an alarm to call for help. The system also signals if a guard has been violently knocked down. TSI PRISM promises to increase safety for prison employees and inmates alike and to
help reduce violence among prisoners. At the same time, it will support investigations of offences inside the prison [Alan oJ].

The chip producer Infineon and the textile manufacturer Vorwerk have developed a “smart carpet”. Microchips and sensors are embedded in the carpet in a checkerboard pattern and exchange data among one another via conductive fibres. With its integrated pressure sensors, the carpet can register whether persons are present in a room and where they are walking. An alarm can be activated, for instance, if a motion trail begins at a window or emergency exit. Moreover, work is underway to identify a person based on his or her typical movements – e.g., length of stride, foot position, and sequence of movements – to enable unobtrusive biometric access control [Vorw 05].

Even the use of pervasive computing technologies will not make identification absolutely secure. This will be examined in greater depth in section 7.2, which discusses safety in pervasive computing with the scenario of universal personal identification. Identification will become more convenient, however, because the application of biometric methods reduces the need for deliberate interaction. This can go so far as to remain entirely unnotice by the person being identified. Moreover, a great many more objects can be identified with relative ease and reasonable expense than is the case today. Due to their high complexity, however, pervasive computing’s identification systems will be used primarily in major public applications in the inner security and health sectors.

### 4.5 Smart homes

The smart home is a potentially important application area for pervasive computing (see e.g., [TrSc 01]). Articles in a house (or apartment) become networked smart objects thanks to integrated processors and sensors. This initially affects classic building services equipment (heating, ventilation, cooling, safety, and lighting) as well as information, communication and entertainment devices (PC, phone, TV, etc.). But wider-ranging visions also incorporate conventional devices and furnishings such as medicine cabinets, mirrors, windows, doors and carpets into the smart home.

The smart home is intended to adapt automatically to the needs of its residents in their everyday home environment, offer them greater convenience and safety, and result in energy conservation. In light of the industrialised nations’ ageing societies, interest in the smart home is being led largely by the desire to enable elderly and disabled people to stay in their own homes. Together with telemonitoring and user-friendly, fault-tolerant residential layouts and furnishings, pervasive computing should contribute to houses and other buildings being equipped to suit the needs of senior citizens.

Applications in the smart home aim to meet residents’ basic demands on their living space:

- Health parameters can be monitored for ill and old people. For example, a smart vest can register key vital signs such as EKG and temperature, transmit them to the patient’s doctor, and call an ambulance in an emergency (see section 4.7).
- Heating, ventilation and light are automatically regulated in order to decrease energy costs. An example of this would be a smart window, which independently opens and closes in response to air quality, indoor temperature, humidity and outdoor weather.
- Active protection against crime is enhanced. The smart carpet, for example, senses when a person is walking and in which direction, and it can thus recognise potential burglars.
- The operation of technical equipment becomes more convenient, and errors are caught automatically. Among the conceivable possibilities are a washing machine that informs a repairman of defects or service requirements, or a bathroom mirror or wallpaper that fades into a television screen.

Since the smart home intervenes directly in the occupant’s privacy, consumer acceptance of solutions plays a crucial role. Consumers are unlikely to embrace a video camera with image recognition.
capable of recognising when a mobility-impaired person has fallen, because they will feel constantly scrutinised. By comparison, pressure sensors in a smart carpet are much less of an encroachment upon privacy and will likely enjoy greater acceptance.

Pervasive computing in the home has yet to become reality. The expense of upgrading and networking building services and household equipment is still too great, and the array of functions offered would overwhelm many users. Companies and research institutes have already built model homes and apartments to test the smart home from both technical and user perspectives. The TRON house constructed in Tokyo in 1989 was the first such pilot project; it contained 380 integrated computers. Philips is running the HomeLab project in Eindhoven with prototypes of smart mirrors and windows that can display video recordings. The Fraunhofer IMS in Duisburg (the Fraunhofer Institute for Microelectronic Circuits and Systems) has built a model home, InHaus, to test and demonstrate the networking of technology that is already widely available. Microsoft has initiated several smart home projects, such as EasyLiving, with a special focus on implementing Windows Media Center in the home.

Other projects and some early products are dealing with selected aspects or individual devices in the smart home. Together with Siemens Residential Health Solutions, Intel has initiated Everyday Technologies for Alzheimer’s Care in Altoona, Pennsylvania. The CareMedia project at Carnegie Mellon University is working on automatic analysis of the behaviour of persons in nursing homes. IBM has developed a prototype wristband for patient monitoring and a smart pillbox. With its Feminity line of home network products, Toshiba has brought networked home appliances to the market. Siemens and Miele are offering similar product lines. The smart carpet from Infineon and Vorwerk is ready for its market launch. Digital Cookware’s smart pan independently regulates burner temperature.

Networking of the home is an essential technological basis for it becoming a smart home. There are still multiple, incompatible standards for home automation technology: X10 and LON in the United States, Konnex, BACnet, and LON in Europe, and ECHONET in Japan. In addition to these, home networking often falls back on the communication standards conventionally used in telecommunications and consumer electronics [BSI 02].

The social potential of the smart home cannot yet be foreseen. Its cautious introduction in practical applications suggests that its current benefit to residents (if any) is more convenient living, but that measurable effects such as reduced energy costs cannot be expected. The experts underscore this assessment: they see the smart home as driven mainly by the availability of new products and services and by increased convenience, but they do not anticipate efficiency gains.

In the long run, though, the smart home offers great potential in assisted living for the elderly, disabled and ill. Combined with medical technology applications, it can be used to monitor and possibly even treat residents – with the use of dosing systems, for example (see section 4.7 below on applications in medical technology). The patient will be allowed to remain at home despite illness or disability, as most people prefer. This will also cut health costs for society at large.

4.6 Electronic commerce

While pervasive computing application scenarios are quite clearly on the horizon for logistics and production and some have even already begun to be implemented, electronic commerce remains largely in the realm of technological research on pervasive computing [SZM 05]. The use of mobile terminals for business transactions – and especially to support financial services – is comparatively widespread [ShLe 05, Buse 02, TBH 06]. At present, three trends are emerging in pervasive computing for electronic commerce:

The idea behind software agents is that autonomous software systems negotiate to buy a product or service. A human customer delegates the authority, within given limits, to negotiate a price and to decide on the configuration of a product or service. In this scenario, a customer might specify a maximum price and desired holiday destination,
and an agent would then book appropriate travel arrangements and a hotel. However, software agents are currently being used only in pilot applications limited to very narrow fields, e.g., to support teleconferencing [Grüt 06].

For real estate, car, and other capital-intensive products, renting and leasing are common business models today. It would stand to reason that in the future with pervasive computing, certain everyday items would no longer be purchased but rented by paying a fee according to usage – that is, pay per use [Flei 01]. This business model is growing in importance for digital media objects such as music clips and films, and its transfer to real smart objects in pervasive computing thus appears realistic for the future.

A pervasive computing object can often be directly assigned to a person. In this way, information on products and services can be tailored to the user’s profile and made available to him or her. Similarly, this approach enables one-to-one marketing, that is, individualised prices and services for each customer. This area also includes the provision of location-based services that can (for example) suggest nearby restaurants or hotels. Such marketing instruments have already begun to be used in the cellular phone system [Flei 01].

Similar to the conventional wisdom on e-commerce over the Internet, the experts see commerce in pervasive computing as driven primarily by offerings of new products and services as well as by cost savings. Also in analogy to Internet commerce, they expect invasion of privacy and inadequate security to be the main barriers to commerce in pervasive computing.

### 4.7 Medical technology

Health and medicine offer a broad application area for pervasive computing, ranging from pure identification and authentication systems to smart objects for patient monitoring. Pervasive computing-based systems for home monitoring are intended to shorten long hospital stays that are mainly due to a need for long-term observation. In addition to huge cost savings, this could also improve the patient’s quality of life. Furthermore, treatment could be markedly improved by continuously monitoring patients who are chronically ill or intermittently at risk, with the option of automatically alerting emergency services. Although the first pilot projects are underway and products are also becoming available, neither home monitoring systems nor medical applications of RFID technologies are widespread yet. One example of a simple application in this area is the pillbox developed by the South African company SIMpill, which sends an SMS to the patient’s doctor if a patient skips multiple doses. Even though RFID and health monitoring systems are not yet taken for granted in routine medical practice, a number of pilot projects have been launched:

- In collaboration with Intel and Siemens, the Saarbrücken Hospital (Klinikum Saarbrücken) has started a pilot project using RFID for patient identification. The objective is to simplify access to patient data. At the same time, this should improve reliability in administering the correct medications at the correct dosage. Approximately a thousand future patients will receive a wristband upon admission with an integrated RFID chip containing a patient number. The technical equipment also includes tablet PCs, PDAs, and a WLAN infrastructure. Doctors and nurses can identify the patient by using mobile terminals to read the patient number stored in the wristband. Authorised members of the medical staff can then access via WLAN a protected database with detailed patient data, including medications and dosages. Encryption procedures guarantee that the data is protected against unauthorised access. This pilot project places special emphasis on drug safety.

The possibility to identify patients faster and more easily will allow nurses to care for patients more intensively and administer drugs more easily and safely. For example, critical data and risk factors such as known allergies can be stored for each patient. In addition, the patients participating in the pilot project can request their own health data via information terminals. This includes data such as blood pressure readings, weight and dates of treatment or discharge. They can also learn about their diagnosed condition and its standard treatments. The Saarbrücken
project is based on an RFID solution already in use at the Jacobi Medical Center in New York City [ArZe 04].

- In Ventura, California, VivoMetrics has developed the LifeShirt, a system for ambulatory patient monitoring. Sensors sewn into these shirts can measure 40 different physiological parameters, such as blood pressure, heart rate and oxygen consumption. The information is first stored in a small recorder on the hip and then forwarded to a data centre for analysis. The doctor can view and monitor the data at any time. If necessary, the patient can also use the device to inform the doctor of symptoms such as dizziness or pain and can make a doctor’s appointment online. According to its manufacturer, the LifeShirt is a “comfortable, washable garment that can be worn at home, at work and while exercising.” [Vivo 04]

- Co-ordinated by the Institute for Information Processing Technology at the University of Karlsruhe, a consortium that also includes numerous companies has created a Personal Health Monitoring System. The project’s goal is to develop a system that measures all vital signs without limiting the patient’s mobility. The data are analysed in a wearable signal processing system and an emergency alarm is activated if necessary. The sensors on the patient’s body transmit their data via cables sewn into the clothing or via cellular signal to a base station that takes the form of either a smartphone or a PDA. Wireless communication uses a Bluetooth-based communications protocol, Personal Area Networking for Advanced Medical Applications (PANAMA). The system is easy to use thanks to self-configuring devices and application identification. Depending on the user’s position, the base station can establish a connection to the Internet via a Bluetooth-capable mobile phone or remotely via a Bluetooth access point. The base station is constantly connected to a central database of patient files, the Electronic Patient Record (EPR), and to a medical service provider. The patients’ data can be examined as needed by doctors, who can then take appropriate steps, including alerting emergency services equipped with automatic localisation [ITIV 05].

- The Wealthy project, coordinated by the Italian textile maker Milior in collaboration with other European companies, was completed at the end of 2005. The project developed a monitoring system integrated into clothing. Its main objective was to develop an especially comfortable system based on a wearable interface. The sensors for measuring vital signs are all integrated into the garment that the patient wears. The data can then be sent from the garment to a central location/database – via Bluetooth for short-range transmission and otherwise via GPRS/GSM. Authorised persons, such as medical staff, will

<table>
<thead>
<tr>
<th>Microelectronics</th>
<th>Mobility</th>
<th>Embeddedness</th>
<th>Ad-hoc networks</th>
<th>Context awareness</th>
<th>Energy autarky</th>
<th>Autonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sensor technology</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication technology</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Localisation technology</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Security technology</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Machine-machine communication</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Human-machine interface</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1: Technology fields necessary in implementing pervasive computing characteristics
have access to the database at all times. The system will also be able to automatically issue an alarm if the patient’s condition turns critical [WePr 05].

The increased use of pervasive computing in medical technology is expected to have a positive impact on health, especially that of the elderly, the chronically ill and convalescent patients, through the use of intelligent implants and monitoring systems. The consistent use of pervasive computing should increase patients’ comfort by enabling them to spend their days in familiar surroundings, yet under a doctor’s care – with a combination of telediagnosis and remote treatment, if necessary. This links with opportunities provided by pervasive computing in the smart home. As a rule, reducing hospital stays will also reduce overall treatment costs in the long run. However, one must exercise caution here with regard to the undesirable side effects of implants and psychological stress for the patient due to constant monitoring [KoSo 05].

Interestingly, the experts regard medicine as the sole application area where pervasive computing is fostered by a wide range of motivations. These include the development of new products and services, cost reductions, increased convenience, efficiency gains and improved safety. Medicine is plainly an ideal application area for pervasive computing. On the other hand, the experts also see numerous limiting factors, such as a lack of user confidence in the system, concerns about safeguarding privacy, inadequate technical implementation – especially with regard to security – and an unsatisfactory human-machine interface. This is understandable due to the extremely high demands placed on medical technology, which has a direct influence on the life and death of the patient.
5 The Technology of Pervasive Computing

Pervasive computing defines a new area in information technology where processing, communication, sensors, and actuator technologies become a part of nearly any environment, device or object created. This will lead to artefacts that are attentive and responsive to the user and that provide efficient means for creation of and access to information anywhere and anytime.

Dr. Albrecht Schmidt, Ludwig Maximilian University of Munich, Germany

Pervasive computing is not an independent technology. Instead, it describes the performance characteristics of an approach for invisible, ubiquitous, and seamless information and communication. Accordingly, a smart object cannot be described in universal terms, since so much depends on the context of its application: It might be an independent, small, mobile device. A smart object might be integrated into a house, or a household device might be transformed into a smart object by integrating the appropriate components. This variety shows that the technological basis of pervasive computing is not always the same; rather, different technologies will be used in each case. Still, full-blown pervasive computing has certain characteristics that will pertain to nearly all application areas, albeit to a varying degree. This study identifies eight technology fields that are necessary for the realisation of pervasive computing’s six characteristics (see Table 1):

The relative significance of each field cannot be deduced from Table 1. A simple example underscores the limits of this matrix: Microelectronics is the precondition for any sort of electronic data processing, yet Table 1 lists it as essential for two characteristics only, mobility and embeddedness. But this does not take into account the international experts’ view of mobility as one of the central characteristics of pervasive computing (see Chapter 4 on the application areas of pervasive computing), which indirectly gives microelectronics more weight. In the realm of production technology – such as lithography and wafer technology – microelectronics is decidedly important for sensor technology, too. This effect is also not shown in the matrix. To obtain a general weighting for all pervasive computing applications, the experts in the online survey were asked to assess the relevance of each technology field for pervasive computing (see Figure 10):

Fig. 10: The comparative relevance of the eight technology fields for pervasive computing

The table suggests that communication technologies and microelectronics are the most important prerequisites for nearly all pervasive computing applications. The experts viewed power supply as surprisingly important, although they by no means regarded energy autarky as an especially important characteristic for all pervasive computing application areas (see Chapter 4 on the application areas for pervasive computing).

The experts estimate that each of the technologies will be mature and thus available in the near future, within a time horizon ranging from about one to four years. According to their description, nearly all...
of the technological requirements for pervasive computing should be fulfilled within the foreseeable future (see Figure 11):

In order to grasp the dynamics of the development of pervasive computing and its dependence on these technology fields, the experts were asked about potential technological bottlenecks that would have especially serious consequences. They identified unsolved problems with the power supply, an inadequate human-machine interface and a lack of well-functioning security technology as particular bottlenecks (Figure 12):

![Fig. 12: Comparison of potential bottlenecks in the pervasive computing technology fields](image)

The following sections will describe the basic principles of the individual technology fields and their significance for pervasive computing. The end of each section systematically summarises the main findings of the expert survey for that technology field. The survey asked about the importance of each field for pervasive computing, availability of the technology, and its significance as a potential technological bottleneck for pervasive computing. To enable closer analysis and to identify prominent developments, the survey also specified central subtopics to be assessed for each technology field.

### 5.1 Microelectronics

Microelectronics – which deals with the miniaturisation, development, manufacture and application of integrated circuits (IC) – is already an essential component in a vast number of technological devices and equipment that shape contemporary life. Consumer electronics, the automotive industry and medical technology are just a few examples of fields in which microelectronics plays a key role.

Currently, microelectronics works with structures smaller than 90 nanometres. At the present rate of development, this should drop to 45 nanometres by 2010 [ITRS 03]. Significantly increased circuit density will yield considerable gains in functional capacity for a given IC size. However, the field of microelectronics is running up against physical limits that are increasingly expensive to overcome. These limits include a highly complex manufacturing process and decreased performance and durability due to undesired current leakage between the printed circuit board tracks.

Integrated circuit packaging – that is, the mounting and bonding of electronic components on a printed circuit board (PCB) – has undergone major changes in recent years. Increasing integration density, greater functionality and costs have been driving this development. Nowadays, solder balls are used to make electrical contacts, rather than wires as in traditional IC packaging [Cosk 99]. Advanced packaging processes, such as flip chip, chip-size package and ball grid array, have assumed a key role in IC manufacturing. In addition to smaller dimensions and lower production costs, these processes offer the advantage of directly integrating packaging into the chip manufacturing process. A number of multinational technology companies manufacture advances packages, including Infineon, IBM and Toshiba.

Key players in standardisation include the industry association Semiconductor Equipment and Materials International (SEMI), the Institute of Electrical and Electronics Engineers (IEEE) and the International Technology Roadmap for Semiconductors (ITRS). They develop widely recognised standards and technology roadmaps to provide guidelines for handling materials, equipment and processes in microelectronics.

The trend in microelectronics is toward even greater integration density, smaller structures and falling unit costs. PCB-based system integration deals with the integration of passive and active electronic components, functional layers, electro-opti-
cal interfaces and sensor interfaces on a PCB or even on a stack of PCBs. In system integration at the semiconductor level, all digital, analogue and mixed-signal functions are integrated directly into a single IC (system-on-chip).

Current research in nanotechnology is looking at how quantum effects can be used at the submolecular and atomic levels to achieve further miniaturisation of microelectronics.

Today’s manufacturing of ICs, which is conventionally based on silicon as a semiconductor, is too expensive for very low-priced smart objects – such as RFID tags for consumer goods and their packaging, which cannot cost more than a few cents. Polymer electronics, which uses carbon compounds as semiconductors, appears highly promising for such applications. Unlike silicon ICs, polymer ICs can be produced in very inexpensive printing processes. However, the performance of polymer electronics is clearly inferior to silicon when it comes to switching speeds and robustness. Polymer electronics offers advantages where electronics need to be flat, flexible and cheap, and where performance standards are relatively low.

Fig. 13: Relevance of microelectronics for pervasive computing

A great many research institutions are working on microelectronics and its peripheral fields. These include various institutes of the Fraunhofer-Gesellschaft, such as the Fraunhofer Institute for Reliability and Microintegration (Fraunhofer Institut für Zuverlässigkeit und Mikrointegration, or IZM) in Germany, the Interuniversity Microelectronics Center (IMEC) in Belgium, Georgia Tech and the Massachusetts Institute of Technology (MIT) in the United States, and the Industrial Technology Research Institute (ITRI) in Japan. In the field of system integration, the Fraunhofer IZM is among those currently working to realise autarkic, distributed microsystems. By the year 2015, IZM’s eGrains should offer computing power, power supply and communication capabilities in a space approximately 2 x 2 x 4 mm. One likely application of eGrains would be in sensor networks [WoSc 03]. The EU-funded Integrated Project PolyApply brings together leading actors in polymer electronics [Poly 0j]. It is working toward mass production of polymer circuits, which offer lower performance than silicon ICs but also lower cost, and which will be used as RFID transponders, for example.

Overall, the experts regard microelectronics as a mature and widely available technology without appreciable bottlenecks for pervasive computing. Nanotechnology and polymer electronics are regarded as future technologies, but since they will only be used in niche applications, they do not represent significant technological barriers.

Fig. 14: Availability of microelectronics for pervasive computing

Fig. 15: Potential bottlenecks in microelectronics for pervasive computing

5.2 Power supply

Supplying power to electronic systems represents an essential condition for using pervasive computing applications. So far, progress in chip technolo-
gies and electronics development has consistently decreased system size, reduced specific power demands and improved performance. Even so, for most applications the power supply is the largest and heaviest component, and the biggest constraint on use.

Supplying power basically poses no problems for applications plugged into the power grid and networked with cables. However, mobile and wireless systems with power self-sufficiency have become important in recent years. Older, radio-supported applications, in particular, consumed a lot of power, which forced the user to change or recharge the battery frequently. More recently, though, energy consumption has decreased due to progress in IC manufacturing and the deliberate, application-based reduction of active times for sensors and modules. At the same time, lithium-ion batteries came into use, offering excellent reliability and long-term stability. The new goal is to do without batteries altogether. To this end, miniature accumulators (storage batteries) would be continuously recharged by photovoltaics, thermogenerators, miniature piezo generators or other converters, without ever needing to plug into a power supply line [JoJo 04].

There are several possibilities for supplying power to electronic systems. The choice depends mainly on the average power consumption but also on the short-term peak load. Ambient conditions must also be considered, such as usage in buildings or in extreme heat and cold. Among classic primary batteries, which are non-rechargeable, alkali batteries are the most commonly used, with lithium-ion batteries growing in popularity [Axma 04]. Other battery types are optimised in terms of size, shape and capacity (zinc-air button cells) for special applications, such as hearing aids, and they too are used by the millions. Although rechargeable accumulators are expensive at initial purchase and have at best half the capacity of comparable non-rechargeable batteries, they are attractive for use in applications with high power consumption. Here, nickel-metal hydrides have largely superseded nickel-cadmium cells due to their greater capacity and their insignificant self-discharge. Rechargeable lithium-ion accumulators have become standard in many applications, because their service life lasts for years due to their exceptionally low self-discharge. The use of such systems is not limited to mobile telephones, PDA and digital cameras. Their manufacturing technology is so simple that practically any shape is possible without much effort. This makes them attractive for use in pervasive computing applications, too.

Multinational companies have dominated the mass market in batteries for portable electronic devices due to their high degree of international standardisation. Leaders here include Panasonic, Sanyo Energy, Seiko Instruments and Toshiba in Japan; Energizer and Duracell in the United States; VARTA Microbattery in Germany; GP Batteries in Hong Kong; and Saft Participations in France.

To simplify the international marketing and supply of batteries and accumulators, their manufacturers co-operate closely in various European and international standards organisations. This collaboration occurs very early, before new types of batteries and accumulators are brought onto the market. The manufacturers reach agreement on their chemical systems, designs, maximum and average useful discharge currents, and other specifications. For accumulators, they commit to a suitable charger system. Thus, despite the manufacturers’ various model names, uniform basic models are available to both consumers and the developers of devices and systems.

Various types of micro fuel cells are presently still in the research stage. Their distinctive feature is that they can generate electricity from hydrogen or methanol. These fuel cells are refillable, have a very large capacity with relatively low weight, and produce only water and carbon dioxide as residue. Due to their complex technology and resulting high production costs, their use of highly explosive energy sources, and their heat build-up, fuel cells will be limited to niche applications for the foreseeable future [GSFF 04].

Panasonic in Japan launched a new primary battery, Oxyride, in 2004. This system is based on extremely fine granulated materials, including nickel hydroxide, graphite and manganese dioxide. Because this results in a larger surface area, these batteries have about a 50% greater capacity than alkali batteries
and also permit a significantly higher current pulse load. This battery type is thus predestined for digital devices, particularly since they cost only 10% more than alkali batteries.

In those cases where initially equipping a device with batteries may not suffice for its entire service life, or where a constant exchange of batteries is impracticable, an ideal technology would enable autarkic, wireless energy provision from ambient sources – so-called energy harvesting. A variety of such technologies are available, some of which have been tested in practice. Each must be considered individually for each application with respect to its energy balance and efficiency:

- Photovoltaic generators, which directly convert energy based on various solar cell principles.

- Piezoelectric generators, which convert mechanical to electrical energy by means of special piezo crystals.

- Thermoelectric generators, which create electrical voltage with temperature differentials between two different metals (the Seebeck effect).

- Electromagnetic generators, where electromagnetic energy conversion occurs according to the familiar dynamo principle.

- Capacitive and electrostatic generators, which use capacitive or electrostatic charges in an electric field to produce energy.

- Thermomechanical generators, which – in contrast to thermoelectric generators – create mechanical energy, which must then be transformed into electrical energy in a second step.

- Electrokinetic microchannel batteries, where electricity is generated as ion-charged fluid (e.g., salt water) passes through microchannels or porous filters, thus separating the fluid’s electric potentials. The fluid transport can be propelled by either static or external pressure on the fluid. Useful currents are only on the order of microamperes, however [YLKK 03].

The potential for improving battery and accumulator systems for portable applications remains great, although the composition of components has been known for years. Due to the great economic gains that could accrue from a clear technological edge, a number of international institutes are working on behalf of industry to further develop portable and alternative power sources. They include the Massachusetts Institute of Technology, the Florida Solar Energy Center and the Los Alamos National Laboratory in the United States; the Alberta Research Council, Inc., and the Institute for Fuel Cell Innova-
tion in Canada; the Tokyo University of Science in Japan; the Atomic Energy Commission in France; and the Fraunhofer Institute for Solar Energy Systems and the Centre for Solar Energy and Hydrogen Research in Germany.

Three aspects of the experts’ assessment of the power supply field are especially notable. Batteries and accumulators are, according to the experts, relevant for pervasive computing, and – despite their high availability – should be regarded as a technological bottleneck. In light of the solutions available today, the experts apparently still perceive a great need for further development to increase capacities and reduce self-discharge. They consider energy harvesting an alternative technology for the future. They judge micro fuel cells to be not particularly relevant for pervasive computing. A likely reason for this is the expensive infrastructure for supplying the cells with fuel, which is more likely to become economically viable in fuel cell used as an alternative power source for cars.

5.3 Sensor technology

Capturing and analysing the real world is one of pervasive computing’s central characteristics. At the heart of this is the sensor as an electronic component that qualitatively or quantitatively registers characteristics of the environment and amplifies, processes and relays them as a digital signal.

Types of sensors and their measuring methods are exceedingly varied, as are the demands placed upon them. Their design and dimensions must be individually adapted to their intended application:

- **Acceleration sensors** are often based on piezoelectric effects, that is, an electric signal is generated by applying mechanical stress (compression or tension) to a capacitor.
- **Flowmeters** rely on inductive or capacitive measuring principles.
- **Pressure sensors** are either based on strain gauges in which electrical resistance changes due to deformation, or they rely on the piezoelectric principle.
- **Moisture sensors** measure changes in electrical resistance when thoroughly moistened.
- A great many different methods are used in gas sensors. These include catalytic measuring methods, where contact with a gas initiates a reaction with the catalyst, which leads to a temperature change and consequently a change in electrical resistance. Sensors based on optical methods recognise the characteristic absorption band of a gas.
- **Temperature sensors** measure the change in electrical resistance when temperatures rise or fall.

The sensor must have an operating range or threshold that is appropriate to the intended application. For instance, a sensor for recognising hydrogen leaks should work only at or above concentrations of 0.4 to 0.5% hydrogen in the air with a reaction time on the order of seconds. If a hydrogen sensor is used to prevent explosions, however, it must detect hydrogen in the 1000 ppm range with an ultrashort response.

The widespread use of sensors has spawned many diverse and often application-based standards for measuring methods, sensor technology, reporting paths and interfaces. But the great need for consistent and integrated data provision is fostering uniform standards at least for linking sensors in networks, e.g., IEEE 1451 of the Institute of Electrical and Electronics Engineers.

The key challenges in sensor development today include reducing the size and weight of sensors and sensor systems and their integration in complex semiconductor systems; decreasing sensors’ power consumption; increasing their performance and reliability; and developing lower-cost production technologies.

One focus of development work is the refinement of existing technologies. In system-on-chip, the sensor is no longer produced as a separate component; instead, it is directly integrated in the chip. Nanotechnology is pursuing new approaches with dramatically smaller and more sensitive sensor elements on the submolecular or atomic level.
important approach is to replace complicated reference measurement systems with easy-to-handle superstructures. Increasing use is being made of sensor arrays, in which a number of different sensor principles are combined into a single component in order to measure a particular environmental characteristic. To cover an extensive environment, sensors are combined in ad-hoc networks in which the nodes spontaneously connect and carry out their monitoring tasks together.

A great many companies supply sensors. In addition to major semiconductor manufacturers like Infineon and Texas Instruments, these include numerous smaller companies (some of which are highly specialised), such as First Sensor, American Sensor Technologies, Applied Sensors and CCI Thermal Technology.

The experts in the online survey evaluate sensor technology as a generally well-established technology that does not pose any serious technical barriers. Interestingly, this assessment also applies to highly integrated, functionally sophisticated sensor networks, which remain, to-date, a pure research topic. The experts take the view that sensor networks will also be ready for practical application in the medium run.

5.4 Communication technology

Communication technology is generally combined with information technology and referred to collectively as information and communication technology (ICT) in order to emphasise the overlap between the two fields. In telecommunications – e.g., mobile communication, satellite communication and telephony – the important subfields are communications engineering, radio engineering, switching technology, signal transmission technology, high-frequency engineering, microelectronics, technical informatics and communications networks. Data exchange between two objects occurs here via cable or radio technology. Wireless communication has become widely established by now because it enables objects to be quite mobile and requires less infrastructure. Since the possibility for objects to communicate is fundamental to the vision of pervasive computing, ICT plays an essential role.

Wireless transmission occurs almost exclusively through modulation of electromagnetic radio waves. Communication via infrared light plays only a minor role as an alternative to radio.

Modulation methods convert data into a form that can be transmitted via antennas through the air interface. In general, modulation refers to alterations in a carrier signal in response to a message signal. The amplitude, frequency and phase of the carrier signal can be altered. One thus distinguishes between amplitude, frequency and phase modulation. Multiplexing allows many transmitter-receiver
pairs to use the air interface simultaneously, by dividing it according to space, frequency, time, or codes. Space-division multiplexing refers to the division of space into cells. Frequency-division multiplexing divides the entire frequency band into disjoint smaller bands. In time-division multiplexing, all channels take turns using the entire frequency band exclusively during their assigned time slot. Wireless communication typically uses a mixture of time-division and frequency-division multiplexing. The newest approach is code-division multiplexing, which is currently used in the third generation mobile telephony system UMTS (Universal Mobile Telecommunications Systems). Here, all transmitters broadcast a coded data stream at the same time and on the same frequency, with the signals overlapping. Each receiver is able to decode the data relevant to it from the overall signal. Independent of the transmission technology, the two devices communicating with each other generally use different communications protocols. There are several different protocols being applied here. The best known of them is the Internet protocol IP, which is used in most of the world’s networks because it is independent of basic network technologies. Its new version, IPv6, which significantly increases the number of addresses that can be assigned to Internet objects, was adopted in 1999 but has yet to fully replace the old version IPv4. An expansion of IP, Mobile IP (MIP), supports the mobility of devices – that is, moving between different networks [BSI 03].

To guarantee a smooth information and communication process, comprehensive standards must be in place, and the various applications must adhere to them. In 1992, the European Telecommunications Standards Institute (ETSI) laid down the DECT standard ETS 300 175 (DECT = Digital European Cordless Telecommunications). This standard is widespread in the home and business areas. It supports both voice and data transmission. By now, over 300 million DECT-based systems have been installed worldwide. The Personal Handyphone System (PHS) is a mobile telephone standard developed in Japan in 1989. At that time, Japan did not yet have a standard comparable to DECT. It was intended mainly to be developed into a new standard that would cost less than conventional cellular systems. At the moment, the most widespread mobile telephone system in the world is GSM, named after its standards organization, Groupe Speciale Mobile. GSM has been expanded with a packet data channel to support General Packet Radio Service (GPRS). Data and voice are handled separately in the network. American standard IS95 is the counterpart to GSM.

The Institute of Electrical and Electronics Engineers (IEEE) has published a number of different standards for wireless networks. The 802.11 standard, which standardises wireless local area networks (WLAN), is widely used. For short-range transmission with a reach of a few metres, Bluetooth (IEEE 802.15.1) has rapidly become popular for communication between devices in a personal area networks (PAN).

Beyond the existing solutions, a number of approaches will be decisive in the further development of mobile communication:

- WiMAX is based on the IEEE 802.16 standard and amounts to a WLAN with a somewhat larger range of up to 50 kilometres.
- Wireless USB enable devices to connect via the air interface by sending signals through their USB port.
- Many mobile telephone providers offer not just the established GSM and UMTS networks but also other wireless networks like WLAN or WiMAX, or they are planning to offer them. Changing between these various networks will soon be easier and seamless.
- Telecommunications networks are being converted to digital voice transmission, in part by using Internet telephony (voice over IP, VoIP).
- In the realm of automated industrial production, there is an effort to replace the existing field bus system with an industrial ethernet – an expanded ethernet based on the IEEE 802.3 standard – which would meet real-time demands. Here, too, the main trend is that systems based on wireless communication are gaining ground. Due to the millions of applications and correspondingly low costs, the main candidates here are Zigbee (IEEE 802.15.4) and Bluetooth, but also WLAN.
The decisive players in the ICT field – especially with regard to wireless communication – are the major mobile telephone providers such as Deutsche Telekom, Vodafone and the Japanese company NTT DoCoMo; makers of network components, such as Cisco and Lucent; and suppliers of digital devices such as Nokia, Motorola, Siemens/BenQ, Palm, Agere, Ericsson, IBM, Intel, Microsoft, Sun and Toshiba. Such companies are increasingly working with representatives of standards organisations to develop complete solutions for information and communication. ICT companies are often involved in developing both the technologies and the standards.

In the online survey, the experts assessed communication technology as a key technology for pervasive computing and also noted that it is already widely available. Despite this fact the experts see a certain risk of technological bottlenecks in the further development of the Internet standard IPv6 for additional address space, and Mobile IP for mobile communication.

5.5 Localisation technology

One interesting facet of pervasive computing is that equipping smart objects with appropriate transmitters and receivers enables precise localisation. Particularly for the provision of location-based services, which offer a service tailored to the user’s geographic position, localisation technology is an absolute necessity.

There are currently three types of localisation systems: satellite-supported, cellular-supported and indoor localisation systems. The satellite-based Global Positioning System (GPS) is the world’s most commonly used localisation and navigation system. It was commissioned by the United States Department of Defense for the military and has been used worldwide since 1998. The system consists of three parts: the space segment with 24 stationary satellites, the control segment with five ground stations that monitor the satellites, and the user segment with GPS receivers in navigation systems, mobile telephones, laptops, etc., that use signals received from the satellites to determine the position.

Mobile telephone companies are capable of pinpointing the location of mobile telephones with the support of the cellular network, because the telephones must establish a connection to the transmitters. The most important mobile telephone networks in Europe are the Global System for Mobile Communications (GSM) and the Universal Mobile Telecommunications System (UMTS). Cell ID – the cell-based localisation technology – functions in both networks. Cell ID identifies the base station to which a mobile telephone has established a connection, and thus the cell where the telephone is locat-
The position of the mobile telephone is then derived from the ID of the cell; the precision of this process depends greatly on cell density and size. Precision varies between 0.1 and 35 kilometres, depending on cell size. In some circumstances, mobile telephone companies can determine the position of a mobile telephone to within a few metres’ precision through techniques such as triangulation.

These systems function poorly inside buildings. There, indoor tracking systems are utilised that use a number of sensors able to exchange information with the devices that are being localised. Depending on the type of sensors, location is determined based on one of the technologies described above. Examples of such sensors include pressure sensors that determine the presence of an object through physical contact; access points to wireless cellular networks, which can ascertain the presence of an object in their area; and automatic identification systems like barcode scanners and RFID systems. One example of an indoor localisation system is the smart carpet (described in section 4.4 on identification systems), which can determine position relatively precisely and reliably by means of pressure sensors.

True standardisation in the field of localisation systems does not exist. So far, GPS is the only global navigation system that civilians can use. Russia’s Global Navigation Satellite System (GLONASS) was developed in the former USSR for military applications and to date has not been opened for civil use. Galileo, a European satellite-supported navigation system currently under development for civil purposes, will guarantee independence from the American GPS. The first Galileo satellite was launched into orbit at the end of 2005; the system will go into operation by 2008. It promises to offer greater precision and reliability and aims to be interoperable with GPS. It will use 30 satellites in orbit at 24,000 kilometres. Two Galileo Control Centres (GCC) in Europe will monitor the satellites’ flight path. In addition, 20 Galileo Sensor Stations (GSS) around the world will transmit their measurements to the GCCs. The GCCs will use the data from the sensor stations to compute the integrity information and to synchronise the time signals of all the satellites with those of the ground station clocks.

Current work focuses mostly on improving localisation techniques. This primarily means increasing precision and sizing down the equipment. At the moment, precision for civil users of GPS is specified at 10 metres. Indoor systems can achieve much greater precision – under a metre – depending on the type and number of sensors employed.
Apart from the American military, which is responsible for GPS, many research institutions (e.g., the Fraunhofer Gesellschaft) and companies are involved in developing localisation systems. The indoor localisation system RADAR from Microsoft Research, for example, is based on the IEEE 802.11 standard for wireless local area networks (WLANs). RADAR is realised completely as a software extension and requires no additional hardware infrastructure. The access points must be placed in the building so that their reception areas overlap. The mobile objects use a laptop with WLAN access. RADAR measures signal strength at the base stations in order to calculate the 2-D position from them. The mobile telephone companies automatically have a Cell ID-based localisation system thanks to their existing infrastructure.

In the online survey, the experts positioned localisation technology as the field that is the least relevant for pervasive computing, compared to all the other technology fields. The experts regarded localisation as a generally mature technology. They see possible technological bottlenecks as most likely to occur with the indoor systems.

### 5.6 Security technologies

A central feature of pervasive computing is that nearly all smart objects can exchange information. Security, which ensures that only authorised persons and objects can access the data meant for them, is thus essential in pervasive computing. The fact that most communication in pervasive computing is wireless only underscores the significance of security technologies, because radio communication can be manipulated more easily than is possible in wired networks.

Many pervasive computing applications intervene in central areas of life without the user always being aware of it. Thus, safety, which ensures that no damage occurs from system failures and operator error, is very important.

A further security requirement in pervasive computing is data protection to safeguard the individual’s privacy. It must guarantee that personal data can be accessed by authorised third parties only. Security thus encompasses the areas of security, safety and privacy protection:

**Security**: Security deals with protection from intentional attacks by third parties. Security objectives in the area of security can be formulated as confidentiality, integrity, non-repudiability, availability, anonymity and authenticity.

The authenticity of an entity – whether a person or an object – is understood as its genuineness and credibility, which is verifiable on the basis of its unique identity and characteristic qualities. The integrity of data means that unnoticed manipulation of data is impossible. Confidentiality means that only authorised persons can access information. Non-repudiability means that entities cannot disclaim the actions they have performed. Anonymisation is changing personal data in such a way that even with a reasonable degree of effort, it is impossible to match the data to the person [Ecke 04].

Many different technologies can be used in authentication. Passwords continue to be a widespread as a way for users to authenticate themselves on a device such as a PC. The four-digit Personal Identification Number (PIN), which is a simplified variant of a password, is widely used for authentication on mobile telephones and automated teller machines. Biometric methods are used increasingly. Fingerprints, in particular, are now being used by devices to identify users. For objects without biometric characteristics, RFID can be used in automatic identification processes for authentication.

In order to guarantee the integrity of data, a checksum is usually calculated from the data. Manipulation can be discovered by comparing the checksum to a reference value. Checksums are typically generated by using hash values, which transform data of any length into a unique value of fixed length. The most commonly used methods are SHA1 and MD5.

Confidentiality is ensured by encrypting data. Two basic types of encryption exist. In symmetric methods, the same secret key is used in both encryption and decryption. In asymmetric methods, a public key (accessible to anyone) is used in encryption, and a private key (available only to authorised persons)
is used in decryption. Symmetric encryption uses the Advanced Encryption Standard (AES) as well as an older method, 3DES, which is based on the old Data Encryption Standard (DES). For asymmetric encryption, the method normally used is RSA, named after its developers, Rivest, Shamir and Adleman. Newer asymmetric encryption methods are based on the discrete logarithm problem in elliptic curves, whereas RSA security relies on the integer factorisation problem. An advantage of the elliptic encryption techniques is that they require less computing power for the same level of security. This method is thus comparatively well suited for use in devices with limited resources, which makes it especially interesting for pervasive computing.

Non-repudiability is achieved with digital signatures. Asymmetric cryptography (see above) is generally used. The relevant data or a checksum corresponding to it are encrypted with a private key that is available only to the signer. The freely available public key enables verification of the sender. A public key infrastructure (PKI) is used in administering the public keys, which allows a key’s ownership and validity to be confirmed by a trustworthy, neutral authority. PKI systems are a central technical component of trust management in digital networks. For trust management in pervasive computing, the Trusted Platform Module (TPM) will in all probability play a leading role. With TPM, the industry organisation Trusted Computing Group (TCG) has defined a hardware-based solution to support key management. The TPM amounts to a smart card securely built into a device. However, the module is associated with a system, not a user. A detailed description of the TPM approach and its use in securely identifying objects is given in section 7.1. The security objectives of anonymity and authenticity would appear to contradict each other. An approach to resolving this contradiction – at least in part – is pseudonymisation as a watered-down form of anonymisation. Here, personal data are altered by an assignment rule so that they can no longer be linked to a natural person without knowledge of the rule. Disguising individuals’ true identities with pseudonyms and administering these identities falls under the rubric of identity management. The aim of identity management is to ensure that identities and the personal data linked to them are consistent, reliable, secure and constantly available.

In contrast to the other security objectives, anonymity cannot be assured by any explicit cryptographic mechanism. However, Frank Stajano has described a protocol that enables anonymous bidding by different parties at an auction. With his Resurrecting Duckling security policy model, Stajano has developed a scheme for connecting devices to one another, without requiring a third, trustworthy authority. Since it offers the possibility of getting by with limited devices, this model is well suited for use in pervasive computing [Sta 02].

Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols that can guarantee authenticity and confidentiality in communication between two endpoints. The Internet Protocol IP, the most-used protocol for communication between various digital devices via different network technologies, has been expanded with the IPSec security standard, which supports authentication and encryption at the IP packet level. Special resource-conserving versions of the IP stack, such as the uIP stack developed by Adam Dunkels and the Swedish Institute of Computer Science, enable the IP protocol to be used in the world of pervasive computing [UIP 05].

Safety: Safety is often equated with reliability. Reliability means that the system works correctly according to its specifications. The effects of a pervasive computing system’s reliability can be more or less dramatic, depending on the area in which it is used. In medical technology, for example, a system’s reliability can be truly a matter of life and death. In logistics, pervasive computing can improve the ability to plan and thus lead to greater reliability [BHR 01]. If in the future many widespread systems – such as door locks, pens, cameras and cars –work correctly only with certain pervasive computing technologies or systems, people will be extremely dependent on these technologies and systems, since their reliability will be essential for performing the simplest actions.

Experience shows that every technical system is error-prone. Safety in a narrower sense refers to a system’s capacity to be fail-safe – to avoid responding to system errors by spiralling out of control and thus endangering the system itself or its environment. At the same time, the system should be fault
tolerant; that is, when operator errors occur, it should react as far as possible in conformity with its specifications. Safety thus basically refers to protection from unanticipated events [BSI 02].

As a general rule, it is harder to develop systems with high safety levels in pervasive computing due to the advanced complexity and networking of very different units. On the other hand, pervasive computing can help improve the safety of other systems. For instance, use of a pervasive computing infrastructure can help increase the safety and efficiency of health care in a hospital [Bohn 03].

### Data Protection

The objective of data protection is to safeguard the individual’s privacy. In pervasive computing, data protection is even more crucial than in conventional information systems. The large number of smart objects and their spontaneous networking undermine the overall system’s controllability. Pervasive computing increases the user’s dependence on a large number of background processes that are highly intransparent. The networking of individual objects and the distributed nature of services make it hard to discern the connections between an action in pervasive computing and its consequences for the transmission and processing of one’s own data. A more in-depth discussion of data protection in pervasive computing can be found in section 7.4.1.

The experts in the online survey assessed security technology as relevant to most pervasive computing applications, though they saw biometrics as necessary only in selected applications. Remarkably, the experts believe that there are some pervasive computing applications where security technology is not relevant. These are probably either “trivial or fun applications”, or else isolated applications without an extensive network, where attacks are fairly unlikely due to the enormous effort an attacker would have to expend.

Compared to other pervasive computing technologies, marketable security technologies are expected relatively late, and a majority of the experts also worry about technical bottlenecks for pervasive computing in this field. This is probably mainly because some of the available security technologies will first have to be adapted to pervasive computing’s strong decentralisation and the limited capabilities of its components. The experts believe biometrics will be used primarily in niche applications.

#### 5.7 Machine-machine communication

Pervasive computing systems will be extremely distributed systems with thousands or millions of spontaneously interacting components. The standardisation of appropriate machine-machine interfaces and their development are thus extraordinarily important for pervasive computing.
Machine-machine communication consists of three tiers that build upon each other: the actual technical level of machine-machine communication, the services architectures that are built upon it, and finally the software agents that act autonomously on behalf of their human users.

In actual machine-machine communication – that is, peer-to-peer communication (P2P) – Sun Microsystems’ JINI (Java Intelligent Network Infrastructure) has established itself as an open industry standard for system development close to the hardware level, while the JXTA standard (named for “juxtapose”) is important for communication higher in the protocol hierarchy. Similar standards have been defined for P2P communication by HP with its Chai Appliance Plug and Play, and by Microsoft with Universal Plug and Play (UPnP).

Service-oriented architectures (SOA) describe a design model for shared use of reusable distributed systems. The aim of service-oriented architectures is to vastly simplify the integration of applications. The basic design principles of SOA are open standards that support the use of Internet protocol-based web services, an integration platform for secure message transport (enterprise service bus), and a dedicated integration instance. Another design model for developing SOAs is the industry standard CORBA (Common Object Request Broker Architecture) for communication between object-oriented software components, which was developed by the industry consortium Object Management Group (OMG).

As the networking of pervasive computing’s smart objects becomes increasingly complex, the potential for danger rises sharply, too. It is no longer feasible to explicitly programme all potential interactions among the objects, because there are just too many possible combinations. In response to this problem, work has been done for some years on software agents that have their own semantic model of their environment. As knowledge-based systems, they are able to make autonomous decisions and to adapt to their environment as a learning system. Agents can thus act independently on behalf of their human users. They translate generally formulated commands into concrete actions, choosing independently among different courses of action without consulting the user. The research field of socionics is examining how agents organise among themselves. Human interaction mechanisms are being deliberately applied as a social model for understanding the decentralised coordination of agents. A great many research groups worldwide are working on software agents, including the Software Agents Group at the MIT Media...
Laboratory and the DFG Priority Programme Socionics – Investigating and Modelling Artificial Societies.

The experts in the online survey rated the relevance of machine-machine communication as average compared to the other technology fields. Strikingly, they assessed the relevance of knowledge-based systems as comparatively low, yet most of them also wondered whether knowledge-based systems might represent a technological bottleneck for pervasive computing after all. This assessment fits with the observation that the experts apparently expect pervasive computing to develop in two stages. In the first stage of isolated applications (PvC-1), knowledge-based systems are of minor significance, whereas they will become important in the second stage of networked smart objects (PvC-2).

5.8 Human-machine interface

The smart objects of pervasive computing require developers who design user interfaces that move beyond the formerly dominant monitor/keyboard principle. Most objects will have a variety of interfaces to their environment, but these will not include visualisation components. Moreover, there will be many implicit interactions in which the user will have little or no involvement in the computing process, to avoid flooding the user with information. Even so, the user must be given the option of controlling the activities of pervasive computing by means of an appropriate human-machine interface.

The human-machine interface is not a self-contained field of technology. It is instead an interdisciplinary challenge that draws on such fields as computer science, ergonomics, the cognitive sciences and microelectronics. These days, the human-machine interface serves nearly all of the human senses:

- Voice command plays an important role in innovative user interfaces. By now, computer-controlled voice output is largely mastered. Speech recognition is more interesting and challenging, and it will continue to require further research. Conversion of speech to text is currently precise enough for dictation machines, for example.

- Similarly, voice command of a system is possible in narrow application areas with delimitable vocabulary, and is already in use, especially in call centres.

- Handwriting recognition functions well today, and it turns up in many Personal Digital Assistants, which dispense with keyboards altogether.

- In the visual realm, a number of approaches offer new forms for the human-machine interface. These are often supplementary visualizations in the user’s field of vision, such as projecting a map onto a car’s windscreen, or displaying virtual elements in the person’s field of view with head-mounted display (augmented reality). In contrast to the 3-D simulations of virtual reality, augmented reality always preserves the connection to the real world.

- Movements in a room can be captured by motion sensors and processed as system inputs, so that virtual objects in augmented reality can actually be handled, for example.

- Interesting developments in displays include flexible, large-area polymer displays, and smart paper – a paper-like rewritable display in which microspheres can be rotated so that each shows its black or white side.

- Driven especially by development of handicapped-accessible systems, sensor systems have been developed (and to some extent already implemented) that depart even further from these audiovisual and tactile paradigms. Among them are computer systems that can be controlled by head and eye movements, a puff of breath, or the measurement of brain waves. It is even conceivable that control functions could be realised directly via implants in the body.

The human-machine interface plays an important role among all makers of consumer electronics and computer systems. Companies such as Microsoft and Siemens maintain their own usability labs in order to test their products. The auto industry and its suppliers – e.g., Toyota, BMW and Mitsubishi, or their suppliers Immerson and Siemens VDO – are also working intensively on the interfaces of their
driver assistance systems, which must meet especially high safety standards.

A central challenge for the human-machine interface is to construct a semantic model of the real world, which would allow the meaning of a spoken sentence to be understood, for example. Such models have been developed as individual applications for self-contained domains, such as medicine, but a general approach does not yet exist. These developments are currently getting a strong boost from the Semantic Web Initiative of the Internet standards organisation, the World Wide Web Consortium. Semantic Web comprises a collection of standards for classification systems such as RDF and OWL, which model the real world in networks of concepts. Whether and how this approach might impact real applications is not yet foreseeable.

According to the experts’ assessment, the human-machine interface plays a rather average role, compared to the other technology fields. They do see speech technology as particularly relevant but also as a possible technological bottleneck. They view the visionary approaches of gestures and implants as less relevant for the further development of pervasive computing.
6 Pervasive Computing: Socio-economic Requirements and Impact

Tomorrow’s computers will be networks consisting of lots of specialised devices that “know” what is going on around them, can “talk” to one another and can proactively use that information. We know what the building blocks are, we know some of the applications that will be developed, but we don’t really know the true impact this will have on society, in the same way that we could not predict the impact of the Internet or mobile phones as little as twenty years ago.

Dr. Allan Maclean, Image Semantics Ltd., Cambridge, Great Britain

The preceding chapters considered primarily the applications of pervasive computing and its technological foundations; this chapter will take a comprehensive look at the impact of pervasive computing. Earlier studies on the development and impact of pervasive computing have focused primarily on specific issues, such as security and sustainability [BSI 04b, Hilt 03]. Supplementing these studies, this chapter addresses questions concerning the drivers and obstacles in pervasive computing development. The cumulative effects of pervasive computing are also addressed here.

At first glance, the field of pervasive computing seems to be characterised by several uncertainties, despite its 15-year history. One indication of this is seen in the fact that the terms pervasive computing, ubiquitous computing and ambient intelligence carry near-equal semantic weight, though each with a different focus. And yet despite certain differences, the concepts behind these terms are by and large the same. The idea of ubiquitous ICT applications available everywhere and permeating our surroundings is universal, at first glance. It is an idea that is centred more or less on smart objects providing users with optimal support inconspicuously. As of yet, however, no study has sought to move beyond general statements and explore in detail the motivations driving the development of pervasive computing applications. What goal in which field should be aimed for with pervasive computing? This kind of differentiated approach helps gather key information regarding both research and development needs as well as pervasive computing’s economic potential. One aspect of this study was therefore to question international experts on the drivers of pervasive computing, its limiting factors and impact.

6.1 Pervasive computing drivers

For clarity and consistency, one set of five key drivers or motivations behind pervasive computing have been selected from the nine application areas discussed in Chapter 4. The five drivers are:

- Economic incentives of offering new products and services
- Economic incentives of reducing costs
- Increasing personal comfort and user friendliness
- Increasing energy efficiency and materials use efficiency
- Increasing security and safety

Experts polled in the online survey were asked to evaluate the influence of each driver in individual application areas on a scale from “very weak” (1) to “very strong” (4). Based on the values given, Figure 37 below depicts each driver’s importance for each application area. There is no single driver propelling the development of pervasive computing forward in all application areas. Instead, we see very different motivations associated with each field. New products and services come closest to constituting a general driver. In production and the military sector, pervasive computing is expected to result in cost savings for health care services, which are chronically in deficit.
Comfort as a pervasive computing driver shows a different picture. In those areas where individuals use pervasive computing directly—motor traffic, communications, the smart home, medical technology and commerce—high levels of personal comfort acts as a strong motivation for introducing such systems. At first glance, it is surprising that reducing energy and resource consumption is not considered a significant driver in production, logistics and commerce. This assessment, however, corresponds with studies showing that increasing Internet commerce has not yielded the expected reductions in logistics volume. It has instead led to an increase in small shipments transported across much greater distances [KIKI 06]. Similar global value chains for individualised goods are expected to result from pervasive computing’s impact on business-related areas. In contrast, it is not surprising that experts consider the use of pervasive computing in motor traffic, medical technology and internal security to be motivated by a desire for greater security.

A look at the drivers behind each application area underscores the different bundles of motives behind introducing pervasive computing (see Figure 38). Interestingly, the experts expect cost savings and improved energy efficiency to play only minor roles in the smart home. Pervasive computing in buildings entails much more than the refined automation of facilities engineering (heating, air conditioning, etc.). It is also worth noting that, according to the experts, the impact of all drivers on medicine is strong to very strong. Clearly, pervasive computing can accommodate several demands in this sector.
6.2 Limiting factors in pervasive computing

Identifying and examining the limiting factors relevant to each application is just as important as identifying the drivers and motivations behind pervasive computing’s development, distribution and application. The current literature describes the phenomenon primarily either via individual case studies (e.g., for RFID technology [BSI 04b]) or in highly abstract and detailed terms (see [Hilty 03]). Analogous to the preceding section, experts were asked to assess twelve limiting factors in terms of the nine application areas. This was done to include the level of different pervasive computing applications, to which the literature has thus far given little attention. The twelve limiting factors are:

- inadequate trust and lack of acceptance on the part of the user
- lack of personal advantages
- privacy
- security issues
- high costs
- technical obstacles (availability and reliability)
- lack of commercial concepts/business models
- customer unwillingness to paying for pervasive computing services
- negative environmental impact/high resource consumption
- lack of legal regulation
- lack of standardisation
- inadequate human-machine interface

Expert survey findings show a similar pattern in all application areas but clear differences among the individual limiting factors (see Figure 39 and Figure 40).

Experts identify human-machine interface, data security and technical obstacles (availability, reliability) as overall key limiting factors. The first two factors come as no surprise. It is curious, however, that technical obstacles are identified as a significant problem in certain areas even though the experts anticipate adequate maturity for key technologies within the next one to four years (see Chapter 5). This finding supports the thesis stated at the beginning of Chapter 4 that there will be at least two stages of pervasive computing implementation. Isolated applications will emerge during the first phase (PvC-1), and a truly networked PvC infrastructure will develop later (PvC-2).

The experts consider environmental sustainability, resource consumption and the lack of legal regulations as lesser limiting factors. Standardisation, however, receives a great deal of attention. The importance of privacy is assessed differently.
depending on the application area considered. Privacy is considered a lesser limiting factor in both production and the military sector. However, it is a considerable limiting factor in security, communications and medicine. The relative weight given to privacy varies among the various professional groups surveyed. Across the board, experts working in industry assign less importance to this limiting factor than experts outside industry do. This was the case, irrespective of the country in which the experts are based. A similar difference between experts working in industry and others could not be established for the security factor.

6.3 Anticipated impacts of pervasive computing

Just as there are numerous drivers and limiting factors for pervasive computing (see above), the realisation and use of pervasive computing will affect both immediate and secondary application contexts. The consequences can be negative or positive, and in some cases they may overlap, making the cumulative impact difficult to measure. For example, whereas improving energy and materials use efficiency is a secondary goal of pervasive computing in a few application areas, the mass production and distribution of pervasive computing components and their attendant energy needs could offset or even negate this effect. This also raises the question as to what extent integrating and embedding system components will render recycling procedures economically prohibitive [Hilt 03]. To gain a summary assessment of the consequences of pervasive computing’s implementation, six impacts were identified that could affect individual application areas both positively and negatively and then evaluated in the international expert survey. The six impacts selected for assessment were:

- privacy
- energy efficiency
- resources/material efficiency
- public safety
- labour efficiency
- support of personal activities

The rating scale used by the experts ranged from highly negative (−2) to very positive effects (+2). The neutral mid-line was set at the scale value of 0.

To obtain a comprehensive assessment of pervasive computing’s impacts, five experts were selected for in-depth interviews held in preparation for the online survey. A modified structure-formation technique was used here. This method was intended to produce a sketch of the negative and positive impacts of pervasive computing over time from today until 2015. A total of ten incisive hypotheses were derived from these interviews and then presented to the international experts for their appraisal and assessment on a scale of 1 (“do not agree”) to 4 (“agree completely”).

The following analysis considers the six aforementioned impacts on nine key application areas and combines these with the experts’ assessments of the hypotheses. For the sake of presentation, three categories have been defined to which individual impacts and hypotheses can be assigned.

6.3.1 Impact on privacy

In their assessment of pervasive computing’s impact on privacy in nine key application areas, the international experts show relative homogeneity, albeit with a slight negative trend (Figure 41). Concerns are strongest in the application areas of automobiles, smart home and commerce, which affect the personal sphere most significantly.

![Fig. 41: Pervasive computing’s impact on privacy](image)
To obtain a differentiated analysis of pervasive computing’s impact on privacy, the international experts were asked to evaluate the following hypotheses:

- **A**: The inundation with personalised information combined with a loss of privacy will lead to regulation in the form of a “digital bubble” that will be implemented using the technical standards of data formatting and middleware.

- **B**: If privacy demands are to be addressed appropriately and sustainably, pervasive computing technologies must implement a design for privacy from the outset. Should privacy issues be handled retroactively, serious deficits in this area are likely to emerge.

- **C**: Awareness of privacy issues in pervasive computing as well as their perception and subjective assessment are part of a dynamic system. The more useful and truly pervasive applications become, the less users will be concerned with their impact on privacy and the potential misuse of data.

- **D**: Users will accept agent technology based on artificial intelligence and the resulting autonomy and delegation of pervasive computing processes once they understand the logic of personalised data automation. This is true for user profiles as context-based personalisation.

![Fig. 42: Evaluation of four hypotheses for pervasive computing in terms of privacy](image)

The experts’ response shows that a pervasive computing design for privacy that conforms to data protection standards is regarded as a requirement for ensuring privacy and is preferred to the downstream concept of context-dependent data protection filters (digital bubble) (see Figure 42). Only a technical implementation of privacy from the outset can prevent serious problems from emerging (hypotheses A and B). Experts view the claim that highly useful applications might offset concerns for privacy as relatively unimportant.

It is worth noting that the experts do not expect user acceptance of automated and personalised pervasive computing functions to be facilitated by an understanding of processing logic alone. The experts appear to consider pervasive computing’s functional logic too complex for people to follow it in detail at any given time. This assessment dovetails with the Taucis Study findings, which suggest that trust is a key requirement for the implementation of pervasive computing [Lütg 06]. Indeed, the importance of trust will most likely depend on the individual application area. In the expert survey, a lack of trust was seen as a potentially limiting factor in medicine, automotives, security and commerce.

Interestingly, the thesis that German experts would rate pervasive computing’s impact on privacy more negatively than their non-German colleagues could not be confirmed. A two-factor variance analysis showed no significant differences for these groups.

### 6.3.2 Economic impact

Labour efficiency in particular is expected to yield positive effects most clearly in the key economic areas of production, logistics and commerce. It will, however, not play an important role in smart homes (see Figure 43). No significant efficiency gains from pervasive computing are expected for housework, professionals working at home, and homecare of the elderly and/or ill.

Moderately positive effects are anticipated for increasing energy and resource efficiency. Significant increases are expected, however, in production and especially logistics.
Three hypotheses delineating the economic impact of pervasive computing were presented to the experts. The topics addressed were outlined as follows:

- **E:** Due to the high-level integration of electronic components into everyday objects, recycling will grow increasingly challenging. Existing recycling procedures for items such as textiles, plastic, paper or glass will have to be adapted for pervasive computing components.

- **F:** The automatic organisation of technical systems is a central feature of pervasive computing. This will facilitate new, economically important business practises and models in commerce and production (self-organised automated production).

- **G:** Context-awareness requires pervasive computing components with a perception of their environment that relies on an “inner world model”. Knowledge-based systems and/or software agents are a key requirement for such models and could thus represent a serious technological bottleneck. Therefore, every effort must be made to find top-quality pervasive computing solutions in this area.

Hypotheses E and F refer to concrete effects of pervasive computing. According to the experts, pervasive computing’s potential for commerce and production is immense because of its ability to self-organise (see Figure 44). Such self-organisation depends on several things, including the availability of fully developed knowledge-based systems.

Developing these systems in turn, however, poses a particular challenge (Hypothesis G). The experts agree that newly adapted recycling procedures will be needed to allow for the re-use of pervasive computing components that have been integrated and embedded into everyday objects (Hypothesis E).

### 6.3.3 Social impact

The experts predict clear positive effects for pervasive computing’s support of personal activities in medicine, home, communications and automobiles, while moderately positive effects are expected in internal and external security, and in production, logistics and commerce. Improvements in security are anticipated primarily in military and security-related applications (inner and external security), but especially in medical applications. The automotive branch will also profit somewhat, according to expert opinion (Figure 45).
Three further hypotheses addressed other impacts of pervasive computing on society as a whole.

- **H**: Fundamental improvements in efficiency resulting from ubiquitous availability will be negated by the increase in time consumption due to the handling of personalised and precise information.

- **I**: The influence of pervasive computing on social behaviour will surpass the influence of television. Human dependency on technology will change qualitatively; people will increasingly lose contact with physical reality and their natural surroundings.

- **J**: The total utility of pervasive computing will take a back seat to the consumption of resources necessary for the production and operation of pervasive computing components.

It is noteworthy that the experts do not anticipate negative “rebound” effects, which would offset positive impacts (see Figure 46). The experts see no rebound effects for labour and attention efficiency (hypothesis H), resources (hypothesis J) or for increasing alienation from one’s environment (hypothesis I). A variance analysis confirmed the supposition that Germans employed in industry would agree less with hypothesis J—that the total utility of pervasive computing would take a back seat to resource consumption—than Germans not employed in industry. Interestingly, the opposite is seen among respondents based outside of Germany: those employed in industry agree most with the hypothesis as compared with every other sub-group. A variance analysis also confirmed the hypothesis that experts based in Germany assess pervasive computing’s influence on safety more critically and view it less positively than experts based outside Germany.

### 6.4 Winners and losers in pervasive computing

To examine the impact of pervasive computing in terms of potential winners and losers, the experts were asked to identify those social groups they expect to be affected in either negative or positive terms by future developments. The respondents were not prompted with examples. Interestingly, several groups, especially the elderly and people with little technology experience, are identified both as pervasive computing’s beneficiaries and its disadvantaged. The elderly and handicapped were mentioned frequently as pervasive computing beneficiaries, as were businesses in the fields of logistics, commerce and technology, and mobile workers. These findings indicate that it is ultimately the manner in which pervasive computing is used that will determine whether these groups will in fact profit or suffer disadvantages as a result of pervasive computing.

To avoid a digital divide in which society is split between those with and those without access to pervasive computing, easy access to pervasive computing in technical, financial and intellectual terms is required. The first generation of pervasive computing applications in particular are likely to demand a certain level of knowledge and requirements that will result in a temporary division between pervasive computing winners and losers. However, this divide should subside as the functional logic of later pervasive computing generations is automated and cost-effective mass production sets in. According to one of the online survey respondents, “Once the technology has matured and becomes publicly available, the less educated will begin to profit from it. If this does not happen, they will continue to fall behind.” The financial attainability of pervasive computing access is also of key importance. An elaborate medical home monitoring system may offer a desirable function. However, as pensions decrease, and if such a device is not adequately covered by health insurance and must be arranged and paid for privately, it will facilitate, rather than overcome division.

---

3 Analysis of variance is a statistical method in which predetermined expected influences between variables are confirmed or rejected (see [Back 06]).
Other groups that experts believe could suffer disadvantages as a result of pervasive computing include small businesses and retail, political minorities, critics or sceptics, marginal groups and persons with “unusual” backgrounds. Also highlighted in this context are persons who intentionally avoid participation in a pervasive computing-based system or those who cannot participate. Pointing to entire countries lacking a pervasive computing infrastructure, some experts also speak of a digital divide on the global level.

6.5 Pervasive computing: assessment of technology effects—conclusions and consequences

The online survey findings fill the gap between the detailed individual analyses of selected pervasive computing issues and technologies [BSI 04b, Hilt 03] and general considerations. The fine-tuned levels of differentiation in the survey and its resulting cross-linkages point to important indicators for pervasive computing development.

The experts’ responses suggest that the current development of pervasive computing is still driven primarily by technology. Clearly, the development of technical concepts is not balanced with adequate user benefits. The European Commission’s concept of ambient assisted living (AAL) is one example of a successfully established utilisation model in the pervasive computing context [EC 03]. The AAL concept brings together the pervasive computing application areas smart home, medical technology and safety to enable the elderly, ill or handicapped to stay in his or her own home as long as possible. This concept foregrounds the technical support of everyday routines, including safety issues. For example, windows can be automatically closed when leaving the house and gas stoves switched off under certain conditions. Vital signs, too, can be monitored. The groundbreaking idea here is that of a supportive technical infrastructure that serves as a co-opera-

![Fig. 47: Key trends, developments and dependencies in pervasive computing. (Arrows within the category describe evolutionary processes, arrows reaching across categories represent influences.)]
tive system. It will not take over all tasks completely, but rather will relieve an individual of those aspects that he or she can no longer accomplish alone, and which are essential to completing an activity safely. This kind of approach calls for both the use of personal profiles for regular activities and routines as well as context-based personalisation for responding to spontaneous decisions. This utilisation model corresponds with the experts’ evaluation that near universally positive effects can be expected as a result of pervasive computing in all application areas relevant to AAL.

The online survey findings together with those of the five in-depth expert interviews show a multifaceted picture of pervasive computing’s developments. Despite a degree of indistinction in some responses, key trends and steps can be derived and placed in relationship to each other. Using these findings, a visualisation grid was developed in which a cumulative cross-section provides an overview of pervasive computing’s key aspects (see Figure 47).

In terms of pervasive computing’s technological development, a process with at least two stages can be expected. During the first stage (PvC-1), the characteristics mobility, ad hoc networking and embeddedness will be realised initially in individual devices. Developed further, the mobile telephone could become a key product offering even more options for communication and control than are broadly available today. In PvC-1, user profiles will help context awareness and a certain ability to personalise be realised. According to the experts, this step will be turn-key ready in the next one to four years, though this will be a step-by-step development, which is the case for all of pervasive computing.

PvC-1 is comprised primarily of isolated smart objects with additional or refined functions resulting from the integration of microcontrollers. Media ruptures will continue in the following interim phase, which will be dominated by use model- or manufacturer-defined isolated applications. Only later will this be replaced by a truly open networking structure (PvC-2).

---

Fig. 48: The two stages of pervasive computing development: individual devices in PvC-1, networked and context-aware smart objects in PvC-2
In equal measure, this interim step is both a requirement for and a consequence of the transition from PvC-1 to PvC-2, which fundamentally affects the issue of user privacy, but also the safety of technical infrastructure. Only a fault-tolerant system that offers opportunities in compensating for functional deficiencies and data loss (redundancy, decentralisation, self-diagnosis, self-configuration, organisation and control) can possibly satisfy the high security demands applicable here.

In addition to the aforementioned characteristics, networked PvC-2 will feature—depending on the application area—widespread energy autarky, highly developed context awareness and automation capabilities. Once these characteristics have been established, complex tasks can then be delegated to pervasive computing applications. Availability here is expected within approximately ten years. Fundamental challenges in terms of data security, protecting the private sphere and privacy will result from the capability of numerous objects in pervasive computing to network spontaneously. A design for privacy must be implemented consistently to meet these challenges step-by-step—as is already the case for PvC-1. Figure 48 summarises the development outlook for pervasive computing as derived from the experts’ responses.
7 Security in Pervasive Computing

The vision of pervasive computing is one of people in enchanted houses, on enchanted streets or beaches, in enchanted offices or forests. Those who carefully look, listen or feel, may notice the myriad signs, messages and teasers - even the physical shifts and changes - that magically keep them on track of their journey, keep them focused on their activity or – why not – pleasantly distracted, so that “being there” feels easier, more pleasurable, more effective and – in the end – better for all. The question is “Who decides what better means?” Not all enchantment is well-intentioned or harmless.

Dr. Walter Van de Velde, CampoRosso, Brussels, Belgium

The exchange of information between large numbers of smart objects is a central property of pervasive computing. Smart objects differ considerably from other objects in terms of their input/output capabilities, sensory interfaces and application processes. Pervasive computing processes are, for the most part, designed to run as inconspicuously and situationally dependent – and therefore semi-automatically – as possible. It is thus essential that information be exchanged between authorised persons and/or objects only. Data and information must be allocated clearly and protected from manipulation and espionage. The secure identification of and communication between objects and persons in pervasive computing is therefore of vital importance. Equally important is the protection of users in the event of smart object failure or malfunction. As the first pervasive computing systems are introduced, technical issues in security, safety and privacy will fast become decisive.

As it stands now, pervasive computing is for the most part a technological vision. However, the general shape of future security architectures in pervasive computing as well as their associated opportunities and risks can be outlined. Using three different scenarios, this chapter explores the unique security challenges posed by pervasive computing in terms of the objectives of security, privacy and safety.

Identifying persons and objects is both an application of pervasive computing (e.g., digital IDs) and a central internal operation required to make pervasive computing services safe and reliable. Because different technical approaches will be used to identify objects and persons, it is essential that we prove able to distinguish between the two. The first scenario provided here considers the identification of objects. The second scenario examines the identification of individuals via biometric universal identification. Both scenarios rely on technology in use currently. These include the Trusted Platform Module (TPM) for object identification and the ICAO-Standard for biometric identification systems. The third pervasive computing scenario involves the interaction between vehicles and telematics systems. It was chosen because several experts responding to the online survey regard this field to be one of the earliest applications of pervasive computing. This scenario takes a visionary look into the future and draws upon the findings of current research projects.

7.1 Scenario 1: Object identification with TPM

In object identification, objects are recognised according to firmly assigned characteristics. We can distinguish three system components.

- An identification number (ID) serves as a unique code for each object. The object contains an ID carrier – usually a chip – in which the ID is stored.
- A reader identifies the carrier-object via the ID.
- The carrier-object and the reader exchange the ID and other information by means of a communication interface.

As indicated in [BSI 04b], the following scenarios constitute foreseeable threats:

- **Falsification of content**: If an attacker gains unauthorised access to an ID carrier, it can change and/or falsify content.
- **ID falsification**: The attacker acquires an ID and potentially accesses an object’s secured informa-
tion. It then uses this information to fake its identity vis-à-vis a reader.

- **De-activation**: An attacker renders the ID carrier useless through unauthorised delete or kill commands, or by destroying the carrier physically. No longer able to determine the ID of the carrier object, the reader cannot recognise the object.

- **Removal**: An attacker physically removes an ID carrier from the carrier object and associates it with another object. Intentionally switching the barcode labels of goods is one such example.

- **Disturbance**: An attacker can disturb the interface, i.e., data exchange between an ID carrier and reader. Air interfaces, for example, are relatively sensitive and can be disturbed by jamming transmitters.

- **Blocking**: An attacker/intruder prevents the identification of an object by blocking the reader, which prevents data exchange.

- **Eavesdropping**: Communication between the reader and the ID carrier via the corresponding interface is intercepted and decoded by an attacker. Interception is quite easy with air interfaces such as radio links.

- **Falsifying the reader ID**: In a secure authentication system, the reader must prove its authorisation to the object in order to be identified. An attacker with its own reader can fake a non-existent reader authorisation.

- **Reader removal/de-activation**: An attacker can de-activate, remove or somehow render a reader useless, thus disabling the object identification process.

- **Adding a reader without permission**: An attacker can install an unauthorised reader that carries out object identification without being noticed. This is possible only if the object identification procedure in use permits a reader to start and/or carry out an identification process without the consent of the object to be identified.

![Fig. 49: Basic types of attack on object identification (confirm [BSI 04b])]
There are different preventive measures for the threats discussed here, all of which depend on their respective baseline technology. Two major technologies are currently being discussed in relation to object identification in pervasive computing: RFID (Radio Frequency Identification) and TPM (Trusted Platform Module). RFID is often used as an independent identification system for objects with no integrated electronic components. Typical RFID applications today include logistics systems in which the movement of goods is monitored using RFID, which is comparable to an advanced barcode label. A TPM, by contrast, is designed as a separate chip that is integrated into an electronic system with a microprocessor and communications system. A TPM, therefore, fulfils the criteria of a smart object in pervasive computing to a greater extent than an RFID-Transponder. A TPM also offers additional comprehensive functions for the secure identification of objects. The following section illustrates the use of TPM in pervasive computing object identification. A detailed analysis of security issues in RFID is given in [BSI 04b].

7.1.1 Trusted Platform Module

Developed and standardised by the industrial consortium Trusted Computing Group (TCG), Trusted Platform Module (TPM) functions somewhat like a smart card embedded within a device [TCG 04a, TCG 04b]. Unlike a smart card, however, the module is not bound to a user, but rather to an electronic device or system, which can be a PC, a mobile phone or a MP3 player. TPM thus allows for the unambiguous identification of objects in pervasive computing. For example, when paying with a credit card by means of electronic communication, there is currently no guarantee that the transaction command was given by the actual cardholder and that the transaction was received by an authorised company. Processes such as these require a relatively high degree of mutual trust. During credit card transactions, order transaction software can use TPM to ensure that data are transmitted to an authorised server. TPM can also ensure that the device used by the individual placing the order represents a trustworthy platform. Data encryption prevents the unauthorised use of credit card and transaction information.

The underlying mode of operation for TPM is anchored in key-based identification and secured access through the storage of passwords and various asymmetrical key pairs in TPM [TCG 04]:

- The Endorsement Key Pair (EK) is non-migratable; it cannot be transferred to other platforms. It involves a RSA key pair that is assigned to a genuine TPM. The EK identifies a genuine TPM and therefore the device in which the TPM is integrated.

- Attestation Identity Keys (AIK) are also RSA key pairs that are created using a genuinely assigned EK. The device user can generate as many of these key pairs as desired. The Endorsement Key Pair (EK) is migratable and can be transferred to other platforms. Because different identities can be created and represented with AIKs, they allow for the creation of pseudonyms and anonymous identities, among other things.

- The Storage Root Key (SRK) serves to encrypt/decrypt all the data and keys saved in a TPM and protect them from unauthorised access. The SRK must be generated; it does not exist at the outset. The SRK is generated by the owner within the TPM by means of a specially designed command. The encoded key never leaves the TPM, but can be deleted by the user.

TPM basic functions are:

- **Creation and protection of cryptographic keys**: Keys are created, used and saved in a secure manner within the TPM. Never having to exit the TPM, they are protected from software attacks. Their level of protection from hardware threats is also very high and comparable to that of smart cards. TPMs are to be built in such a way that any physical manipulation or destruction of the module inevitably entails the destruction of data, because the data cannot be decoded/read without an intact TPM.

- **Sealing**: By creating a checksum from the system configuration (hard and software), data can be bound to a single TPM (sealing and sealed storage). Data are encrypted on the basis of a checksum. Decoding is possible only when the
same checksum is once again identified, which, in turn, is possible only on the same system. Sealing prevents the data from being read if the TPM breaks down or is lost.

> **Hardware protection:** The TPM can determine whether the system hardware has been manipulated as soon as the computer or device in which the TPM is integrated is switched on (authenticated boot). Assuming the device was delivered by the manufacturer in a trustworthy condition, the activation of the device should be equally trustworthy.

> **Third party attestation:** The user must have his AIKs signed by a Trusted Third Party (TTP). The certificate produced during the creation of the TPM must also be sent to the TTP by the user. A service provider, however, can verify himself via TTP only. This attestation allows the provider to verify whether credible components are in use on the user’s system, and whether the attestation is signed with an AIK. The service provider can check via the TTP whether the second party has a TCG-compliant system; it does this, however, without being able to truly identify the issuer of the AIK. This procedure has the disadvantages of being relatively expensive and complex due to the required TTP, which is usually provided in the form of Trust Centres.

> **Anonymous attestation:** The Direct Anonymous Attestation (DAA) procedure is based on a complex mathematical procedure, a so-called group signature scheme, which does not require a TTP [BCC 04]. This improvement is designed to eliminate a major criticism of the attestation procedure, namely the complex and expensive attestation via a Trusted Third Party.

### 7.1.2 Security of object identification via TPM

The following discusses object identification security using a TPM with a focus on security, safety and privacy.

**Security**

The possible threats to object identification specifically in terms of TPM implementation are examined first:

> **Falsification of content:** An attacker could attempt to falsify data by gaining unauthorised write access to the TPM chip. This type of attack can succeed only if the EK and any other secure information, such as other keys, remain unaltered and allow the reader to continue identifying the TPM chip ID correctly. In order to create a new AIK, for example, an attacker must successfully submit the faked identity of an authorised person to the TPM and/or device. The likelihood of an attack depends more or less on how difficult the object’s owner makes it to fake his/her identity.

> **ID falsification:** The attacker acquires an ID and potentially accesses an object’s secured information. It then uses this information to fake its identity vis-à-vis a reader. This can occur either via the use of a device able to emulate various TPMs, or by producing a duplicate TPM chip. Such an attack results in the circulation of several objects with the same identity. This type of attack is highly unlikely at this point; as of yet, there are no devices able to simulate and/or duplicate TPMs.

> **TPM de-activation:** An attacker renders the ID carrier useless through unauthorised delete or kill commands, or by destroying the carrier physically. Depending on the manner in which the TPM has been de-activated, the reader is either no longer able to determine the ID of the object or no longer able to recognise it. The TPMs technical specifications, however, are designed in such a way as to protect the data by rendering them useless in the event of such an attack.

> **TPM removal:** An attacker physically separates the TPM from the carrier-object and associates it with another object, which then assumes the ID of the original object. Because a TPM is usually embedded and/or integrated firmly in an object, it is relatively difficult, if not impossible, to remove it without destroying it.
Eavesdropping, blocking and disturbance: The TPM is integrated firmly in the object to be identified. The three threats to communication between the reader and the object to be identified are not influenced directly by the TPM. Their particular risk level depends on the interface and the protocol used. Radio links are especially high-risk in comparison to a cable or other type of fixed interface. The TPM does, however, offer mechanisms that support the use of adequately secure communication protocols.

Falsifying the reader ID, unauthorised addition of a reader: In a secure authentication system, the reader must prove its authorisation to the object in order to be identified. If an attacker seeks to mask his/her reader as read-authorised, it must take on a corresponding identity. This type of attack is either very easy or almost impossible to carry out, depending on the security measures used. A TPM offers mechanisms that make such an attack very difficult. Ideally, a reader would also feature a built-in TPM, so that the object could easily identify the reader and determine its authorisation and vice-versa.

Reader de-activation and/or removal: The TPM has no influence whatsoever on the de-activation or removal of the reader. The risk involved here is very much dependent on the design of the reader.

The TPM process provides extensive support for applications and/or users in achieving security objectives, in particular the secure authentication of objects. The TPM process also makes it possible to protect confidentiality by creating and storing data encryption keys in a more secure manner than pure software-based solutions.

The TPM process also supports the protection of anonymity by permitting the resulting AIKs to represent different identities. The process can also lead to the loss of anonymity, however, because a device with a TPM can be clearly identified via EKs. If a genuine affiliation between a device and a person is achieved, then it is no longer possible for the user of the device to remain truly anonymous. In pervasive computing, a distinction must be made between the competing security objectives of anonymity, on the one hand, and identification and authentication on the other. The ultimate goal should be to give the user the freedom to choose between the two.

The availability of an application is not directly influenced by a TPM. A TPM is, however, able to ensure the integrity of a system and to recognise changes in hardware and/or in the system configuration (cf. authenticated boot). This makes it essential that an intentional change to the system does not lead to an unintentional system failure.

The TPM can support the non-repudiability of actions by creating and saving the keys necessary, for example, to sign data. These keys are usually signed by a trustworthy third party, as described above.

Privacy

On the one hand, a TPM can enhance privacy by supporting the protection of personal data by means of sealing (see above) or data encryption. However, on the other hand, it is also possible to gather personal and/or behavioural information about a person when using a TPM while a corresponding device is being allocated to this person. This is not a problem as long as the user is able to switch the TPM off at will. If TPM use is mandatory, however, an individual user cannot protect him/her-self from the collection of data. It would be possible for service providers to offer and/or withhold particular services whereby, once again, user-related data could be collected. The risk is minimal, however, as long as the requisite conditions – in particular the forced use of the TPM – are not in place. The question arises as to whether it is preferable to bind data directly to people during the identification process, instead of binding data to devices and then devices to persons. It is possible, for example, to encrypt the data with a key extracted from biometric characteristics. This data would also be transferable in an encrypted form among devices and bound to the user only.
Safety

A TPM has no fundamental influence on the safety of the objects into which it is integrated. For example, a computer continues to function even after a TPM has malfunctioned – with the exception, of course, of the functions provided by the TPM. Today’s microelectronics allow for the integration of an additional TPM chip into an electronic system that reduces safety only insignificantly in the event of malfunction. However, depending on how the TPM application is implemented, the entire system could fail in extreme situations. If, for example, the entire hard drive of a laptop were encrypted and the key needed to decrypt the system were contained in the TPM, the system would no longer be functional if the TPM malfunctioned. The object itself – the laptop – could continue to be used, e.g., after the hard drive was reformatted and a new system installed, but the old hardware and software system would be unusable. Everyday objects with data such as texts, images and music could be affected by the TPM. Documents from certain text and image processing programmes, for example, could not be opened using other programmes if they were interconnect­ed with the functions of the TPM. [Hans 04]. A technical monopoly such as this would affect the safety of digital documents.

If all, or at least several, essential applications are inter-connected with a TPM in such a way that the failure of a TPM would entail the failure of the application, it is urgent that a backup strategy for TPM failure be created, especially if one aims to avoid a scenario in which TPM failure means a loss of the device. A solution in which replacing the TPM with an identical system (clone) is made easier carries with it the attendant danger that attacks made possible by the cloning of a TPM are also made easier.

7.1.3 Opportunities and risks of object identification with a TPM

A TPM provides the technical means with which object identification in pervasive computing can achieve security objectives such as authentication, anonymity, confidentiality, integrity and non-repudiability. However, it is crucial that the means provided by the TPM are actually used by the system into which it is integrated. The provider of a TPM-based application and the user of the TPM device profit differently depending on the type of application.

Digital Rights Management (DRM) is one of the key fields in which TPMs find application. In the music industry, for example, many efforts are currently underway to limit the playing of music on certain devices. One scenario includes designing an MP3 player in such a way that the user could play music on that specific device only, using an Endorsement Key Pair. This would introduce an effective means of protection against pirate copies, which would surely lead to a major reduction in music industry losses resulting from unauthorised copying. This would limit, however, the user’s freedom of use with the device and/or his/her music by preventing it from being copied onto another device. A similar scenario is possible in the use of the TPM process in PCs, whereby the use of licensed software would be inevitable. There is currently no protocol governing the manner in which TPM security functions could be implemented with the greatest consideration possible for security and interoperability in application environments.

Even more questions are raised by the fact that the TPM makes it possible to identify objects unambiguously. When object identification simultaneously allows the allocation of the object to a person, which is explicitly requested in many cases, it becomes impossible to maintain the anonymity of the user. Pervasive computing in particular allows for the clear traceability of actions. This, in turn, allows for the creation of both virtual and real profiles, e.g., purchasing profiles, which are based on the movement and behaviour of users. This form of profiling poses a great challenge to privacy and consumer protection, and will require special legal attention.

Another major field of operation for the TPM process, in addition to DRM, is Trusted Computing, i.e., the creation of trustworthy platforms and devices with a TPM. For example, orders and/or purchases made via mobile phones, which are transformed into trustworthy platforms through the use of a TPM, illustrate the use of TPM in pervasive computing. Without the use of a TPM, the trustworthiness of participating devices remains open as
manipulation, in many cases, cannot be recognised immediately.

On the one hand, the use of a TPM promises a clear security gain. On the other hand, however, authentication carries with it the potential for misuse by allowing a third party to restrict control over the hardware. A third party, such as a bank or digital content provider, can render the execution of an action dependent upon the current status of the client’s system. These functions do indeed help protect the digital content of service providers and users. However, a service provider could also build in market entrance barriers or create user profiles. TPM makes it possible to link a particular software to a particular hardware, which means that TPM use might support alliances between hardware and software producers, with, for example, the goal of displacing competitors from the market.

In terms of the further development of TPM-based security mechanisms in pervasive computing, special attention must be paid to the fact that the security gains associated with the ability to clearly identify users imply a resulting loss of anonymity. Considering the social importance of the two equal security goals of authenticity and anonymity, it is essential that an open discussion about the possible consequences of TPM take place among users and application and service providers. One solution might be the introduction of individual freedom of choice between authenticity and anonymity depending on the application context.

### 7.2 Scenario 2: The universal ID

Access to buildings and events, the use of services and transport, business transactions – all of these activities can be carried out by authorised persons only. The authorisation to perform an action, along with the corresponding identification of the person performing the action, is protected in many ways by special forms of identification. Consequently, there are currently several IDs and cards such as passports, personal IDs, driver’s licences, health cards, insurance cards, credit cards, EC cards, company IDs, client cards and tickets for public transport, etc. Due to the sheer quantity of ID documents needed in daily life, the concept of a universal identification (UID) is likely to emerge. The UID would encompass all of the above functions while simplifying serviceability for its holder.

There are currently several pilot projects with aspects along the lines of a UID. While Austria’s current “Bürgerkarte” (citizen card) contains only a person’s name and address, a new version is in the works that would contain additional information such as the social insurance e-card containing social data, the Bankomat card containing account data and a student ID containing matriculation information [ASIT 06]. Belgium, Finland, Italy and Switzerland have already introduced similar citizen cards. Other multi-functional card applications include, for example, the National ID Card in Oman, the Moscow Social Card in Russia and the National Health Insurance Card in Taiwan. [Glob 06, Horn 05]

There are similar initiatives in Germany, too. The electronic passport (ePass) has been in effect since November 2005, while the electronic health card is currently in the pilot project stage. The creation of a digital ID is also being discussed, often in connection with the health card [Stru 06].

The more far-reaching D-Me scenario is described in [DBSL 01]. D-Me is a device capable of ad-hoc identification and communication. It can, for example, be integrated into clothing and even implanted into people.

The pilot projects described here with respect to multifunctional cards and the D-Me scenario represent the starting point for a possible UID scenario in pervasive computing. The cards already in existence today, with their accompanying infrastructures and...
mechanisms, would be parts of such an identification solution.

The UID encompasses a large number of both long-term and temporary functions such as insurance cards, credit cards, EC cards, company IDs, public transport passes and airplane tickets. Forms of official personal identification, such as driver’s licenses, social insurance and health insurance cards, and their accompanying data, could also be transferred to the UID. Combining previously distributed and function-specific ID carriers onto one UID carrier would result in an all-encompassing personal digital key for pervasive computing. The user could use this to identify him/herself and carry out a number of different private, public and national applications. Such a UID would not necessarily have to take on the appearance of a smart card, but could, for example, be integrated into an armband or wristwatch, as described in the scenarios in [DBSL 01].

One of the major properties of a UID in pervasive computing is that it allows for the unambiguous digital identification of its owner. With the implementation of digital personal identification, identification via knowledge can be distinguished from identification through ownership and biometric characteristics. For example, if a person is identified only via the possession of the UID carrier, such as a handheld, only the UID carrier is recognised. This form of identification results in the same security problems, risks and opportunities described in section (7.1.3.) on object identification. Furthermore, it is important that only the person assigned the UID has access to the UID carrier. The secure identification of such a person is dependent upon it.

Identification via knowledge functions in a similar manner, for example, by means of a password or a PIN. In this case it is important that the information required to perform the identification is accessible only by the authorised person. It is also essential that the password/PIN cannot be guessed. A common form of identification combines ownership with the knowledge of a password or PIN, as for example, in the use of debit cards. In this case, the physical card must be provided and a PIN entered in order to conduct a payment transaction. If the card and PIN are given to another person or stolen, both characteristics can be transferred to another person, which means that here, once again, personal identification takes place only indirectly via the object. In pervasive computing, identification via secret passwords and PINs plays only a subordinate role, because the implicit communication of smart objects with users and among each other does not permit an opportunity to enter a PIN or similar signature. In the personal identification of the UID, human biometric signatures carry out a more secure identification than recognition via object possession. A person can be identified based on individual biometric data or a combination thereof.

The UID scenario described here does not entail, in spite of the use of biometric identification, neither the mandatory capabilities of the electronic passports already in existence nor of the projected digital personal ID. Legal regulations in Germany, particularly § 18 of the German Passport Law (PassG) and § 4 of the Personal ID Law (PauswG), oppose such coupling, each with respect to use in the non-public sector [BMJ 06]. The scenario assumes, however, that the UID will follow the biometric procedure specifications set by the International Civil Aviation Organisation (ICAO) for electronic passports, which currently offer the highest degree of security. Many citizen ID projects today are already arguing for compatibility with ICAO guidelines [Meis 04].

The world’s major certification authorities – the ICAO refers to them as the Country Signing Certification Authorities (CSCA) – play a vital role in the UID scenario. They are responsible for ensuring the maintenance of security. In the UID scenario, this task could be given to either a public or private institution. Both variants are in use today: the top certification authority of the Austrian citizen card is A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH in Vienna. Other private certification service providers are also possible: in Hong Kong the national Hong Kong Post serves as the only certification authority for digital IDs. As far as one can tell, every country has corresponding national signature laws that each certification authority must satisfy [Horn 05].

In addition to its ability to represent different IDs from different contexts, a UID would also contain both changeable and unchangeable information. This could even occur within one context itself. For
example, while biometric identification data would remain unchangeable, other data on the ID could be changeable. For example, this could mean allowing for a change of address without having to issue an entirely new UID. Other UID functions that facilitate frequent changes will most likely also become the rule. This applies, for example, to the process of determining a person’s professional status, i.e., whether someone is a student, a trainee, employed or unemployed, as well any associated authorisations such as special admission prices. The same applies to public transport tickets and their respective tariffs, special offers and much more. Under certain circumstances, it might be desirable for the cardholder to be able to change specific data themselves, e.g., at public terminals specially designed for this purpose.

7.2.1 The biometric identification system of UID according to ICAO

Even before the attacks on the World Trade Center on 11 September 2001, the International Civil Aviation Organisation (ICAO) had already defined standards for digital travel documents with biometric functions and communication abilities via RFID. The attacks have expedited the USA’s introduction of digital passports in international tourism. The first German digital passports were issued in November 2005. Although the ICAO standards apply to travel documents, it appears that many national IDs and an entire series of citizen cards will also follow this standard. [UrMe 05].

According to ICAO standards for the security mechanisms underlying the UID, a global Public Key Infrastructure (PKI) is required to sign and check digital documents. Each participating country must create a two-stage PKI consisting of exactly one Country Signing Certification Authority and at least one Document Signer (DS). The CSCA is the top certification authority in a country for travel documents. There is no superordinate certification authority in the world. This is the only way to guarantee that each country has complete control over its own

---

Fig. S1: Relationships between actors in Universal ID
keys. Document Signers are authorities authorised to sign digital documents and make the actual physical UIC carriers, such as the German Bundesdruckerei (the now privatised federal printer in Germany). For the UID, either public or private institutions could assume the role of the highest UID certification authority, similar to the CSCA. There can be several UID certification authorities in one country, or one certification authority for several countries. In the following UID scenario, the CSCA is replaced by the term "top UID certification authority". Private or public institutions could also take on the function of a Document Signer similar to that of the Bundesdruckerei. This could be a central service provider for the institutions involved in the UID. Institutions such as health insurance companies, commercial businesses and municipal offices, for example, could distribute the UID carrier.

The key-pair created by the top UID certification authority is used exclusively for the certification of DS institutions. Each DS has at least one key-pair that can be produced by the DS itself. The private key is used exclusively for signing digital documents, while the public key must be signed by the top UID certification authority. The duration of use for the DS' private key is much shorter than that of the public key. This allows for the least possible number of UIDs to be affected if the key is compromised. [ICAO 04a] shows how a compliant structure can be implemented without having to fix all the characteristics in detail. For example, one can choose to implement either the passive or only the active authentication described below. Ideally, all mechanisms would be implemented.

The ICAO has four planned mechanisms to achieve the security objectives of authenticity, integrity and confidentiality in personal identification: passive authentication, active authentication, Basic Access Control and Extended Access Control [ICAO 04b].

Passive authentication: Passive authentication allows for the verification of the authenticity of the data on the chip. It also determines whether the data have been changed. However, there is no check whether or not the UID carrier is the authentic carrier-object for the chip. During the authentication the Document Security Object (DSO) is read, by which the Document Signer can be verified. The DSO is a data structure signed by the DS according to RFC 3369 [ICAO 04b]. The signature of the DSO is examined with the help of the public key of the DS. The validity of the Document Signer’s certificate, signed by the top UID certification authority, can be verified with the public key of the top UID certification authority. The relevant data are read and the associated checksums (hash values) are examined. If the signatures of the hash values are correct, one can assume that the data has not been changed.

The ICAO also specifies two optional schemes designed to increase the security of the authentication: Basic Access Control and active authentication.

Active authentication: Active authentication serves above all to protect against UID cloning. It does not, however, provide protection from unauthorised users reading the content of the UID card. The UID features a key-pair comprised of one private and one public key each, and the public key is signed by the Document Signer. The public key for active authentication must be linked to the corresponding UID carrier and to the corresponding biometric data. Otherwise, an attack involving the use of another UID carrier than the one presented as an oracle designed to answer active authentication requests is possible. For this reason, active authentication is accompanied by optically scanning the person with the UID carrier.

Basic Access Control: Basic Access Control (BAC) guarantees the confidentiality of data contained in the UID chip. The ICAO adopted Basic Access Control due to the fact that communication between identification documents and a reader can be intercepted within a range of up to several metres, as was demonstrated by the German Federal Office for Information Security in experiments involving standard RFID systems [FiKe 01]. There are two secret keys stored on the UID that are designed to ensure that the data contained in the UID chip is read by authorised readers only. Following ICAO specifications, the keys can be derived from optically readable data on the UID carrier. A wristband provides relatively little space in comparison to a card. The ability to store optically readable data on a small surface is therefore essential. Data could, for example, be stored using a 9 x 9 point matrix (dotcode) on a one square centimetre surface with high infor-
mation density and error correction capabilities. This data would then be read using a compliant reader. Dotcodes have been in use for some time now, mostly in industry [BARC 04]. A 9 x 9 point code entails 81 bits of entropy at random scores. If greater entropy is desired, a larger matrix of 16 x 16 points (256 bit) on approximately 1.5 square centimetres is conceivable. It is important here that a genuinely random number is used for the optically readable UID number to prevent the UID carrier from being tracked (see the discussion on tracking below). To access the data stored in the UID, a reader must have a sightline connection to the optically readable data. This prevents data from being read secretly.

Extended Access Control: The top UID certification authority in each country determines who has access to the biometric data of UID carriers. UID issuers associated with other top certification authorities must agree to the respective access rules of the original top certification authorities. This authorisation can be refused or revoked at any time. The UID carrier verifies the reader’s authorisation and thus guarantees its validity. The UID chip then checks the reader certificate as part of a challenge-response protocol. However, one significant risk remains: as long as the certificate is valid, a reader could continue to accept the top UID certification authority of a UID, even if the authorisation for that UID has been recently revoked. This could occur, for example, in the event of policy changes relating to the issuer. Issuing certificates with shorter periods of validity would help limit this risk.

The following section explores the potential impact of a combined UID for personal identification on security, privacy and safety.

7.2.2 The security of a universal ID

Security

Taking into account ICAO-defined mechanisms for biometric personal identification, the following section discusses relevant potential threats to security.

Falsification of authenticity: In principle, it is possible that an attacker could attempt to forge a UID – i.e., to write a chip with his/her own data. This could, however, be detected by using the passive authentication scheme described above. The private keys of the DS and the top certification authority must be stored in such a way as to make them inaccessible to unauthorised persons, especially as an attacker could use them to create a UID chip with a false identity.

Integrity falsification: It is conceivable that an attacker might attempt to alter the content of a UID chip. In this case, passive authentication should provide the same protection it would in the case of a fake passport. It is also possible that, should an attacker gain access to the private key of the DS or the top UID certification authority, s/he could create a UID chip with a fake identity rather easily.

Copying the UID carrier: An attacker could attempt to copy a UID chip’s data without being seen, for example if s/he has access to a lost UID carrier or comes close to it. Active authentication can prevent this from happening. The private key of the UID chip is not readable; the chip itself cannot be duplicated.

Skimming: An attacker could attempt to use a reader to read a UID without the owner noticing. The Basic Access Control described above protects against skimming. At a recent ICAO meeting, experts recommended including additional Faraday cages [Juels05] to protect digital passports from unauthorised reading. This could be very useful for a UID carrier, especially if realised as a smart card. This could be slipped into an aluminium covering, which would make illicit reading even more difficult.

Eavesdropping: An attacker could attempt to eavesdrop on the communication between a UID carrier and reader. Based on today’s RFID standard technologies, active communication is limited to a maximum range of 15 cm. However, passive eavesdropping on communication is possible up to a distance of 2 metres [FiKe o]. For this very reason, ICAO has decided to encrypt communication by using Basic Access Control, which presupposes an optical line of sight between reader and UID carrier.
Access to biometric data on the chip: The Extended Access Control mechanism described above is decisive in rendering access to biometric data difficult. Without this mechanism, access to the data on the UID carrier chip entails automatic access to biometric data.

Man-in-the-middle attack: In a man-in-the-middle attack, the attacker targets both the system environment and the user card. The attacker manipulates communication between the reader and the UID carrier by intercepting the data stream between the two components and then either manipulating the data at both ends or passing on new commands and answers. It is possible that neither side would notice that communication is taking place with a false partner. This kind of attack must be rendered impossible, especially while security precautions are being established. A man-in-the-middle attack also includes the manipulation of verification results on their way from the UID carrier to the reader. In line with the findings of the ePassport feasibility study, various interfaces could be defined with a UID as a smart card [Reich 05]. These might include a contact-bound interface for establishing key security applications and a contactless interface for less critical UID functions. In general, however, contactless chip cards compliant with ISO/IEC 7816 now provide security mechanisms comparable to those of contact-bound chip cards.

Tracking: An attacker can compute a key by optically reading the data. With access to a reader, s/he can create motion profiles. This means that the attacker could collect information on whether a person is at a certain location at a certain time. Protection against such an attack requires that the static key of the UID be assigned randomly. This prevents the key area from being isolated, which is required for a successful brute force attack. As long as the contained key area is large enough to prevent an attacker from locating the key, such an attack remains largely impossible.

First and foremost, the UID would render genuine user authentication possible. This would be its primary function. Often linked to authenticity, the goals of confidentiality and integrity would be facilitated by a UID.

The UID could support anonymity if it offered a function involving the supply of pseudonyms. The provision of pseudonyms, however, is effective only if it can be guaranteed that no access to the UID’s other data and functions would be granted. If this were not the case, then the UID would serve the purpose of identifying people, which implies the exact opposite of anonymity.

The availability of an application is not directly influenced by a UID. However, since the UID serves to identify individuals, a UID malfunction or breakdown automatically means that an application requiring UID authentication would no longer function. Because it allows for the confirmation of a person’s identity, the UID is suitable for supporting actions designed to achieve non-repudiability.

Privacy

In the UID scenario, many personal data are stored on the UID. It is therefore very important that the data stored on a UID cannot be read by unauthorised institutions. This also means that authorised bodies will have access only to the specific data for which they are expressly authorised. Multi-application chip card technology could be used for UIDs in the form of a smart card. This technology makes protecting certain data on a smart card from access by non-authorised bodies possible. Current developments in smart card technology allow for the implementation of different, individually-protected applications on one medium. This can be done, for example, by using different, application-specific PINs, passwords or authentication keys [Reich 05].

However, a technical solution for a UID wristband that would give only authorised institutions access to the data relevant to them without involving direct interaction with the user would be unsatisfactory. The user him/herself must be given the opportunity to decide in each case, when and who has access to which parts of his/her UID.

In addition to the risks posed by unauthorised access to UID data during normal use, a lost UID poses an equally high risk in terms of data protection. The UID contains a multitude of personal data on, for example, the person’s health or financial sta-
tus, and numerous institutions have access to portions of this data. These risks are pronounced particularly when insufficient security measures have been implemented to prevent unauthorised persons from gaining access to the data of a lost or stolen UID.

The question remains as to whether a distribution of risk, i.e., the distribution of data onto several identification media, is more sensible than the use of only one UID carrier. The principle utility of the UID, i.e., the bundling of many functions into one medium, would indeed vanish, but, on the other hand, the risk of data misuse would be reduced significantly.

Safety

Unlike individual cards and documents, a UID has no fundamental influence on the safety of the procedures into which it is integrated. The integration of different chips and functionalities in a UID carrier should affect safety minimally. If the UID carrier is not functioning properly, the application or process into which it is embedded will either be discontinued or at least disturbed—depending on the implementation scheme. The loss of a UID carrier poses a very high risk, especially considering the multitude of applications that might be associated with it.

Security threats in biometric personal identification

In recent years, the use of biometric methods has increased enormously. This is due primarily to technological advances that allow for the rapid and relatively high quality of biometric characteristics measurement and evaluation with comparatively little effort. [BIOPIII] includes a detailed discussion of the different approaches used for identity documents. The potential for using facial geometry as a biometric characteristic – as examined in [BIOPII] – could also be used in a UID application.

Biometric characteristics include:

- iris or retina patterns
- fingerprint
- face
- palm structure and vein recognition
- hand geometry, hand line structure
- voice and speech patterns
- handwriting
- keystroke rhythms
- voiceprint
- gait
- scent
- DNA (genetic fingerprint).

Biometric identification follows a distinct process. In the initial "enrolment phase", a reference sample (template) is generated by a person’s biometric characteristics. This sample is then saved in digital form and protected from unauthorised access. When the person next encounters the biometric system, an up-to-date sample is taken and compared to the reference sample. The system then decides whether or not the two samples are adequately similar and thus, for example, whether access may be granted or not.

There are several different kinds of conceivable attacks on biometric identification systems:

Sensor deception: The biometric sensor represents the first point of attack on a biometric system. For example, many optical and capacitive fingerprint sensors can be deceived by means of a mock fingerprint. An attacker can more or less "easily" deceive these sensors, depending on their characteristics and quality. Individuals talented at imitating other voices might be able to imitate a person’s voice well enough to fake an identity at a certain microphone. A good make-up artist would most likely be able to deceive an average camera by giving Person A the same facial bone structure as Person B. However, if the sensors and the biometric process are of a high enough quality, such an attack would prove very difficult.
**Data acquisition attack**: Fingerprint data are considered to be public domain because people usually leave them unwittingly and imperceptibly on objects they have touched. In a data acquisition attack, a fingerprint can be taken from an object such as a used glass. After transferring the print to paper, the data can be then scanned and digitalised. A professional attacker would presumably be familiar with the data formats of the system – even if these are proprietary and not published by the manufacturer – and that they would be able to generate the proper verification data from the raw data. Where no security mechanism is in place to prove the immediate origin of the sensor’s verification data, a smart card with, for example, a fingerprint sensor, would function as if the data were coming from the sensor and being processed by the trait extraction. The security status of a successful biometric user verification would be recorded on the card and would therefore facilitate misuse of a protected function.

**Hardware/Software manipulation**: If an attacker can modify hardware and/or software, they might also be able to influence specific aspects of the verification process or even the entire process. This possibility, however, rarely arises.

**Reference data falsification**: An attacker could attempt to change or switch the reference data used for comparison with the data generated during the verification process. When Person A succeeds in replacing Person B’s reference data with his/her own, then Person A will, of course, be identified by the system as Person B. The success of such an attack depends upon the structural conditions of the specific system. Biometric reference data are generally supposed to be secured in such a way as to make this impossible.

**Falsifying the result**: An attacker can try to falsify the results of the verification process directly. At the very end of the process, and independently of it, the result is changed according to the attacker’s wish. A system that allows such an attack would not only provide zero protection, but would also provide the attacker the opportunity to prevent other persons’ access.

**Hill climbing**: This type of attack requires that the attacker gain knowledge of similarity values, which result from comparing reference traits (templates) with query traits. In a type of brute force attack, the attacker then tries to increase the similarity values by performing minimal changes to the acquired query traits. There are mathematical procedures for this trial-and-error process. However, one can easily protect oneself against this kind of attack by ensuring that the system does not pass on any similarity values to the outer world, but rather only the values “successfully identified” or “not identified”.

**Replay attack**: Another possible attack entails the system configuration permitting access to the data line through which the biometric verification data are transferred. An attacker can then record the data of a successful user identification and use it for a so-called replay attack after they have stolen the card from its rightful owner or at least taken possession of it for a period of time. As is well known, many users will leave their biometric smart card in the card reader all day long so as to avoid having to insert the card for each authentication process. The attacker bypasses the biometric sensor and sends the recorded data again to the user card. At this point, they would have the opportunity to misuse the card.

**Trait theft**: An attacker can remove a finger and take it with him/her. This kind of theft is much more difficult to perform with facial features. Dynamic traits such as a signature or other characteristics that depend on human behaviour, such as a person’s gait, are impossible to steal; they can only be imitated.

### 7.2.3 Universal ID: opportunities and risks

A universal identification would spell for an initial increase in user comfort. The user would be able to identify him/herself securely for a number of digital communication transactions – in public transport, at the doctor’s office, in a hotel, at the bank and at public offices – without having to remember several PIN numbers and passwords or run the risk of having a stolen UID misused.

In addition to this high degree of user friendliness, a UID would allow strong biometric identification...
mechanisms to be used for almost every process in which the user must be identified as a person, all with relatively little effort. Although this type of strong identification exists in some cases today, e.g., personal IDs must be shown to purchase a prepaid mobile phone, open a bank account or when signing a purchase or rental contract, the use of an omnipresent UID could make this the norm. The ease and availability of the UID could prompt the creation of a new set of procedures even for secondary processes and small financial transactions. For example, the date of birth contained on the UID would make it possible to determine the age of a person attempting to purchase cigarettes. The UID could also be used as the only ticket needed for access to public transport. People who either cannot or will not own a UID would be excluded from these processes, which could lead to a splitting of society into UID owners and non-owners. It is therefore imperative that UID issuing be an open and inexpensive process for everybody. One must also be able to guarantee that all processes can be used without a UID and that this alternative access is not associated with any specific consequences – such as high fees or less comfort.

In a UID scenario, several data can be stored on a UID, some of which are very sensitive. Also, all institutions wishing to use the UID’s authentication for their processes must have access to the data on the UID. In principle, these institutions thus have access to very private data and are able to create user and motion profiles over time without the knowledge of the UID owner. It would also be possible for the UID owner to manipulate his/her own data. An adolescent, for example, might attempt to change his/her age so that s/he could gain access to prohibited products such as tobacco and alcohol. UID security thus faces special demands. Specific data must be protected from manipulation by other bodies – such as other issuers or the owner of the card him/herself – and data from other issuers must be protected against an unintentional overwrite. Ideally, the data should be stored on the medium in such a way that only authorised users can gain access in the manner intended by the issuer.

For the user, the loss of a UID would be much more serious than the loss of individual cards. If the UID carrier, either in the form of a card or a wristband, featured a sufficiently strong level of access protection that prevented its use by anyone other than the user him/herself, then it would be possible to issue a copy of the ID, or even several identical IDs, so that if one is lost, its integrated functions could be replaced quickly. Alternatively, if a UID is lost, it should be possible to issue a replacement quickly. However, considering the many different issuers involved, this would prove less than simple. One potential solution to this problem would be to establish a top certification authority similar to the Country Signing Certification Authority associated with the electronic passport. Such a UID trust centre would manage all of the necessary data and would therefore be able to issue a new medium quickly. However, given the much larger amount of data contained in a UID as compared with that of an electronic passport, this would involve a significantly more complex process. Furthermore, as manager of the entirety of an individual’s data for all applications, such an issuing authority would be able to establish unwanted cross-linkages at any time. Clearly, a centralised issuing authority poses a high risk to an individual’s private sphere. The potential for misuse and the high sensitivity of data must be thoroughly considered in deciding whether such a UID trust centre should be state-run, private or a combination thereof. Given the crucial importance of such a centre for the entire UID system, its operator would have to meet very high security demands. A breakdown at the centre would result in a breakdown of the entire system and a deliberate infiltration of the centre’s key administration would compromise all identities in the entire system.

7.3 Scenario 3: Distributed telematics systems

For some years now, considerable progress in automotive engineering has been made thanks to the increasing integration of micro-technological and micro-electronic components. In addition to optimising processes such as motor management and brake performance with ABS, new functions have been added recently that support and assist the driver. Vehicles are becoming co-operative systems. Sensors monitor the road’s surface, automatically switch on windshield wipers and headlights, and control driving safety within physical limits.
Advanced systems provide night vision capabilities with movement sensors able to identify pedestrians long before a driver can see them. Navigation systems are yet another form of electronic support that have become standard in new cars. By combining data gathered directly by the car’s sensors and positioning data from GPS, exact information on the most effective and safe route possible can be produced. In addition, GPS and (soon) Galileo data can be used to provide traffic updates and other information on location-based services, such as the way to the next hotel or auto repair shop.

Currently, most telematics systems are centrally organised, which poses certain problems. Updates on icy road conditions, traffic jams, construction sites, etc., must first be reported to the central station before they are entered and/or updated in the telematics system. This process unavoidably results in a time delay. Certain drivers may not receive information fast enough to avoid situations such as a traffic jam.

One solution to this problem comes in the form of a distributed telematics system that uses all information gathered by each vehicle with local sensors. As the modern vehicle is, in effect, a mobile sensory station, the various pieces of information collected by individual vehicles could be made available to other drivers. A form of direct communication can be created between vehicles with the use of ad-hoc networks. This car-to-car communication allows information to be exchanged to optimise traffic flow. For example, one vehicle’s information can notify others about pedestrians, obstacles or accidents on the road, but also about icy patches that might not have been processed by a central telematics system. Such warnings could either be sent automatically between vehicles or communicated based on the driver’s need, as was done via CB in the past.

Other types of information exchange based on this structure are conceivable, such as the transfer of specific and location-dependent tips or directions. This information could be exchanged either within closed groups or communicated by individual drivers to the entire network. Vehicles could also be provided Internet access to road networks, which would, in turn, use the individual vehicles as relay stations. Sensor stations placed at the side of the road near dangerous locations could send warnings to approaching vehicles. These stations could also help to increase the area in which Internet access is available for the vehicle. This kind of capability, however, demands a relatively open and flexible access to the ad-hoc system, which is most easily created with existing standards such as WLAN or, in the future, WiMAX. Alternatives include UMTS or individual transmission standards. Connecting to backbone networks would allow a vehicle to communicate bi-directionally with several service providers such as hotels and gas stations. Information between different transport systems could also be exchanged in intermodal transport, which would optimise travel times.

Active safety applications could, at first, merely assist drivers, intervening in the actual control of a vehicle only when the driver ignores information and warnings. The driver’s behaviour at the wheel could also be monitored at the same time and, for example, the speed of the car reduced in the case of sudden speed limit changes or fog. An ecological approach to traffic management could include, for example, a smog alarm that steers heavy commercial vehicles with particularly high emissions clear of sensitive areas or even guides them to the next car park.

The distributed telematics system scenario includes the following actors:

- vehicles
- their drivers
- the infrastructure, which consists of traffic signs – e.g., electronic apparatuses for flexible traffic lanes, traffic signals and traffic or local signs – and transport telematics systems, such as traffic and park guidance systems, toll systems, navigation and detection system, as well as
- facility services and applications provided by motorway restaurants, petrol stations, car parks, hotels etc.

The scenario for distributed telematics draws upon:

- current research projects such as Germany’s Net-
work on Wheels [NOW 05] [NOW oJ], the EU’s PReVENT [Prev oJ], the US’s Vehicle Safety Communication (VSC),

- the completed European research projects Inter-Vehicle Hazard Warning [IVHW 03], FleetNet – Internet on the Road [FEL 01] [Flee oJ] and SOFTNET (Software Engineering for Soft Networking) [BRSS 02] [SOFT 02]
- the activities of the industrial consortium Car2Car Communication of Europe [C2C oJ] and Advanced Cruise Assist Highway System Research Association of Japan [ITS 03] [InOs 04]

7.3.1 Security in decentralised telematics systems

Communication in distributed telematics systems generally occurs via ad-hoc networks. The security of these networks must be guaranteed at all times. Confidentiality and data integrity must be ensured even when, for example, data dissemination occurs spontaneously and is carried out in broadcast mode. Appropriate measures must be taken if the receiver is to have confidence in the data. The following three problems must be solved:

- Communication between vehicles and the infrastructure system is based on a highly dynamic ad-hoc network. There are unknown participants and time for communication is short.

- Radio communication technology is based on standards set in the home and office area, which means attackers can disturb communication and manipulate systems relatively easily.

- As communication participants, all vehicles differ due to their different manufacturers and generations. However, all vehicles should be able to communicate safely with one another. [Lüb k 05]

Security

Four areas subject to threat can be identified in this scenario. These include routing, car-to-car communication, vehicle-to-infrastructure communication and the driver communication with the system.

Routing attacks: When vehicles communicate among each other and with an infrastructure in an ad-hoc network, it is possible that a node along the communication route between two partners is not adhering to the prescribed routing protocol or preventing communication [PSSS 05]. Such a failure can lead to the incorrect disclosure of data packets. Intended falsification of position can lead to a denial of service (DoS) at the end nodes. Mechanisms must therefore be developed that can recognise individual node failure and bar negative impact as much as possible. Network security and data protection solutions are currently under development in [NOW 05].

Routing within ad-hoc networks is particularly vulnerable because attacks do not necessarily have to come from outside – they can be carried out from nodes within a routing path. Given that each participating node simultaneously represents a routing node, this is a critical point. Should an attacker be located on the routing path, or act as a general participant in an ad-hoc network, s/he can attempt to perform the following attacks:

- Network interference: The attacker uses regular routing mechanisms to, for example, overload individual nodes or an entire area with messages. The attacker’s goal here is to cut off the node and/or an entire area by overloading the network (DoS attack). The attacker could also discard routing packets. After successfully creating a routing path, which contains the attacker’s node, it even could discard all data packets (Black Hole Attack, or those of a certain participant (Grey Hole Attack) [HuPe 04]. Other possible routing attacks include wormhole attacks [Hu 03], the creation of routing loops and network partitioning [MiMo 02] through false routing information. Wormhole attacks occur when the attacker sends node messages to a node in the network with which s/he is connected via a secure tunnel. The messages then enter the network via the addressee.

- False message infiltration: False message injection includes both signalling packets and data packets. In other words, different messages can
be falsified and sent, depending on the process used. [ABDF 0J] discusses beacon and location query messages as signalling messages that are required for routing and potentially vulnerable to message infiltration. An ad-hoc network can tolerate false messages up to a certain point, beyond which routing operability can no longer be guaranteed.

Violation of the private sphere: The private sphere and/or the anonymity of a participant are threatened if data packets are eavesdropped or motion profiles can be established (e.g., via positioning data in [ABDF 0J]) through a node on the routing path.

Attacks on car-to-car communication: Communication between vehicles includes warnings against obstacles that, for example, cannot be seen on the road ahead. Two types of attacks can be identified here. The first involves the injection of false messages; the second involves disturbing the entire system.

Injection of false messages: An attacker can attempt to create new valid messages, to re-send saved or previously sent messages, or modify existing messages. To create new valid messages, an attacker must either override the cryptographic system or acquire authorisation to create and disseminate new messages. An attacker could also manipulate a vehicle’s hardware, e.g., modules and sensors, in such a way that false messages are generated automatically by the manipulated elements. To manipulate a message, an attacker must be able to intercept a message, save it temporarily, and breach its integrity protection, i.e., crack its cryptographic algorithm. If an attacker can re-inject an old message, this means s/he is able to deceive the corresponding communication protocol. This is typically done by falsifying protectionary mechanisms such as time stamps and creating new valid time stamps that replace the old stamps or inject the message quickly within a valid time frame.

System disturbance: There are different ways to disturb a system. An attacker can try to de-activate or disturb various nodes, which would lead ultimately to a DoS attack. The attacker could then overload the system’s electronics with an

![Fig. 52: Traffic management with distributed telematics systems](image-url)
electromagnetic impulse. S/he could also exploit vulnerable points in individual systems with the goal of de-activating and/or shutting them down. Wireless communication is especially vulnerable to DoS attacks, because attackers with strong knowledge of RF technology can relatively easily prevent communication through the use of jamming transmitters. Finally, an attacker can attempt to exploit weaknesses in the standard IEEE 802.11p, upon which the networks used for car-to-car communication are likely to be based. An attacker’s goal here would be to disturb, falsify or eavesdrop on communication.

**Attacks on vehicle-to-infrastructure communication:** In terms of susceptibility to attacks, vehicle-to-infrastructure communication is more vulnerable than car-to-car communication. Infrastructural entities are more easily accessed, disassembled and destroyed than individual vehicle components. The example of traffic signs in rural areas illustrates this principle. Infrastructural entities can also be connected to various fixed networks such as the Internet. There two possibilities here: fundamentally disturbing the system or sending false messages.

- **System disturbance:** To disturb a system in terms of a DoS attack, an attacker can simply destroy certain elements or render them inoperable in the widest sense. Disassembling or destroying street signs is a relatively easy procedure for an attacker. A sophisticated communication system designed to ensure security will not help much in protecting against this type of vandalism. A similarly easy, but more effective attack entails interrupting the power supply to corresponding entities. An attacker could also use jamming devices that would prevent any wireless communication within a certain range. Given that vehicle-to-infrastructure communication is essentially dependent upon WLAN use, those threats described in [BeSa 03] typical for IEEE 802.11 are also relevant here.

- **Injection of false messages:** The points discussed above regarding threats to car-to-car communication also apply to the injection of false messages in vehicle-to-infrastructure communication. Changing or exchanging traffic signs is yet another relatively easy way for an attacker to send false messages. These signs could then send messages and warnings to vehicles within their range on command by the attacker. For example, an attacker could maliciously place a sign indicating a reduction in speed to 30 km/h on a motorway. This sign could be configured in such a way that only those vehicles featuring an automatic speed limit function that has been activated by the driver would respond to it. Should not all vehicles be using the automatic speed limit function from the very start, this kind of attack would result almost inevitably in traffic accidents. Another attack might involve communication between a vehicle and a motorway rest stop, in which the restaurant menu or petrol prices could be manipulated. A motorist could even refuel with the improper fuel. Infrastructural elements permanently connected to the Internet are also more vulnerable to the dangers facing contemporary computer networks such as viruses, worms and other damaging software. If sensors are used, these too could be exchanged, manipulated or faked to send false messages automatically.

**Attacks on driver communication:** In terms of potential attacks on those interfaces explicitly involving a driver, there is only one physical interface to consider: that between driver and vehicle. Within this scenario, this means that the driver relies upon communication via those systems and/or networks that are integrated within his/her vehicle. If WLAN or other technologies such as Bluetooth are used within the vehicle, then all known threats to these individual technologies are also possible here. It should be noted that a driver in a moving vehicle who is communicating via Bluetooth with his/her vehicle is much more difficult to eavesdrop on than a person sitting on a bench and surfing via WLAN on the Internet. If the interface between a driver and a vehicle is in the form of a display or other format, then attacks on this interface are limited to attacks on the vehicle itself. All communication through the logical interfaces takes place via the vehicle. For this reason, the threats are the same as with routing, car-to-car and vehicle-to-infrastructure communication. Each threat to a network route between participants affects the logical connection. Further threats include all the known high-level threats such as message injection and fal-
sification by a third person or the driver him/herself.

In this scenario, the driver communicates with other drivers, services and/or service providers, and traffic telematics systems. The driver is thus exposed to attacks from all of these entities. Also, the incessant flow of information and queries sent to a driver can result in stimulus overload, depending on the system and the range of events it communicates. Drivers could be distracted in the same way drivers are currently distracted by using mobile phones while driving. The driver could also make poor decisions based on false information provided him/her by the system, which might not be functioning properly or have been attacked by destructive software. In extreme cases, this might lead to an accident.

Sending an emergency call is the most important service used by a driver in the event of an accident or breakdown. Other foreseeable applications include automatic payment of toll or parking fees and the use of general information services such as entertainment for rear passengers, sport reports and stock updates. The impact of a successful attack varies, depending on the application. Whereas the failure of entertainment services can be, at best, annoying to rear passengers, delaying or preventing an emergency call can be a matter of life and death.

At the moment, there is no safety architecture able to ensure the goals of security for communication in a distributed telematics system. However, solutions are currently under development with pilot projects such as the NOW Project [NOW 05].

**Safety**

Increasing road safety is the fundamental task of telematics systems. Even the rather simple task of monitoring basic conditions can have a significant effect on overall safety. The ability of telematics systems to influence vehicle operation depends upon whether the vehicle is still or under extreme operational conditions. Today’s distributed telematics systems support and assist the driver only indirectly, meaning that they have initially no direct influence on the operation of the vehicle and thus on the vehicle’s safety, as decisions regarding vehicle operation are made by the driver alone. However, as mentioned above, each additional sub-system affects the vehicle’s operational reliability and brings with it potential safety risks that must be taken into consideration. The more directly a distributed telematics system can influence the vehicle’s operation, the more dramatic a potential mistake can be. The presence of several metrics and sensors within such a system poses a fundamental problem, as they can be manipulated and deceived.

In such a case, the driver and/or the vehicle could over-react, or respond incorrectly or unfavourably to a given situation. Such an event could affect safety in such a way that the system would no longer be able to adjust for the mistake, for example by engaging ABS or ESP. Plausibility checks [ABDF 01] are one means of enhancing safety. For example, data picked up by sensors could be compared with messages received by other drivers. This way, such things as warnings against icy conditions in summer would simply be ignored as implausible.

If all of a vehicle’s on-board systems are networked, and if the car has a permanent connection to the Internet, an attacker could, under certain circumstances, pose a threat to the safety of the automobile. Drivers who use such systems must be able to switch either individual components or the entire system off at any time in order to protect against potential damage.

**Privacy**

Distributed telematics raises difficult and serious issues in terms of data security and privacy. The position of a vehicle and therefore its driver is always detectable and can be stored, allowing for the creation of comprehensive motion profiles. The possibilities here reach far beyond those of the toll system recently initiated in Germany, which is limited to the Autobahn and has no effect, for example, on urban centres. When the location of a vehicle is detected, no personal data is initially generated. The driver and owner of a private vehicle are frequently not the same person. However, the vehicle can generally be associated with a person close to the owner or a member of the owner’s family. This
means that, in principle, one is dealing with the collection of data that can be attributed to a person.

Other personal data, such as a driver’s favourite radio stations, could also be registered automatically. A driver’s purchasing habits could be monitored, for example, if s/he pays for goods at petrol stations and restaurants using a pre-installed system in the vehicle or if the payment is initiated via an automated system. User profiles could also be created using data gathered on the driver’s use of local services.

Vehicles are likely to connect externally with telematics systems, but also “inwardly”. In other words, devices such as mobile telephones, PDAs and computers used by the driver and passengers are likely to be temporarily integrated within the vehicle’s network. This is the case particularly if the vehicle features Internet access. In parallel with the underlying concept of pervasive computing, this kind of inter-connectivity enables carriers of personal data to be linked with a global communication and information system. They are thus, in principle, universally accessible. Appropriate mechanisms are needed to protect these data from unauthorised reading and manipulation.

7.3.2 Opportunities and risks in distributed telematics systems

The objectives for creating intelligent vehicles capable of communication include improving traffic flow, increasing energy efficiency and comfort. In principle, these goals are to be met by improving traffic safety. "Because 93 percent of accidents are the result of human error, the EU Commission has set itself the ambitious goal of halving its 41,000 annual traffic fatalities by transforming the automobile into a rolling communication centre by 2010" [Reck 06]. Distributed telematics systems allow for a significant improvement in traffic safety by providing an exhaustive picture of the potential dangers lurking in the vehicle’s immediate and extended environment. Up-to-date information on the traffic situation along a driver’s route also allows for improved traffic flows. In addition to facilitating economical driving, this also improves overall traffic security [PSSS 05].

Though distributed telematics systems can help to improve traffic safety and traffic flow significantly, they also entail considerable risks with respect to data protection. If used consistently, such systems can easily produce motion profiles and thus be stored as personal data.

This data security risk is exacerbated by the fact that the individual components of a vehicle are integrated more and more strongly, communicating with each other via a bus system. Today, ABS, ESP and other components must be co-ordinated in order to maintain control over the vehicle according to the laws of physics. Further developments in driver-assistance systems have led to components that feature a central control unit. This unit also communicates with its digital environment via car-to-car communication and telematics systems. Information on a vehicle’s steering and braking behaviour can be linked to the data of its driver, thus allowing a person’s driving style to become an additional part of his/her data profile. Sensor data could be easily stored and read to contain damage, specify repairs and “personalise” maintenance. However, it could just as easily record travel and accident data – without the explicit intent of the driver.

The integration of components in distributed telematics systems and the creation of a total system also threaten the vehicle’s basic functions. A successful attack against the vehicle might lead to the sudden use of its brakes or ABS malfunction. As vehicle malfunction could, in extreme cases, result in a severe accident or death, very high security standards are required for these systems. Whether or not the risks outweigh the opportunities depends entirely upon how the systems are designed and implemented. As is the case in the aerospace industry, this raises the question whether the ultimate power of decision should be given to humans or to a technical system. There are solid arguments in favour of each option. Legal issues as well as the degree of functional and informational security are determining factors here.
7.4 Outlook Security requirements for future pervasive computing

Ongoing miniaturisation allows for the ubiquitous presence of computers and smart objects. This phenomenon, along with the interlinking of digital networks and attendant pervasive computing, is leading progressively toward the context-aware and adaptive exchange of information. The concept of cyberspace is thus being turned inside-out. No longer depicted as a digital simulation, the real world will become part of a ubiquitous digital network. Realising pervasive computing leads to a situation in which a digital terrain will exist in parallel to the physical landscape. This terrain will not limit itself to humans and their communication; it can potentially involve and depict the environment in its entirety. The number and density of nodes within pervasive computing’s technical infrastructure will determine to a great extent the performance of this digital terrain – and therefore its degree of resolution and gradation.

While today’s users are usually conscious of the ICT applications they are using, several exchange and application processes will run independently in pervasive computing. In terms of its own claims, pervasive computing will function only when two conditions are met – when smart objects interact seemingly imperceptibly with one another and when services emerge that are available at all times and require no explicit human operation. Information processing becomes an endless background activity.

Pervasive computing systems thereby exhibit a unique set of characteristics as compared to other information systems. Pervasive computing systems are largely decentralised and complex systems involving a multitude of service providers and operators. This also means that pervasive computing systems will be vulnerable to several different types of disturbances, attacks and technical malfunctions. Human beings will not take conscious note of several interactions in pervasive computing.

One can therefore assume neither a user’s explicit consent to an activity nor knowledge of the possible consequences of his/her actions. In addition, vast amounts of data will be involved with pervasive computing, which could easily result in personal data or data attributed to a person being collected and evaluated automatically.

Some initial requirements for the security of future pervasive computing systems can be derived from the pervasive computing scenarios presented here. Others have reached similar conclusions, including [Frie 06] and [Lütg 06]. Whereas [Lütg 06] emphasises user control over the pervasive computing system, [Frie 06] emphasises user comprehension of the security architecture.

7.4.1 Privacy in pervasive computing

The protection of personal data will apply in pervasive computing as in other ICT systems. [Frie 06] provides a detailed discussion of European regulations applicable to pervasive computing. Consumer protection and copyright protection are among the many regulations included.

There are two key directives addressing the recognition and maintenance of privacy: the US Privacy Act of 1974 and the EU directive 95/46/EC. The first addresses the gathering and distribution of personal data contained in files held by U.S. national authorities, the second concerns the protection of the individual with respect to the use and trafficking of personal data. Germany’s Federal Data Protection Act (Bundesdatenschutzgesetz) as well as the OECD’s regulations protecting individuals’ private sphere and the international exchange of private data also address this issue. In its 1983 judgment on census-taking, the German Constitutional Court (Bundesverfassungsgericht) devoted special attention to the particular risks involved in automatic data processing and ultimately acknowledged privacy (informational self-determination) as a fundamental right.
The fundamental right of informational self-determination

“In the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the Art. 2 Par. 1 GG in connection with Art. 1 Par. 1 GG. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data.”

Excerpt from Judgment of the First Senate (Karlsruhe, Dec. 15, 1983) in verbal negotiations October 18 and 19, 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in proceedings on the legality of census-taking in Germany.

Privacy is meant to ensure an individual’s ability to control the portrayal of him/herself in various social roles. It is also the basis of free and democratic communication. Privacy aims to create a mode of communication that enables individuals to have control over the exchange of information pertaining to them and exercise free, democratic will. There are three maxims with respect to personal data: data minimisation, authorised use of data and data processing transparency, i.e., enabling individuals to monitor and consent to their data being processed.

In pervasive computing, however, the principles of data protection run up against subjective and objective limits. Alone the expected multiplication of data processing procedures in all facets of life will exceed users’ attention spans. In addition, ubiquitous computer technology will be designed to run in the background and provide imperceptible support to human beings in their everyday activities. No human being would accept having to acknowledge and confirm thousands of notices or directions in their daily activities.

It remains unclear whether the data acquired through many pervasive computing applications could be associated with an individual or not. If and when this data becomes associated with an individual, it often does so only after the fact, which makes it difficult to establish criteria for limiting the use of personal data. The permanent exchange of data between different media and applications also makes it particularly difficult to ensure that data are used for authorised purposes only – especially considering the fact that data are stored in networks that constantly change their logical structure. The close link between the real and digital worlds in pervasive computing would enable an individual’s motions to be tracked. This could be done by following a smart object in a person’s possession on its path through the digital terrain. As the properties of context-awareness and autonomy grow in pervasive computing, so too will the need for service providers to comply with data protection requirements such as information processing transparency, data authorisation and data handling consent. User trust in data protection adherence is therefore of crucial importance, if pervasive computing is to gain acceptance [Frie 06, Lang 05a].

Pervasive computing does not stop at national borders. The protection of an individual’s private sphere must be international. And yet, data protection models in the United States and Europe already differ fundamentally. In contrast to European framework legislation, data protection in the United States is regulated by a combination of statute law, state legislation and voluntary obligation [Genz 04]. In Europe, the principle of explicit consent applies in the processing of personal data in information systems (opt-in), while many regulations in the United States are based on the user’s expressed denial of his/her personal data being processing (opt-out). At the moment, the Safe Harbour Agreement between the EU and the U.S. Department of Commerce permits the transfer of personal data, and U.S. companies comply voluntarily with strict European data protection regulations. However, several problems with the agreement remain, including the disclosure of personal data to third parties and the actual implementation of European data protection regulations within participating U.S. companies [DPP 04]. As of yet, it remains unclear whether the Safe Harbour Agreement will provide a sufficient basis for the consistency needed in pervasive computing data protection regulations between the United States and Europe. No such agreements currently exist with Japan and South Korea, where pervasive computing activities are also widespread [Frie 06].
7.4.2 Security

As information systems, pervasive computing systems are threatened by eavesdropping, disturbance, falsification of trusted communication lines, and access to or manipulation of protected information. The imperceptibility, ubiquity and inter-connectivity of smart objects make these attacks particularly dangerous, precisely because actions within the system cannot be monitored by individuals, service providers or infrastructure operators. Digital identity theft constitutes one example of a direct attack on the integrity of pervasive computing. By shattering the trust in a harmonious linkage between the real and digital world, this kind of attack would damage the very idea of pervasive computing directly and sustainably.

The technical means for protecting security in pervasive computing are, in principle, already available. However, many of the existing security technologies will need to adapt to pervasive computing’s limited hardware components and high level of decentralisation. This applies above all to the implementation of a public key cryptography, which is costly in terms of resources, and the attendant need to create a central certification authority. Generally, the weakest link in an security chain will determine the security level of the entire system.

In pervasive computing, as in other digital networks, the IT security goals of authenticity and anonymity are in competition with one another. The possibility of a secure identification of persons brings with it a loss of anonymity. This also applies even when objects only are identified, as they usually can be directly or indirectly associated with a person. In case of doubt, one must decide which security goal has priority. Ideally, the user should be able to make this decision him/herself on a case-by-case basis.

Freedom of access without discrimination will play a decisive role in the overall acceptance of pervasive computing. One obvious idea would be to enforce the use of a security infrastructure in smart objects. This would be possible, for example, with a TPM that prevents unauthorised copying of digital media and the illegal manipulation of hardware and software integral to a system’s security. On the other hand, this could also result in weakened or discouraged market competition, censorship of unpopular political content and to the exclusion of certain groups from participating in pervasive computing. When the use of pervasive computing becomes the norm in certain situations – such as payment or identifying persons – it is essential that the technology be user-friendly, and its access non-exclusionary and reasonably priced. Otherwise, pervasive computing threatens to create a digital divide in which the elderly and the poor are refused access to fundamental activities in society.

Non-exclusionary access also implies the guarantee that no data profile can be created to determine a user’s access to services (scoring). Such profiles are already used in market research. Profiles are used, for example, to draw conclusions regarding a person’s creditworthiness based on their residence location, which is then used to offer them certain interest rates for credit. A person’s actual creditworthiness is not considered; instead, the credit fault rate of his/her neighbourhood is assumed to accurately reflect his/her own creditworthiness. There is currently considerable debate over the extent to which “scoring” practices violate data and consumer protection laws [KaWe 05]. Because of the sheer quantity of data in pervasive computing that enables group profiling, this question becomes particularly controversial in scenarios involving scoring-based access such as automatically denying residents of districts with a high percentage of hooligans access to football stadiums.

7.4.3 Safety

Pervasive computing can increase the reliability of many applications, such as medical monitoring for seniors and patients at home, while driving a vehicle and in public administrative offices. The invisible ubiquity of smart objects will also mean, however, that the actions carried out in pervasive computing will go largely unnoticed and will not be controlled by users. Malfunctioning systems and technical disturbances will therefore often go unnoticed or will be recognised too late. In pervasive computing systems, a malfunction can lead to considerable property damage, physical injury and even death. It is therefore imperative that alternative solutions
able to assume key functions in a crashed system be in place.

7.4.4 First steps toward a privacy-compliant pervasive computing

Although the general requirements for protecting the private sphere in pervasive computing have been discussed in detail, it remains uncertain exactly how these requirements are to be implemented in system architectures. There are currently three initial responses:

In [BeHa 05] and [Crut 05], the metaphor of a digital bubble as a contextual filter is used to describe a technical solution to protecting the private sphere. Surrounding a person like a digital shield, this bubble would regulate interaction with other pervasive computing actors. The filter can vary; it can permit unhindered transfer or implement a total blockade. The challenge lies in accepting and transmitting information that the user has authorised while preventing unauthorised information from doing the same. To allow for the automatic (in pervasive computing terms) exchange of information that goes largely unnoticed, profiles and rules need to be defined that comply with a user’s needs and wishes while permitting anonymity and the creation of pseudonyms. The goal here is to strike a balance between interaction and a user’s private sphere.

The architecture of a Privacy Awareness System (pawS) for pervasive computing is presented in [Lang 05b]. Defining user preferences for handling their personal data makes up the very core of pawS. These preferences are compared automatically with the digitally-stored data protection rules of service providers. If the preferences and rules are in agreement, then the personal data are passed on to the service provider, who then is obliged to adhere to these rules. Similar approaches are discussed in [HoLa 04] and [YaKa 05].

The controllability of pervasive computing applications is crucial and inseparable from the issue of privacy protection. According to surveys and scenario evaluations conducted by the TAUCIS project, a German government-sponsored assessment of pervasive computing’s implications for society, large sectors of the population generally show positive attitudes toward technology and expect fundamental improvements in many areas of life. On the other hand, people also fear an increasing dependency on technical systems and attendant loss of control [Lütg 06]. This manifests itself in the fact that “soft” pervasive computing scenarios are evaluated more positively than “hard” scenarios. Soft scenarios involve systems that provide references and recommendations only, such as notification that an individual’s car needs to be taken in for official inspection. Hard scenarios involve systems acting

![Fig. 53: Digital bubbles as digital terrains with varying privacy requirements](image)
autonomously, such as the automatic engagement of a vehicle’s brakes when it goes over the speed limit. The study concludes by recommending that if a high degree of acceptance for pervasive computing is to be achieved, users should be granted the broadest possible look at and control over pervasive computing services. The study also notes a clear decline in the level of pervasive computing acceptance when individual access to pervasive computing services is based on general group profiles such as those that determine a person’s creditworthiness based on their residency.

It is still far too early for a final word on future security architectures in pervasive computing. And yet, it is abundantly clear that data security must be a central technological component of pervasive computing, if user acceptance is to be ensured. As with any information system, the data protection principles of data minimisation, transparency and consent must also apply in pervasive computing. The data security technologies in a pervasive computing of the future must be easy-to-use, understandable and free of discrimination. The user must have the freedom to choose at all times for him/herself – without fear of disadvantages – which data s/he wants to transfer to which service providers, and how these data are used. It is especially important that the user be able to switch off any of the pervasive computing services that interact with him at any time. Binding regulations and attendant means of monitoring are needed to assure the user that pervasive computing’s data protection mechanisms cannot be circumvented in technical or organisational terms.
8 Future Outlook

Pervasive computing will be able to sense our situations and anticipate our needs and proactively act in our best interests, much like a very good human friend or our parents.

Prof. Dr. Daniel Siewiorek, Carnegie Mellon University, United States

Today, pervasive computing is still mostly a vision of technology, much like the World Wide Web 10 years ago. Extensive development work will be necessary to realise nearly all of its characteristics, such as autarkic power supply, machine-machine communication, the human-machine interface and security technologies. Apart from RFID-based logistics and security systems, there are very few pervasive computing applications currently in existence. Yet the dissemination and use of the Internet and mobile telephones over the past decade suggests how quickly ICT can develop, affecting and even transforming large segments of society in the process. Based on the in-depth interviews and online survey conducted for this study, two initial theses on the future of pervasive computing can be formulated:

In the short run, pervasive computing is the continuation of the Internet by other means. The development of pervasive computing is typified by two characteristics that may appear contradictory at first glance. On the one hand, only a few pervasive computing applications (narrowly defined) exist at present. On the other hand, international experts expect such applications will be realised within the next one to five years. Most likely, these early smart objects will mostly offer integration of different functions – which will include, in particular, certain sensory capabilities – and data exchange via mobile broadband, enabling connection to the Internet. As a logical consequence, the first pervasive computing applications will probably draw heavily on what is already realised in the Internet in rudimentary form. Audiovisual and data communication will merge, existing media ruptures will be overcome, and the possibility of digital communication will become ubiquitous [Bott 04]. Pervasive computing offerings will be called up via a multitude of everyday electronic devices, while the services themselves will be provided by a central, Internet-based IT infrastructure. The close correspondence between web services and the aspirations of pervasive computing is also reflected in what are expected to be its early uses. Since mobility is a central characteristic in the early stage of pervasive computing, one can assume that enabling Internet connectivity from any device will be a main focus. Smart objects will thus, in a sense, represent a materialisation of available online services. In the coming years, pervasive computing will be typified not by the refrigerator or range automatically connecting to recipes, but by ubiquitous access to information and services available over the Internet.

In the long run, pervasive computing will noticeably change processes in the personal, economic and public realms. In the long term, as pervasive computing is integrated into everyday objects and they become networked, information and control systems that are presently centralised in industry, transport, the service industry and the public sector can be decentralised and expedited. In the personal realm, ubiquitous ICT will bring new functions to everyday objects and more opportunities to communicate anytime and anywhere. To gain a sense of both the potential and the limits of emergent pervasive computing, its central forerunner, the Internet, can serve as a model. With the dissemination of the Internet in society and the economy, a number of social and economic processes have indeed changed significantly or even fundamentally. In economic terms, though, one cannot speak of a purely Internet-based society and economy. Still, there are individual industries that are undergoing profound change and that find themselves in crisis due to digitalisation and the Internet. The music and film industries furnish the most vivid example, since their products, which are already available in digital form anyway (CD or DVD) can easily be copied to other digital media.

Based on experiences with the Internet and its constant development and expansion, as well as on the characteristics of pervasive computing, one can identify central fields that will shape pervasive computing in the future:

The often-implicit actions and the high degree of networking in pervasive computing make it hard to
explicitly perceive and control system activities. This makes it all the more important that the user can totally trust the services and content of pervasive computing. This trust involves:

- the non-repudiability and accurate content of services
- the security of information in pervasive computing and
- the careful treatment of personal data.

Implementation of these standards will need to rely equally on technological, organisational and regulatory instruments.

On the technological side, there is still a great need for research and development in many areas. A broad spectrum of challenges awaits industry, science and research support, especially in regard to autarkic power supply, the human-machine interface and security technologies. The formulation and implementation of technical standards will exert a decisive influence on the introduction and impact of pervasive computing. Open standards – like PC architecture in the 1980s and the Internet in the 1990s – seem particularly well-suited to separating the development of the infrastructure from that of the products based on it. This will make it possible to create a broad range of freely-combinable pervasive computing products that compete unreservedly with one another. Technology suppliers for the pervasive computing infrastructure, service providers, users’ associations and standards organisations are thus called upon to agree on appropriate open standards, in order to counter tendencies toward monopolisation.

Like the Internet, pervasive computing is not beyond the law. Users’ acceptance of a system will depend heavily on rules that will guarantee that they can have the necessary trust in its services and content. These include ensuring that business and legal actions are legally binding, defining liability for services and faulty content that cause damages, and protecting the privacy of data. Even though pervasive computing does not, in principle, create any new requirements beyond those of other distributed information and communication systems, its invisibility and ubiquity will generally require that existing rules be adapted. This is particularly clear regarding data protection. It remains to be seen whether the existing instruments for data protection will prove adequate over the long run in light of the complexity of information processing and networking in pervasive computing. Here, service providers must develop transparency mechanisms, for instance, so that the individual can foresee the long-term consequences of accepting or rejecting an exchange of information.

Due to its functional logic, pervasive computing cannot be confined to individual countries. Internationally uniform rules are thus an essential requirement for the widespread introduction of technology. At present, though, very disparate regulatory approaches stand in the way of this in such realms as consumer law, data protection, freedom of speech and the press, and copyright law. On top of this come highly varied approaches to how such rules should be implemented – for example, in the form of voluntary commitments, certificates or laws. Internationally uniform rules are urgently needed here, with effective mechanisms for verifying and enforcing compliance. Otherwise, certain pervasive computing services with specific access barriers may be offered or usable only in certain countries, while they are banned entirely in other countries, as is currently the case in China with restrictions on Internet access and search machines.

An essential question in establishing a pervasive computing infrastructure is how to ensure simple, cost-effective and unimpeded access to services. This is especially important when certain public and commercial services are offered solely – or at least preferentially – via pervasive computing systems. This could affect purchasing age-restricted products like alcohol and tobacco, for instance, or accessing health care services. Particularly in regard to public services, care must be taken that society is not split into participants and non-participants in pervasive computing, with noticeable disadvantages for non-participants.

Pervasive computing has the potential to dramatically change production and business processes. This can mean not only that processes will become increasingly decentralised and flexible, but also that
newly available information will increase market transparency. This would tend to favour small and flexible companies. On the other hand, large companies are better positioned to make the major investments initially required for pervasive computing and to set standards for cross-company pervasive computing infrastructures that benefit themselves most of all. Companies, their associations and economic policymakers are called upon to ensure that the opportunities of pervasive computing are equally open to all companies.

Considering that pervasive computing is in its infancy and the necessary technologies are at best partially available or not at all, it is impossible to foresee all of its social implications. However, the technological vision of pervasive computing is clearly recognisable in its contours, and its technical implementation and application within the next ten years seems generally possible; this will entail fundamental socio-economic challenges, as discussed above. Clearly, pervasive computing is a highly dynamic paradigm that harbours a tremendous potential. The challenge lies in following its development attentively, and shaping it actively to exploit its positive effects while avoiding its potential negative effects as much as possible.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL</td>
<td>Ambient Assisted Living</td>
</tr>
<tr>
<td>ABG</td>
<td>Automated and biometrical-based border control</td>
</tr>
<tr>
<td>ABS</td>
<td>Antilock brake system</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AIK</td>
<td>Attestation Identity Key</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
</tr>
<tr>
<td>BACnet</td>
<td>Data Communication Protocol for Building Automation and Control Networks</td>
</tr>
<tr>
<td>BAN</td>
<td>Body Area Network</td>
</tr>
<tr>
<td>BMGS</td>
<td>Bundesministerium für Gesundheit und Soziale Sicherung (Federal ministry of health and social security)</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik (Federal office for security in the information technology)</td>
</tr>
<tr>
<td>CORBA</td>
<td>Common Object Request Broker Architecture</td>
</tr>
<tr>
<td>CSCA</td>
<td>Country Signing Certification Authority</td>
</tr>
<tr>
<td>DAA</td>
<td>Direct Anonymous Attestation</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital European Cordless Telecommunications</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DFG</td>
<td>Deutsche Forschungsgemeinschaft (German Research Foundation)</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>DS</td>
<td>Document Signer</td>
</tr>
<tr>
<td>EAN</td>
<td>European Article Number</td>
</tr>
<tr>
<td>ECHONET</td>
<td>Energy Conservation and Homecare Network</td>
</tr>
<tr>
<td>EKG</td>
<td>Electrocardiography</td>
</tr>
<tr>
<td>EPR</td>
<td>Electronic Patient Record</td>
</tr>
<tr>
<td>EPC</td>
<td>Electronic Product Code</td>
</tr>
<tr>
<td>ESP</td>
<td>Electronic Stability Program</td>
</tr>
<tr>
<td>ETS</td>
<td>European Telecommunications Standard</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>GCC</td>
<td>Galileo Control Center</td>
</tr>
<tr>
<td>GLONASS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GSS</td>
<td>Galileo Sensor Station</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ITRS</td>
<td>International Technology Roadmap for Semiconductors</td>
</tr>
<tr>
<td>JINI</td>
<td>Java Intelligent Network Infrastructure</td>
</tr>
<tr>
<td>JXTA</td>
<td>Juxtapose</td>
</tr>
<tr>
<td>LON</td>
<td>Local Operating Network</td>
</tr>
<tr>
<td>MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>NOW</td>
<td>Network on Wheels</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OMG</td>
<td>Object Management Group</td>
</tr>
<tr>
<td>OWL</td>
<td>Web Ontology Language</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PANAMA</td>
<td>Personal Area Networking for Advanced Medical Applications</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PHS</td>
<td>Personal Handyphone System</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PReVENT</td>
<td>Preventive Safety</td>
</tr>
<tr>
<td>PvC</td>
<td>Pervasive Computing</td>
</tr>
<tr>
<td>RDF</td>
<td>Resource Description Framework</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RSA</td>
<td>Asymmetric encryption, named after its developers Rivest, Shamir und Adleman</td>
</tr>
<tr>
<td>SEMI</td>
<td>Semiconductor Equipment and Materials International</td>
</tr>
<tr>
<td>SIVAM</td>
<td>Sistema de Vigilância da Amazônia</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-orientated architectures</td>
</tr>
<tr>
<td>SOFTNET</td>
<td>Software Engineering for Soft Networking</td>
</tr>
<tr>
<td>SRK</td>
<td>Storage Root Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TAUCIS</td>
<td>Assessment of technological implications of ubiquitous computing and informational self-determination</td>
</tr>
<tr>
<td>TCG</td>
<td>Trusted Computing Group</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TRON</td>
<td>The Real-time Operating System Nucleus</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party</td>
</tr>
<tr>
<td>UID</td>
<td>Universal identification</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UPC</td>
<td>Universal Product Code</td>
</tr>
<tr>
<td>UPnP</td>
<td>Universal Plug-and-Play</td>
</tr>
<tr>
<td>VITA II</td>
<td>Vision Technology Application</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VSC</td>
<td>Vehicle Safety Communication</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
Index

A
Accumulators 14, 37, 39
AES 45
AIK 62, 63
Ambient assisted living 57
Anonymity 17, 44, 45, 64, 65, 66, 71, 77, 83, 84
Artificial intelligence 13, 54
Asymmetric encryption 45
Augmented reality 48
Authenticity 17, 24, 44, 45, 66, 69, 70, 71, 83
Autonomy 12, 14, 22, 23, 32, 54, 82

B
Ball grid array 3
Basic access control 69, 70
Batteries 14, 21, 37, 38, 39
Biometrics 28, 46

C
Comfort 14, 15, 16, 25, 33, 50, 51, 73, 74, 80
Communication 5, 9, 10, 11, 17, 21, 23, 26, 28, 29, 30, 32, 34, 36, 40, 41, 42, 44, 45, 46, 47, 48, 58, 60, 61, 62, 64, 66, 67, 68, 69, 70, 71, 73, 75, 76, 77, 78, 79, 80, 81, 82, 83, 86, 87
Communication technology 5, 9, 32, 40, 42, 76
Confidentiality 44, 45, 64, 65, 69, 71, 76
Context-awareness 20, 55, 82
Cost savings 14, 15, 25, 31, 50, 51
Country signing certification authority 68, 74

D
Data protection 15, 16, 17, 18, 44, 46, 54, 71, 76, 80, 81, 82, 84, 85, 87
Digital bubble 54, 84
Digital rights management 65
Document signer 68, 69
Driver assistance systems 10, 25, 26, 49

E
E-commerce 21, 31
EAN 25
ECHONET 30
EKG 29
Elliptic encryption techniques 45
Embeddedness 34, 58
Energy autarky 14, 22, 32, 34, 59
Energy efficiency 14, 15, 50, 51, 53, 80
Energy harvesting 14, 38, 39
EPC 25
External security 5, 16, 23, 26, 27, 55

F
Flip chip 35
Fuel cells 14, 37, 39

G
GLONASS 43
GPRS 32, 41
GPS 42, 43, 44, 75
GSM 32, 41, 42
GSS 43

H
Human-machine interface 5, 14, 26, 32, 33, 35, 48, 49, 52, 86, 87

I
ICAO 5, 60, 67, 68, 69, 70
Identification systems 5, 21, 23, 24, 27, 29, 43, 60, 72
Identity management 14, 45
Implants 22, 33, 48, 49, 84
Indoor localisation systems 42
Inner security 21, 23, 26, 27, 29
Integrity 26, 43, 44, 64, 65, 69, 70, 71, 76, 77, 83
Inter-connectivity 80, 83
IPv6 41, 42
ITRS 35

J
JINI 47
JXTA 47

K
Knowledge-based systems 16, 20, 47, 48, 55

L
Labour efficiency 53, 54
Localisation technology 5, 32, 42, 43, 44
Logistics 5, 14, 16, 21, 23, 24, 25, 30, 45, 50, 51, 54, 55, 56, 62, 86

M
Material efficiency 53
Medical technology 5, 15, 22, 30, 31, 33, 35, 45, 51, 57
Military 14, 15, 16, 21, 23, 26, 27, 42, 43, 44, 50, 53, 55
Miniaturisation 10, 13, 23, 24, 35, 36, 81
Mobile IP 41, 42
Mobility 12, 14, 22, 23, 30, 32, 34, 41, 58, 86
Monitoring 21, 22, 24, 26, 27, 30, 31, 32, 33, 40, 56, 79, 83, 85
Motor traffic 5, 14, 21, 25, 50, 51

Non-repudiability 44, 45, 64, 65, 71, 87
Object identification 5, 60, 61, 62, 63, 65, 67

PIN 44, 67, 73, 91
Polymer electronics 36
Power supply 5, 14, 32, 34, 35, 36, 37, 39, 58, 86, 87
Privacy 5, 6, 11, 12, 15, 16, 17, 18, 26, 27, 29, 30, 31, 33, 44, 46, 52, 53, 54, 59, 60, 63, 64, 65, 70, 71, 79, 81, 82, 84, 87
Production 5, 13, 14, 15, 16, 17, 18, 21, 23, 24, 25, 30, 34, 35, 36, 37, 39, 41, 50, 51, 53, 54, 55, 56, 87
Pseudonym 17
Public key infrastructure 45, 68
Public safety 27, 53
PvC-1 12, 13, 23, 48, 52, 58, 59
PvC-2 13, 23, 48, 52, 58, 59

RADAR 26, 44
RDF 49
Recycling 13, 16, 53, 55
Reliability 15, 18, 25, 31, 36, 37, 39, 43, 45, 52, 79, 83
RFID 9, 23, 24, 25, 27, 28, 31, 32, 36, 43, 44, 52, 62, 68, 69, 70, 84, 86
Routing 12, 76, 77, 78
RSA 45, 62

Safety 5, 6, 12, 14, 16, 17, 18, 26, 27, 28, 29, 31, 33, 34, 44, 45, 46, 49, 50, 53, 56, 57, 59, 60, 63, 65, 70, 72, 74, 75, 76, 79, 80, 83
Security 5, 6, 9, 11, 12, 14, 15, 16, 17, 21, 23, 26, 27, 28, 29, 31, 32, 33, 35, 44, 45, 46, 50, 51, 52, 53, 54, 55, 59, 60, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 76, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87
Security technology 14, 32, 35, 46
Semantic web 49
Sensor networks 23, 27, 36, 40
Sensor technology 5, 32, 34, 39, 40
Smart card 27, 28, 45, 62, 67, 70, 71, 73
Smart carpet 29, 30, 43
Smart home 14, 16, 21, 23, 29, 30, 33, 50, 51, 53, 57
SMS 31
Symmetric encryption 45

System-on-chip 36, 39

TCG 45, 62, 63
Telematics 6, 21, 26, 27, 28, 60, 74, 75, 76, 77, 79, 80
Tracking 21, 24, 43, 70, 71
Trust management 14, 45
Trusted platform module 5, 45, 60, 62
Trusted third party 63

Ubiquity 10, 11, 18, 83, 87
UMTS 41, 42, 75
Universal identification 60, 66, 73
UPC 25
UPnP 47

Virtual reality 11, 48
Voice command 48
VoIP 41, 91

Weiser, Mark 10, 21
WiMAX 41, 75
Wireless communication 32, 40, 41, 42, 78
WLAN 31, 41, 44, 75, 78
Literature

[ABDF 05]

[Alan oJ]
ALANCO TECHNOLOGIES, Website to the product TSI PRISM

[ÄrZe 04]

[ASIT oJ]

[Axma 04]
AXMANN, P., Einführung in alkalische Systeme: Konstruktionsprinzipien, Materialien, Strom-Spannungscharakteristik, Eigenschaften, Lebensdauer. OTTI-Profilforum Wiederaufladbare Batterien – Schwerpunkt: Stationäre Systeme, 04/05/2004, Ulm

[Back 06]

[BARC 04]

[BaWü 05]

[BCC 04]

[BeHa oJ]

[BeSa 03]

[BGS 04]

[BHR 01]

[BMGS 05]

[BMI 05]
BUNDESMINISTERIUM DES INNEREN BMI, Press release to the electronic passport, 08/07/2005 (http://www.bmi.bund.de/cln_012/nn_662928/Internet/Co

[BM] oJ
BUNDESMINISTERIUM DER JUSTIZ, JURIS GMBH, Website „Gesetze im Internet“
(http://bundesrecht.juris.de/index.html, retrieved on: 24/03/2006)

[BMWA 05]
BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ARBEIT, BUNDESMINISTERIUM DES INNEREN, BUNDESMINISTERIUM FÜR GESUNDHEIT UND SOZIALE SICHERUNG und BUNDESMINISTERIUM DER FINANZEN, Bundeskabinett beschließt gemeinsame eCard-Strategie. In: Gemeinsame Pressemitteilung der beteiligten Ressorts vom 09/03/2005

[Bohn 03]

[Bott 04]

[Bove 04]
BOVENSCHULTE, M., Kraftzwerge schützen Soldaten und Motorradfahrer. Frankfurter Rundschau of 04/08/2004

[BrSe 03]

[BRSS 02]

[BSI 02]
BUNDESMAT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK, Integrierte Gebäudesysteme: Technologien, Sicherheit, Märkte, SecuMedia, Ingelheim 2002

[BSI 03]

[BSI 04a]
BUNDESMAT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK, Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddocumenten – BioP-I, Öffentlicher Abschlussbericht, 07/04/2004

[BSI 04b]
BUNDESMAT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK, Risiken und Chancen des Einsatzes von RFID-Systemen, SecuMedia, Ingelheim 2004

[BSI 05]
BUNDESMAT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK, Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen BioP-II, Öffentlicher Abschlussbericht, 23/08/2005

[BSI oJ]
BUNDESMAT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK, Website of the BSI for the ePass

[Buse 02]

[Cosk 99]

[Crut 05]
(http://www.troubador.co.uk/ices/, retrieved on: 24/03/2006)


[GMRL 04] GRADE, M., MEIER, K., RECH, B. und LÜBKE, A., Physikal IEEE 802.11_Measurements in Automotive Environment, draft, Volkswagen AG, Wolfsburg


[Hilt 03]

[HoLa 04]

[Horn 05]

[Hu 03]

[HuPe 04]

[IATA 04]
IATA: Electronic Ticketing, 2004

[ICAO 04a]

[ICAO 04b]
INTERNATIONAL CIVIL AVIATION ORGANIZATION, PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, 01/10/2004

[InOs 04]INOUE, H., OSAWA, S. et al., Dedicated Short-Range Communications (DSRC) for AHS Services, Proceedings 2004 IEEE Intelligent Vehicles Symposium, June 14-17, 2004, Parma, Italy, pp-369-374.

[IkGo 04]

[ITIV 05]
INSTITUT FÜR TECHNIK DER INFORMATIONSVERARBEITUNG DER UNIVERSITÄT KARLSRUHE, Personal Health Monitor mit innovativer mikrosystemtechnischer Sensork, 2005

[ITRS 03]

[ITS 03]

[IVHW 03]
DEUFRAKO, Kurze Projektbeschreibung zu Inter-Vehicle Hazard Warning (IVHW), In: 1. Die DEUFRAKO Themengebiete, 17/11/2003

[JoJö 04]

[Juels 05]

[KaWe 05]
KAMP, M. und WEICHERT, T., Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher. Interner Forschungsbericht, Unabhängiges
Landeszentrum für Datenschutz Schleswig-Holstein, Kiel 2005

KlKi 06]
KLAUS, P. und KILLE, Chr., Die Top 100 der Logistik, Deutscher Verkehrs-Verlag, Hamburg 2006

[KoSo 05]

[Lang 05a]

[Lang 05b]

[LübK 05]

[Lütg 06]
LÜTGE, G., Was darf Technik?, Die Zeit, 9.3.2006, Nr. 11
(http://www.zeit.de/2006/11/RFID-Umfrage, retrieved on 29/03/2006)

[Meis 04]
MEISTER, G., Die Rolle der Smart Card in der eSociety. Relevanz für das Design von Chipkartenapplikationen, 14. SIT-SmartCard Workshop, Darmstadt, 03-04/02/2004

[MiMa 02]
MICH, Y. und MASUDA, S., Mitsubishi’s ASV-2 Passenger Car Obtained Japan’s Land, Infrastructure and Transport

[MiMo 02]

[NOW 05]
DaimlerChrysler AG, Network on Wheels; Projekt-Homepage, 2005
(http://www.network-on-wheels.de/, retrieved on: 24/03/2006)

[NOW 06]
TU München, Network on Wheels
(http://www11.in.tum.de/forschung/projekte/now/, retrieved on: 24/03/2006)

[Odri 05]

[Ortl 06]
ORTLAND, E., Wer kontrolliert die Datenströme? Forum Humanwissenschaften der Frankfurter Rundschau vom 14/03/2006

[Poly 06]
POLYAPPLY, Website of the projekt „PolyApply“
(http://www.polyapply.org, retrieved on 29/03/2006)

[PSSS 05]
PAULUS, I., SCHULZE, M., SPECKS, W. und STEINBERG, K.-E., Fahrzeug-Fahrzeug und Fahrzeug Infrastruktur Kommunikation in Europa, Technischer Kongress 2005

[Prin 05]
PRINCE, P., United States Sets Date for E-Passports. The RFID Journal, 25/10/2005

[RaEU 04] RAT DER EUROPÄISCHEN UNION, Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Nor-
men für Sicherheitsmerkmale und biometrische Daten in
von den Mitgliedstaaten ausgestellten Pässen und Reise-
dokumenten. In: Amtsblatt der Europäischen Union,
29/12/2004, L 385/1-6

[Reck 06] RECKMANN, J., “Intelligente” Autos sollen Leben retten;
Frankfurter Rundschau of 23/02/2006

[Reich 05] REICHEL, H. ROSSNAGEL, A. und MÜLLER, G., Digitaler
Personalausweis – Eine Machbarkeitsstudie, Deutscher
Universitäts-Verlag, Wiesbaden 2005

[Sche 88] SCHEELE, B. und GROEBEN, N., Dialog-Konsens-Methoden
zur Rekonstruktion subjektiver Theorien. Tübingen, p. 34
ff., 1988

[Schily 05] SCHILY, O., Speech at the acatech-symposium „Computer
in der Alltagswelt - Chancen für Deutschland?” on
28/06/2005 in Berlin
(http://www.bmi.bund.de/cnr_012/mn_122688/Internet/Co
ntent/Nachrichten/Archiv/Reden/2005/06/Schily__aca-
tech__Symposium.html, retrieved on: 26/04/2006)

[ShLe 05] SHIN, B., und LEE, H.G., Ubiquitous Computing?Driven
Business Models: A Case of SK Telecom’s Financial Ser-

[SOFT 02] SOFTNET, Description of projects, 20/07/2002
(http://www.lorsoft.de/indexII.html, retrieved on:
29/03/2006)

[SpRe 05] SPECKS, W. und RECH, B., Car-to-X Communication, Elek-
tronik im Kraftfahrzeug, Baden-Baden, 06-07/10/2005

[Staj 02] STAJANO, F., Security for ubiquitous Computing, John
Wiley & Sons, 2002

[StAn 99] STAJANO, F. und ANDERSON, R., The Resurrecting Duck-
lings: Security Issues in Ad-Hoc Wireless Networks. In: Pro-
ceedings of 3rd AT&T Software Symposium, Middletown,
New Jersey, USA, 1999

[Stru 06] STRUIF, B., Fraunhofer SIT, proceedings for the 16. SIT-
Smartcard Workshop, 08/02/2006, Darmstadt

[StSc 02] STRASSNER, M. und SCHOCH, Th., Today’s Impact of Ubi-
quitous Computing on Business Processes, Pervasive 2002
– International Conference on Pervasive Computing,
Zürich, 26-28/08/2002

[SZM 05] SCHMID, B. F., ZIMMERMANN, H.-D., MIERZEIEWSKA, I.B.,

[TBH 06] TIWARI, R., BUSE, St. und HERSTATT, C., Customer on the
Move: Strategic Implications of Mobile Banking for Banks
for Technology and Innovation Management, Hamburg
University of Technology, Feb. 2006

[TCG 04] TRUSTED COMPUTING GROUP, TCG Specification Archi-
tecture Overview, Specification, Revision 1.2, 28/04/2004

[TCG 0Ja] TRUSTED COMPUTING GROUP, Homepage
(https://www.trustedcomputinggroup.org/, retrieved on:
24/03/2006)

[TCG 0Jb] TRUSTED COMPUTING GROUP, TPM Work Group
(https://www.trustedcomputinggroup.org/groups/tpm/,
retrieved on: 24/03/2006)

[TrSc 01] TRÄNKLER, H.-R. und SCHNEIDER, F., Das intelligente
Haus, Richard Pflaum Verlag, München, 2001

[UIP 05] SWEDISH INSTITUTE OF COMPUTER SCIENCE, Website to the uIP Embedded TCP/IP Stack, 07/02/2005 (http://www.sics.se/~adam/uiip/, retrieved on: 29/03/2006)


[Veri 04] VERICHIP CORPORATION, VeriChip Corporation Confirms that the Attorney General of Mexico and some of his staff have been ‘Chipped’. Press release of the VerChip Corporation of 14/07/2004


Pervasive Computing

Trends and Impacts

The communication and information technology sector is continually reinventing itself. While the PC used to meet everyone’s objectives during the 90s, the first decade of the new millennium is witnessing a new focus on mobile devices, enabling access to communication and data networks, irrelevant of location or time. Regarding the future for information and communication technologies, IT experts predict them to become likewise ubiquitous and invisible: In Pervasive Computing, microcomputers will be integrated in common devices, making them smart objects with numerous services for their users. During glazed frost on roads, the driver assistance system throttles the car’s celerity and warns the following cars. If a storm is coming, the window in the smart home closes by itself. Passengers in the subway keep their monthly ticket in the pocket, are automatically identified and the travelling fare is written off from their account.

How realistic are such visions? What consequence has Pervasive Computing for society and economy? What is the status regarding the security of such services, which are barely noticed by the users?

The presented study provides, via an international expert-questioning, an overview on the technological trends and possible areas of application for Pervasive Computing. It additionally gives a view on the socio-economic drivers and consequences of this technological vision. The study also discusses security scenarios and drafts requirements for the security and data protection in Pervasive Computing.

The study has been prepared on behalf and in collaboration with the German Federal Office for Information Security (BSI) by VDI/VDE-IT Innovation + Technik GmbH, Berlin; Fraunhofer Institute for Secure Information Technology, Darmstadt; and Sun Microsystems GmbH, Kirchheim-Heimstetten.