Electronic-Onboard-Ticketing: Software Challenges of an State-of-the-Art M-Commerce Application

Dominik Haneberg, Kurt Stenzel, Wolfgang Reif

Lehrstuhl für Softwaretechnik und Programmiersprachen
Fakultät für Angewandte Informatik
Universität Augsburg
86135 Augsburg
haneberg@informatik.uni-augsburg.de
stenzel@informatik.uni-augsburg.de
reif@informatik.uni-augsburg.de

Abstract: In this paper we present E-ON (Electronic-Onboard-Ticketing). E-ON is an innovative m-commerce application using state-of-the-art technology. E-ON is a location-based service that enables a customer to purchase railway tickets directly on the train. A Personal Digital Assistant (PDA) implements the user interface. The connection between the customer's PDA and the service is established using Bluetooth, a new short-range communication technique. All parts of the application are programmed in Java.

1 Introduction

Looking back at the e-commerce experience one could be quite disappointed concerning the prospects of e-commerce. There is not much left of the e-commerce hype. Different problems inhibit the success of e-commerce on the market:

- Inefficiencies in the utilisation of the potential of the Internet to design individual, intuitively-usable and therefore profitable solutions for customers and inefficiencies in the composition of inter- and intraorganisational value chains [Ba02].
- Inexperience of the management [Br02].
- Security concerns. Missing software engineering methods specific for e-/m-commerce applications.
- No individualization of the services, just commodity products available.
- Bad usability of services and mobile Internet access.
- Absent technical possibilities.

Given these problems and the earlier set-backs the question is: “Why again?”

The answer is simple: The problems that lead to the collapse of the e-commerce hype can now be overcome, given the knowledge gained from the failure of many e-commerce services and the improved techniques, especially for mobile services. The main advantages that the next generation of services profits from are:

- Mobile Digital Assistants (MDA) with short range communication and a better display.
- Context information for location-based services.
- More knowledge in service design and an experienced management.
- New security techniques.

The possibility to localize the customer and the short-range infrastructure free networks (e.g. Bluetooth) allow for new individualized, location-based and context-aware services with a high utility, the display of MDAs enables better usable user-interfaces than mobile phones. State-of-the-art software technology for m-commerce applications helps to rule out security deficiencies. For e- and m-commerce applications certain design principles are now available that lead to better and more reliable applications.

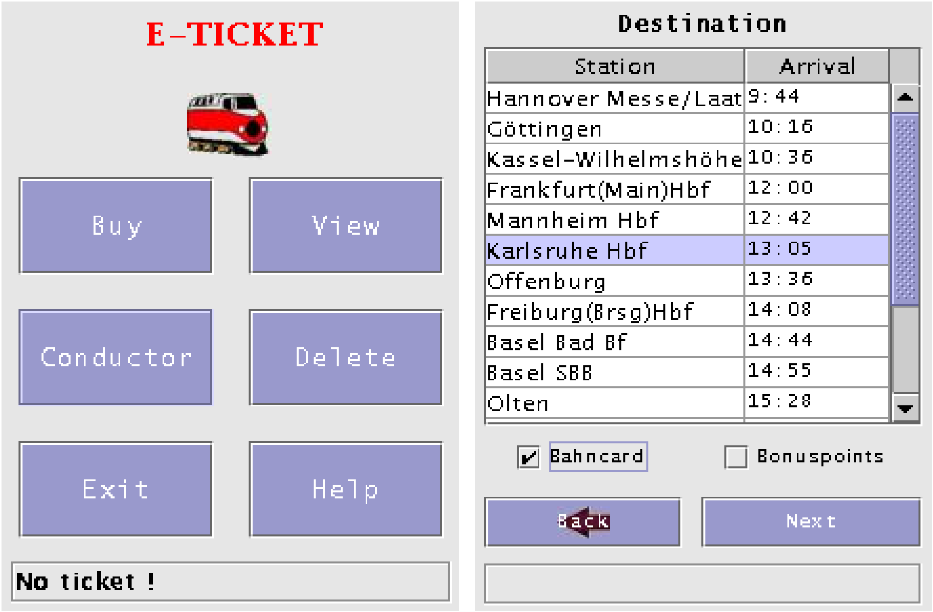
In this paper we describe an interesting location-based service as well as the technological and the software-engineering tasks arising from such an application. Electronic-Onboard-Ticketing is a service to electronically sell railway tickets directly on the train. We start with a description of the service (Sect. 2), Sect. 3 looks into the details hidden behind the first impression. In Sect. 4 the technology used is described, Sect. 5 deals with security issues and Sect. 6 gives details of the implementation. Section 7 provides a summary.

2 The E-ON Application

“Electronic-Onboard-Ticketing” is a very simple and convenient method to buy a ticket for a train. A traveller boards a train without a ticket. (Of course, this must be allowed. In Germany, it is possible for long distance trains.) This is attractive for persons that know the connections, but cannot or do not want to decide on the train in advance. After taking a seat the traveller starts the ETicket application on his PDA (see the left side of Fig. 1). The application program must be loaded onto the PDA in advance (for security and compatibility reasons).

The PDA opens a radio connection using Bluetooth to a server located in the train. The server sends back all further stations for the train, and the traveller selects his destination and other options, e.g. the tariff (see the right side of Fig. 1). Since Bluetooth is location-based the server knows whether the traveller is sitting in the first or second class. So this information does not need to be provided explicitly.

The selection is sent to the server. The server computes the price and issues the electronic ticket to the PDA (on the left of Fig. 2). Finally, the traveller pays by transmitting credit card data to the server (or by using another e-payment system), and obtains a receipt. The whole process of buying a ticket is extremely simple and can be done with three clicks. It should be noted also that the service itself does not require any personal data of the traveller or a previous registration. The anonymity depends completely on the payment method.



No ticket !

Station	Arrival
Hannover Messe/Laat	9:44
Göttingen	10:16
Kassel-Wilhelmshöhe	10:36
Frankfurt(Main)Hbf	12:00
Mannheim Hbf	12:42
Karlsruhe Hbf	13:05
Offenburg	13:36
Freiburg(Brsg)Hbf	14:08
Basel Bad Bf	14:44
Basel SBB	14:55
Olten	15:28

☑ Bahncard □ Bonuspoints

Figure 1: The first two steps to obtain a ticket

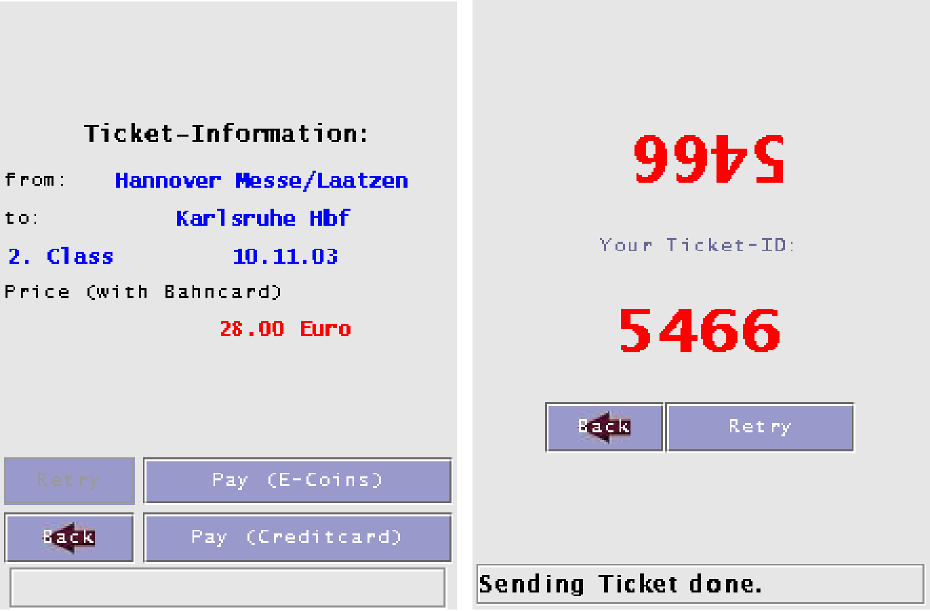
Ticket inspection is even simpler. When asked to present a ticket the traveller pushes one button on the PDA. This transmits the ticket to the conductors handheld. If more than one ticket is inspected at the same time, e.g. in a compartment, the traveller shows the PDAs screen with a four-digit number to the conductor (on the right in Fig. 2). The conductor inspects the ticket as he would inspect a paper ticket and sends the check information back. It should be noted that inspection of an electronic ticket can be done significantly faster than a paper ticket because the computer can perform several checks automatically and highlight this information so that the conductor sees at a glance if everything is in order.

This service has several advantages over other possible scenarios to obtain railroad tickets.

- It is very easy to select the ticket information (destination etc.).

- There are no running costs, neither for the railroad company nor the traveller, because Bluetooth connections are free of charge.
- There are no privacy concerns for the traveller – he has complete control when and what information is transmitted. The service itself is completely anonymous.
- The service is secure for both parties.
- The service can easily be augmented (delays, connections, finding a free seat).
- The service is practical with current technology (cf. a scenario where boarding and leaving the train is registered "automatically").
- Ticket inspection is more convenient and faster than for paper tickets because of the checks done by the computer.

In this paper we focus on the software-engineering aspects of the application. It is not our goal to conduct a thorough economical analysis of the service. Furthermore, due to space restrictions it is not possible to discuss all details.



Ticket-Information:

from: Hannover Messe/Laatzen

to: Karlsruhe Hbf

2. Class 10.11.03

Price (with Bahncard)

28.00 Euro

5466

Your Ticket-ID:

5466

Sending Ticket done.

Figure 2: Ticket Payment and presentation to conductor

3 Technological Challenges

That part of the service that runs on the travellers PDA seems very simple. However, it poses a number of software engineering challenges because different antagonistic requirements have to be met. These challenges are not unique to the E-ON service, but arise in this or other form in every m-commerce application. The requirements and challenges that must be met are:

- The application must be easy to use for the customer. Furthermore, the customer should always be aware what he and the application is doing, so that he never does anything inadvertently (e.g. exposing credit card data, buying two tickets if only one was wanted). This awareness must be achieved without stuffing the customer with incomprehensible technical information.
  This is a challenge for GUI design, especially for a small display with few input possibilities.
- Radio transmission is inherently unreliable. A transmission may be blocked by physical means or garbled by interference. For example, Bluetooth and WLAN use the same frequencies, and experience shows that WLAN may be seriously hampered by Bluetooth. A transmission may also fail if the range of the receiver is left. Since Bluetooth has a range of maximum 10 meters, this will happen if a traveller moves through the train.
  This means that the application must be able to resend messages, inquire the state of a transaction from the server, and restart aborted transactions. This has consequences for GUI design and security.
  For example: If no answer was received after sending payment information – did the message fail to reach the server, or was the answer lost? Automatically trying to re-establish a connection and re-sending the message violates the requirement “awareness of what the application is doing” (and the user will notice this because of timing issues and time delays). Other approaches may be inconvenient, incomprehensible or suspect to the user (e.g. to request him to push the “pay” button again), or insecure.
- The service must be secure against third parties and against fraud between the service provider and the customer. Everybody with a suitable receiver can eavesdrop on a radio transmission. Encryption is important but not the only answer. Status inquiries (see topic 2.) may reveal information. A replay of recorded messages may lead to a situation where an attacker obtains a ticket that is charged to another customer. The railroad company wants to detect forged tickets. The customer wants to be sure that he receives the goods for his money, etc.

These requirements are antagonistic: Improving reliability may reduce security, improved security may reduce easiness of use, and vice versa. To meet these challenges a software engineering methodology must be employed that is specifically tailored to m-commerce applications.

4 Technical Details

The application was designed to be usable with small portable devices that in the near future many people will have. We decided to use a Personal Digital Assistant as device for the customer. The larger graphical display of a PDA is beneficial because it is easier to design a good user interface, compared to e.g. a mobile phone. Because the service was planned to make use of the possibility to localize the customer to automatically issue a ticket for the correct class, a short-range communication technique was favored in order to get a precise localization.

For the communication, Bluetooth [Bl] was selected. It offers some advantages compared to other possible communication standards, but of course it is possible to realize a similar service with the other techniques, provided that some adjustments to the service are made.

- Infrared communication has a very short range and therefore many receivers would be necessary in a wagon. In the Bluetooth case only a few receivers per wagon are enough. Additionally infrared works only if the communicating devices are in sightline of each other. Therefore usage is inconvenient.
- WLAN is used for IP-based networks and requires more administration when used, compared to the simple ad-hoc networks that can be built with Bluetooth devices.
- Using mobile phone-based communication, e.g. GPRS or UMTS, has two disadvantages. Firstly, every transmission costs money while the Bluetooth link is free of charge and secondly, a precise localization of the customer is not possible with mobile phones. The accuracy of the localization of mobile phones is not sufficient because the service needs to know in which wagon of the train the customer is in order to produce a ticket for the appropriate class.
- Bluetooth includes protocols to search available services in the surrounding and request the parameters needed to communicate with and use the service.

Two factors influence the number of receivers necessary in each wagon. Firstly, the range of the Bluetooth devices in PDAs is up to ten meters and secondly, only eight clients can simultaneously connect to one receiver. The range of the radio connection can be shortened further by obstacles, e.g. compartment walls, and resulting radio shadows. Both limits suggest that one receiver per wagon will not suffice but about three should be enough. As the Bluetooth devices are cheap (manufacturers mention five USD per receiver [Sy02]), this is not a problem.

All in all the equipment necessary in a train is not excessive. E-ON needs a small computer per train to issue and store tickets, approximately three Bluetooth receivers per wagon, a network connecting the receivers to the server and a portable and Bluetooth-capable device for each conductor, used to check the electronic tickets. To provide the service each train has its own computer that is supplied with the correct data for the train. The service can then be provided from the train server alone, communication with systems outside the train is not necessary while the train is on its way.

An important design decision was that the server in the train does not only issue new tickets to customers but is also responsible for their storage and it also takes part in checking the tickets. This is due to security demands and described further in Sect. 5. The main consequence is that the customer's PDA and the device of the conductor do not communicate directly. When requested to present his ticket, the customer activates the appropriate function of E-ON. The PDA then transmits an unique and secret identification of the customer's ticket to the server. The server looks for the corresponding ticket and checks that it was not presented earlier by someone else. The conductor then loads the presented ticket from the server, checks the data and sends the obliterated ticket back to the server.

As described in Sect. 5 cryptography is used to establish the security of the application. We use up-to-date cryptographic primitives all considered reliable.

- For the exchange of session keys we use elliptic curve Diffie-Hellman key agreement.
- For symmetric encryption of data we use AES [Na01].
- For digital signatures DSA based on elliptic curves [Na00] is used.

5 Security Aspects

The chance of a m-commerce application like E-ON to be adopted in practice is determined to a great extend by the risks for the involved parties. Therefore security is an important issue in designing such a service. Naturally the service provider and the customer have different and probably antagonistic interests. In the E-ON application the railway company as service provider wants to be sure that e.g.:

- a ticket cannot be “upgraded” in a way that it is valid for a longer trip,
- a ticket is used only once,
- only tickets that are paid are accepted by the conductor,…

These security demands reflect the service provider's vital interest not to be cheated. On the other hand we have the security claims by the customer, e.g.:

- The anonymity of the customer is assured.
- If the customer pays, he receives a ticket that is accepted by the conductor.
- The ticket bought by a customer cannot be stolen by someone else.

As example, we will briefly describe how wrong application designs lead to the unattainability of two of the above demands.

- Assume the ticket is stored on the customer's PDA combined with a digital signature to verify its authenticity. When requested to present his ticket, the customer transmits the ticket and the signature to the conductor's device which checks the signature and displays the ticket data. The conductor verifies them and obliterates the ticket. The obliteration is transmitted to the customer's PDA. In this scenario it is not possible for the railway company to be sure that a ticket is not used more than once. A customer who bought a ticket can transmit a copy of the ticket and the digital signature to an accomplice in another part of the train in which a different conductor is responsible. The two conductors have no way to know that they both check and accept the same ticket.

- Now we describe attacks that realize a breach of the customer's security demand that his ticket cannot be stolen. Assume the ticket, including an unique identification number is sent unencrypted to the customer. When asked to present his ticket, the customer's PDA transmits the ticket identification to the server and the server sends the appropriate ticket to the conductor. The problem is that an attacker could have eavesdropped on the ticket purchase and present the stolen ticket identification earlier than the real owner of the ticket. The real owner could not present a valid ticket and would be considered as a fraudster. By encrypting the communication it can be averted that the attacker steals a ticket and uses it himself. But the security demand of the customer is still not guaranteed completely. Assume the train crew changes and the new conductor must check the tickets again. The attacker could have recorded the presentation of the ticket at the first time the customer sent the ticket identification to the server and reuse this recorded message at the second ticket check. He cannot read the contained ticket identification but he can resend the complete encrypted message. Yet again the real owner of the ticket would be considered a fraudster because he tries to present a ticket that was already presented to the new conductor. Note that the attacker does not achieve a personal benefit because for the first ticket check he must have his own valid ticket. But it is important to consider attackers who only want to cause damage (cf. virus authors in the Internet). The second described attack can be overcome by adding a counter to the ticket presentation message that must be incremented each time the ticket is presented. As the attacker cannot decrypt the data from a ticket presentation, he cannot modify the included counter and all messages he records are out-of-date for the next ticket check.

In the case of E-ON the design is affected by technical conditions: the usage of Bluetooth for communication and the fact that PDAs are not tamper-proof. The impacts are discussed in the following.

Although no attacks with manageable complexity on the Bluetooth link encryption are known at the moment, there are some indications that an application should not rely on the security mechanisms embedded in Bluetooth alone [XB01, JW01]. Additionally the usage of security realized by the implementation allows for an easy change of the networking technique if required. Therefore the communication protocols used to buy or obliterate a ticket make use of cryptographic functions to ensure the desired security properties.

PDAs are not tamper-proof devices. A tamper-proof device ensures that unauthorized access, modification or copying of stored data is not possible. As a PDA does not satisfy this property it is possible for the owner of a PDA to copy his ticket, including its digital signature, and transmit both to another person. Therefore the tickets must be stored on a server which is under the control of the railway company. It can be seen from this case that security concerns and technical abilities of the used devices directly influence the application design and the possible approaches. In the case of a tamper-proof device the application could be designed differently. A ticket could be stored on the customers device and the obliteration of tickets could be done offline, i.e. without communication to the server that issued the ticket.

Most of the security demands require cryptography to be used. Adequate cryptographic protocols guarantee the non-disclosure of confidential data, they ensure that a ticket cannot be stolen and so on. The problem is that cryptographic protocols are hard to design and error-prone [AN95]. A good solution to overcome this problem is to formally analyze the cryptographic protocols. For E-ON we used a development method originally designed for smartcard-based applications [HRS02]. Security protocols are modeled using UML [RJB98, OMG03] activity-diagrams so that a continuous design method can be used (assuming the software architecture is also modeled using UML).

6 Implementation

The application was designed using standard UML, as customary in current software engineering. However, after the first implementation was finished, a lot of testing was necessary to cope with the unreliable radio connection.

The complete application, consisting of the customer and the conductor clients and the ticket issuing server, is written in Java [Jo00]. The prototype ran under Linux, using an Java-API provided by the University of Rostock [SH] to access the Bluetooth devices. The customer and the conductor client consist of approximately 11000 lines of code. The server is made up of about 10000 lines of Java[1]. This is only the application logic and the user interface, the code for the Bluetooth API and the implementation of the cryptographic functions are not included. It must also be said that the server we implemented offers only basic functionality needed for the prototype. It can only use one Bluetooth device, the handling of multiple Bluetooth receivers, as necessary in a real train, is not implemented. The server only issues, stores and obliterates tickets, all functions necessary to process the clearing of payments is not part of the code.

E-ON uses cryptographic routines from the Flexiprovider implemented by the CDC Flexiprovider Group at the Darmstadt University of Technology [CD02]. It provides state-of-the-art elliptic curve cryptography which well suits devices with limited resources [He02]. Extending certain diagrams of the UML model allows for a seamless treatment of security protocols (see Sect. 5).

The customer client has a simple and intuitive user interface, three “clicks”' suffice to buy a ticket. The user interface is designed according to guidelines for the design of user interfaces on small devices [Sh, Os]. The application can be operated with the fingers, the usage of the input pen is not necessary. While the implementation was developed, the user interface was evaluated by a cooperating research group from the University of

[1] Thanks to Tiana Lieske and Holger Grandy for their support.

Freiburg [In]. Based on the results of the user tests the user interface was improved further.

In the implementation, the application logic that is responsible for the communication protocols, the part accessing the Bluetooth device, and the user interface are strictly separated. This is a consequence of the design philosophy for security critical applications. The program parts dealing with the security, in this case the protocol implementation, must be separated from the user interface. This helps to prevent errors and enables an exchange of the user interface. It also lessens the effort necessary to get a correct protocol implementation. The encapsulation of the communication simplifies the usage of the communication device and allows a simple change to another communication technique if necessary. The separation of these three core parts of the application also follows a general design principle, the separation of concerns.

The most problematic part in the implementation is the attempt to compensate the unreliable radio connection. A lot of work went into the design of suitable recovery points and status information for the user. As we use Bluetooth it can happen that the transfer of the data between the server and the customer is stalled or interrupted. This means that the processing of a protocol may be blocked for some seconds or even unrecoverably interrupted. Therefore it is important to always inform the customer about the state of the application, i.e. if the processing is currently active, stalled or must be restarted. Uncertainty about what the application is doing greatly harms the usability. Recovery points in the protocol are necessary because an aborted connection should not mean that the user must restart at the beginning.

7 Conclusion

In this paper we presented E-ON (Electronic-Onboard-Ticketing), an interesting and useful yet simple m-commerce application. E-ON is a location-based service for the easy purchase of railway tickets on the train. It uses Personal Digital Assistants as customer devices and Bluetooth, a radio-based networking technique, for communication. Though small, E-ON poses surprisingly complex software engineering challenges.

We described the application design and the problems associated with such a service. Technical details and information about the implementation were presented, as well as a glimpse on the security problems incorporated in e- and m-commerce applications. Different security requirements of service provider and customer were described, as well as possible attacks on the service if an insufficient design is employed.

8 Acknowledgments

The work presented here was done as part of the research project “Go!Card”. Go!Card is sponsored by the German Research Foundation (DFG) in the priority programme “Sicherheit in der Informations- und Kommunikationstechnik”.

References

[AN95] Anderson, R. and Needham, R.: Programming Satan's Computer. In: van Leeuwen, J. (Ed.), *Computer Science Today: Recent Trends and Developments.* Springer LNCS 1000. 1995.

[Ba02] Baily, M. N.: The New Economy: Post Mortem or Second Wind? Technical report. Institute for International Economics. 2002.

[Bl] Bluetooth SIG: *Bluetooth Core Specification v1.2.* Bluetooth SIG. https://www.bluetooth.org/spec/.

[Br02] Bredemeier, W.: Die Entwicklung der deutschen Informationswirtschaft bis 2006. Technical report. Institute for Information Economics. 2002.

[CD02] CDC Flexiprovider Group, Chair Prof. Dr. J. Buchmann.: Flexiprovider. http://www.flexiprovider.de. 2002. TU Darmstadt.

[He02] Henhapl, B.: Platform Independent Elliptic Curve Cryptography over F_p. Technical Report TI-6. Department of Computer Science, Darmstadt University of Technology. 2002.

[HRS02] Haneberg, D., Reif, W. and Stenzel, K.: A Method for Secure Smartcard Applications. In: Kirchner, H. und Ringeissen, C. (Eds.), *Algebraic Methodology and Software Technology, Proceedings AMAST 2002*. LNCS 2422. 2002. Springer.

[In] Institut für Informatik und Gesellschaft, Abtl. Telematik.: Atus – A Tookit for Usable Security. http://www.iig.uni-freiburg.de/telematik/atus/index.html. Universität Freiburg.

[Jo00] Joy, B., Steele, G., Gosling, J. and Bracha, G.: *The Java (tm) Language Specification, Second Edition*. Addison-Wesley. 2000.

[JW01] Jakobsson, M. and Wetzel, S.: Security Weaknesses in Bluetooth. *Lecture Notes in Computer Science*. 2020:176+. 2001.

[Na00] National Institute of Standards and Technology: *FIPS 186-2, Digital Signature Standard (DSS)*. January 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.

[Na01] National Institute of Standards and Technology: *FIPS 197, Advanced Encryption Standard (AES)*. November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[OMG03] The Object Management Group (OMG): *OMG Unified Modeling Language Specification Version 1.5*. 2003. http://www.omg.org/technology/documents/formal/uml.htm.

[Os] Ostrem, J.: Palm OS User Interface Guidelines. http://www.palmos.com/dev/support/docs/ui/UIGuidelinesTOC.html.

[RJB98] Rumbaugh, J., Jacobson, I. and Booch, G.: *The Unified Modeling Language Reference Manual.* Addison-Wesley. 1998.

[SH] Sedov, I. and Haase, M.: Bluetooth API for Java. http://wwwiuk.informatik.uni-rostock.de/, http://www-md.e-technik.uni-rostock.de/.

[Sh] Shadish, B.: Handheld User Interface – Ten Commandments. http://www.mobilecoders.com/Articles/mc-01.asp.

[Sy02] Synopsys, Inc. : Synopsys DesignWare IP Solution Enables Pervasive Bluetooth Adoption, http://www.embeddedstar.com/press/content/2002/9/embedded5196.html, 2002

[XB01] Thomas G. Xydis and Simon Blake-Wilson: Security Comparison: Bluetooth Communications vs. 802.11. Technical report. Bluetooth Security Experts Group. 2001.