Requirements and Technologies for Ubiquitous Payment

Sandra Gross, Elgar Fleisch
University of St. Gallen
Institute of Technology Management
Email: {sandra.gross, elgar.fleisch}@unisg.ch

Matthias Lampe
ETH Zurich (Swiss Federal Institute of Technology)
Department of Computer Science
Email: lampe@inf.ethz.ch

René Müller
UBS AG
Marketing Technology, Client Workbench & Channels
Email: rene-za.mueller@ubs.com

Abstract: With the upcoming of ubiquitous computing, banks and financial institutes meet new chances and challenges in their business. The goal of this paper is to identify requirements and test technologies for ubiquitous payment (u-payment). The work was done in a joint research project of our research team and United Bank of Switzerland (UBS). To derive the results the project team conducted interdisciplinary innovation workshops, built demonstrators and analyzed user and UBS experi-ences. The paper first evaluates the key features of u-payment in comparison to mobile payment (m-payment). Then, it describes the Preferred Payment Architecture (PPA), which is developed by Mobey Forum, a global, financial-industry driven forum. UBS is one of the founders of the forum and presses ahead with this architecture as this recommendation implements the requirements of customers, financial institutes and merchants in equal measure. The research team developed the test platform BluePay, which implements some chosen requirements of PPA in order to gain experiences with local payments in a store with the technologies Bluetooth and Radio Frequency Identification (RFID). The main results of this work are a definition of u-payment by the authors as unobtrusive, ubiquitous, invisible, and in the environment integrated payment, an evaluation of technologies and requirements of the u-payment system demonstrators, and some implications for the adoption path from m-payment to u-payment.

Key words: mobile payment, ubiquitous computing, payment architecture, RFID, Bluetooth

Introduction

With ubiquitous computing (Ubicomp) technologies banks and financial institutes are asking whether ubiquitous payment (u-payment) systems can contribute to competitive advantages. This paper sees u-payment a subgroup of m-payment. On the one hand, Forrester estimated a yearly revenue of m-payments in Europe of 26 billion USD in 2005 [Fore01], Frost & Sullivan 25 billion USD in 2006 [Mobi02] and Reuters even 50 billion USD in 2006 [Reut01]. On the other hand, the m-payment market is in a constantly flux due to a wide variety of payment solutions, technologies, scenarios, consumer expectations, and penetration strategies of payment service providers. The systems change and are subject to a high or low market penetration according to the parties' requirements: Customers, financial institutes, and merchants alike want a convenient way to perform payments, even though they have different motivations. For instance, the customer wants a convenient and trustworthy way to pay, the financial institute needs automatic and economic settlement of the payment. Based on these considerations, it would be desirable to handle different payment methods with a standardized architecture. The customer should be able to choose his preferred device, his mobile phone or PDA, and choose the appropriate financial service (e.g. financial information or payment). Today, these services are rendered by mobile payment (m-payment) systems. U-payment systems should offer services, for which the customer defines the level of interaction with the technical system according to his context. This view enables seamless payment such as automatic payment in public transportation. In this case, the customer might abandon his mobile phone in favor for an identity card to achieve the highest convenience for unobtrusive payment.

The goal of this paper is to examine how u-payment systems could look like and to analyze first experiences of payment systems that are on the transition from m-payment to u-payment. The results were derived from literature research, interdisciplinary workshops and the development of the u-payment test platform BluePay.

The structure of this paper is as follows: First, the differences between m-payment and u-payment are examined. Then, the Preferred Payment Architecture (PPA) of Mobey Forum[1] is introduced in order to show one standardized way of how to deal with requirements of different value chain partners in payment. Third, the paper describes the test platform BluePay that was developed by the research team of our department and UBS. BluePay puts several requirements of the PPA into practice. Then the authors summarize chances and challenges in practice, and finally conclude how the development of u-payment could look like in the future.

[1] UBS is one of the founder members of Mobey Forum (www.mobeyforum.org).

From m-payment to u-payment

The following two sections show that it is difficult to draw the exact border between m-payment and u-payment clearly. The authors give respectively a short definition of the terms and the application areas of the technologies.

M-payment

M-payment can be understood as any access to payments, where at least one participant uses a mobile device. This is often a mobile phone ([Kru01], [IWW02], [KPT02]). Other devices are for instance personal digital assistants (PDA), or items in which transponders are integrated. This could be an identity card. The data stored on the transponder is transmitted via radio communication to a reader and passed through to a financial network [ThRoJ].

Frost & Sullivan extracted several application areas for m-payment in a study [ITW02]:

- Automated point-of-sale payments (vending machines, parking meters and ticket machines)
- Attended point-of-sale payments (shop counters, taxis)
- Mobile-accessed Internet payments (merchant WAP sites)
- Mobile-assisted Internet payments (fixed Internet sites using phone instead of credit card)
- Peer-to-peer payments between individuals

U-payment

There is no common definition of the term u-payment yet. The authors take the definition of ubiquitous computing proposed by the researchers at the Xerox Palo Alto Research Center as orientation for a possible characterization of u-payment. They defined ubiquitous computing as the most unobtrusive way for human beings or for objects to interact with a computer system [Weis99]. This leads to a definition for u-payment as ubiquitous, invisible and unobtrusive payment, which is integrated into the environment and regards the context of the payer. The payer can be either a human being or an object. This means, that the payment process should not interrupt the payer in his current action or should not interrupt running processes, unless a process change initiates the payment. An example for the latter could be if the change of a machinery part triggers the payment for the new part in maintenance and repair. M-payment systems vary in the degree of human interaction between payer and the technical system. The above definition would classify payment systems with a low level of human interaction closer to u-payment as others.

Examples for application areas of u-payment are automatic toll or automatic self-checkout in stores. Speedpass represents one payment system with minimal human interaction: Radio Frequency Identification (RFID) chips are integrated into key fobs so that the customer can pay at ExxonMobile service stations by simply holding the key fob in front of the RFID reader [Exx02]. The degree of human interaction depends on implemented security features such as an active payment authorization by the customer. There are several companies investigating on u-payment scenarios such as Accenture. They work on object-to-object payment scenarios. The underlying assumption is, that products or objects will trigger payments when product associated services are used. Every-day objects or industrial goods will be equipped with RFID tags and sensors. Sensors and tags will be able to communicate with a micropayment infrastructure. The user will be able to concentrate on the usage of the objects instead of concentrating on the payment process [DSt01]. The objects are context sensitive and their buying decisions and actions are based on implemented rules, which take the contextual situation into account. Some industrial applications could be promising from a business perspective such as [Acc02]:

- Automatic spare part management,
- Real-time inventory management which keeps supplies coming,
- Individual risk evaluation for insurances for driver individual insurance fees derived from automatically generated driver profiles.

Preferred Payment Architecture

The Preferred Payment Architecture (PPA) is developed by the Mobey Forum and will enable user-friendly and secure mobile banking and payment services in a standardized way. It encompasses the requirements of standardization bodies, financial institutions, mobile device manufacturers, network operators, consultancies and merchants. The PPA is no new standard, but builds upon existing standards and describes an open architecture [Mob00]. The Mobey Forum aims at a widely accepted standard that is accepted by all parties. This is the reason why PPA is designed technology independent and can therefore be used for m-payment and also for u-payment.

The following section summarizes the PPA requirements. They are valid for the three different scenarios remote payments, local payments and mobile banking services. As the demonstrators of the project team should implement concepts of local payment (real POS in a store) and remote payment (only payment information stored on the mobile device is the RFID-identification number), these two versions of the PPA are regarded here. The demonstrators could easily be enhanced with mobile services features such as personalized financial information, but this is beyond the scope of this paper.

Requirements

Financial institutes must learn from the critical success factors of mobile payment systems in order to achieve technical, organizational and economic goals such as a high market penetration. The learnings and the consolidated requirements of all parties are summarized in Table 1.

Type of Requirement	Requirement Description
Customer Proposition	• Convenient user experience • Freedom to choose bank, operator and handset, and change them independently from each other • Mobile financial services have to have wide acceptance and usability • Customer habit enhanced • Technical and perceived security
Business Priorities	• Banks authenticate their customers while providing banking and payment services • The service proposition has to offer value for all relevant parties • Business processes of different players have to remain independent of each other • The solution has to scale across all financial service opportunities • Branding has to also be available within mobile environments.
Technical issues	• Open and non-proprietary technologies have to be used • Existing standards and solutions should be used, where possible • Technological solutions have to enable independence between banks, operators and mobile phones • End-to-end security, secure authentication, and non-repudiation have to be guaranteed
Implementation issues	• Implementation costs to banks, merchants and consumers have to be relatively low • Time-to-market is of critical importance

Table 1: PPA Requirements [Mob00]

Remote Payments

Remote payments encompass a variety of transactions including buying of goods, services, or content using a mobile device, for example, buying ring tones using a mobile phone via Short Messaging Services (SMS). Today, the majority of remote payments are done using SMS. More complex payments are done using the mobile Internet, which is

enabled through communication technologies such as General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS). The requirements for the customer are a mobile device with an integrated browser.

The PPA for remote payments implements the so-called three domain payment process (see Figure 1), which ensures the responsibility of the issuer and acquirer bank for their systems. In addition, the communication between all parties must be guaranteed and underlie auditing restrictions. The following technologies are involved:

- *Server Based Wallet (SBW)*: The SBW manages customer information about the customer's credit or debit account and a security certificate. With remote payments, the wallet does not reside locally on the customer's device but on a server of the issuer bank or of a trusted third party, which fulfills the PPA requirements.
- *Interoperable Security Protocol*: The protocol ensures the security of the payment transactions between the issuer bank, the acquirer bank, and the merchant. Possible protocols are 3 Domain Secure (3D Secure) of Visa, 3 Domain Secure Electronic Transaction (3D SET), used mainly in Europe, or Secure Payment Application (SPA) of Mastercard. The issuer bank or the SBW service provider can choose the authentification mechanism, as long as the liabilities are regulated.
- *Customer Authentification*: Customers can identify themselves using a personal identification number (PIN) or a password. With certificates in place, e.g. a local PIN will restrict any access to the private key.

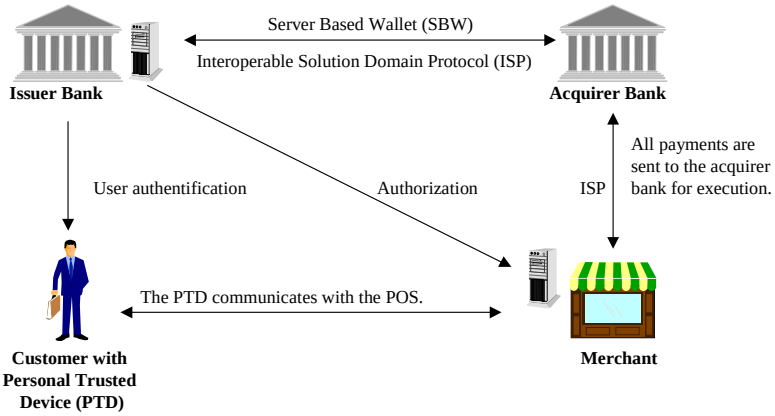

Figure 1: PPA for remote payment

Local Payments

There are already a broad variety of local mobile transactions on the market. One possibility is to use mobile phones as digital wallets. The key requirements for mobile

payment devices are user-friendliness, security and payment system reliability. The PPA for local payments suggests bank issued credentials and applications on a chip, enabling access to the appropriate payment method. The chip embeds the standard of Europay, Mastercard and Visa (EMV). The PPA for local payments is shown in Figure 2. PPA suggests various technology alternatives for payment methods, transport protocols and connectivity [Mobe02]. One of the demonstrators of the test platform BluePay implemented the connectivity technology Bluetooth, the second demonstrator incorporated radio frequency transmission. Bluetooth is suitable for the exchange of bigger quantities of data between payment device and POS. The project team chose RFID for a second demonstrator to implement a so-called soft identification – the exchange of a unique identification number of the payer with the POS with optional confirmation by an offline PIN.

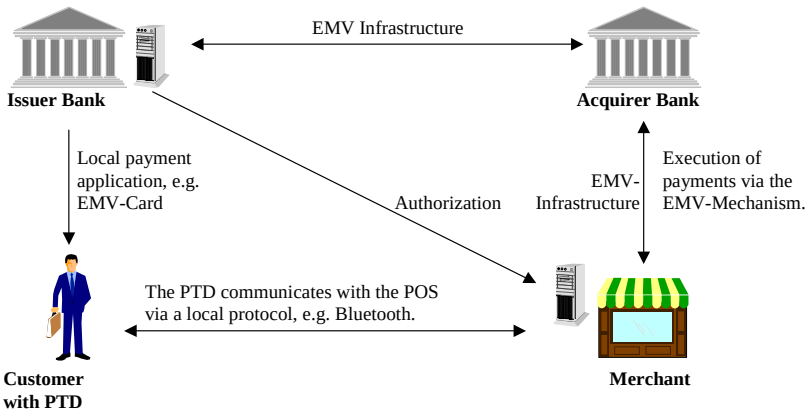

Figure 2: PPA for local payment

U-Payment Test Platform BluePay

The project team developed the u-payment test platform BluePay for local payments using the technologies Bluetooth and RFID. Regarding PPA requirements, an emphasis was placed on: (1) local payment scenarios, using a combination of the PPA for local and remote payments, (2) open, non-proprietary, and existing standards such as Bluetooth and RFID, and (3) the independence between dealers and financial institutions, since payments are executed via the EMV-mechanism. Based on the test platform different payment demonstrators where implemented which can be used for payment scenarios such as retail or public transportation.

The objective of BluePay was the test and evaluation of Bluetooth and RFID for the implementation of u-payment systems. In addition, it was also evaluated to what extent it is possible to reduce or eliminate the explicit interaction of the customer in the payment process.

Two variations of BluePay were addressed: *customer identification to initiate the payment* and *local exchange of payment information*. The following sections, describe these two variations using two implemented POS demonstrators, which are embedded in a Ubicomp retail scenario, in which the POS automatically identifies all products using RFID tags on the products.

Customer Identification to Initiate Payment

The first variation of BluePay is a local payment demonstrator, in which a local identification of the customer initiates the payment process. The PTD only stores the customer identification and no further payment information, such as credit card numbers. This additional information is kept in a customer database in the backend systems of participating banks or third parties (see Figure 3).

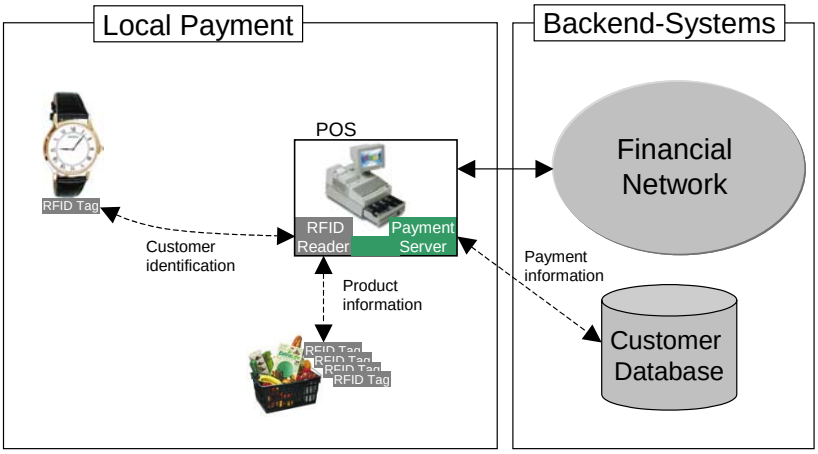

Figure 3: System architecture of 'customer identification to initiate payment'

We chose RFID as the identification technology in our demonstrator, since it provides a fast reliable way to identify the customer. The RFID chip to identify a customer can be incorporated in an object, which the customer already carries such as a watch or mobile phone. The RFID reader is integrated in the POS, which in our scenario also identifies the products. The unique identification of the customer allows retrieving the payment

information from the customer database and executing the payment using the financial network and the EMV mechanisms. Although the payment is initiated locally, it uses a payment process similar to the server-based wallet concept.

In our scenario the customer does not need to confirm the payment by entering a PIN, since a fast and convenient payment with minimal interaction was required. We call this process *soft identification*. However, the customer gets feedback of the payment process such as status of the payment using a display of the POS and an optional PIN confirmation can be activated. The demonstrator also offers the customer to access and change payment information and payment preferences via a Web page. Possible preferences could include limits for using soft-identification (e.g. usage for amounts below EUR 50).

Local Exchange of Payment Information

In this second variation of BluePay, the PTD has to be able to store all necessary payment information, which is transferred via a local wireless connection between the POS and the PTD (see Figure 4).

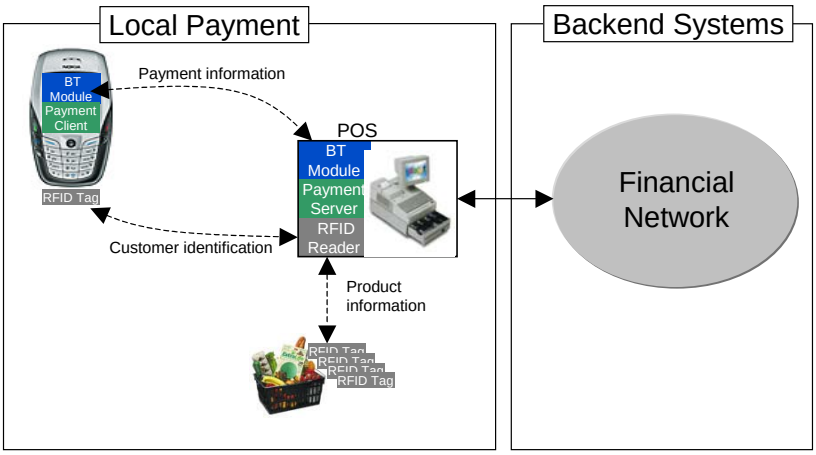

Figure 4: System architecture of 'local exchange of payment information'

The payment process in this demonstrator is initiated by the identification of the PTD, which in our case is a mobile phone with Java and Bluetooth capabilities. Since establishing a connection between mutually unknown Bluetooth devices can take in the worst-case several seconds [SiR03], the PTD is identified using a RFID chip, which stores the Bluetooth MAC address of the PTD. When the PTD is identified using the

RFID reader in the POS, the Bluetooth address allows establishing the connection in a fast and reliable way. After the Bluetooth connection has been established, the *Payment-Server* component on the POS exchanges the necessary payment information with the *Payment-Client* component on the PTD. This includes credit card details to execute the payment via the EMV mechanisms, and payment preferences, which are stored on the PTD, such as limits for soft identification as described above.

In our scenario, the customer gets feedback about the payment process on a display of the POS and the display of his mobile phone. Payment information, payment preferences and electronic receipts can be accessed using the mobile phone.

Chances and Challenges of U-Payment in Practice

Based on the interdisciplinary workshops conducted with the business idea generation method [Gros02] and the user experiences with the test platform BluePay the authors could identify chances and challenges of u-payment in practice in four main areas: business models of u-payment, technical feasibility, security and privacy, as well as standards. As standards are dealt already within the Mobey Forum, they are not described here any further.

Business Models

Although there are already existing application scenarios for u-payment, there is still missing clarity about the business models related to u-payment. The role of financial institutes could be to facilitate u-payment for their customers. The project team evaluated that promising applications probably occur rather in business-to-business than in business-to-customer scenarios. Unobtrusive inter-company payment systems would rely on products, which identify and localize themselves (e.g. in a supply chain), and which automatically trigger the payment process in real-time. Therefore, some business model questions have to be resolved such as cost sharing of the infrastructure, or cost/benefit considerations.

Technical Feasibility

There are still some challenges in practice even with well-established technologies. Their implementation in a real environment often poses surprising problems. In the case of the test platform BluePay, the Bluetooth-demonstrator allowed to identify the payer uniquely in the test environment. However, when there were several payers in the queue in a shop, who were ready to pay with their devices, the system had to decide which payer was the right one for the products. The
u-payment system had to ensure the correct payer-POS relation. The problem could not

be solved completely, but by some technical adjustments it was possible to reduce it: through antenna arrangement and antenna power lowering.

Security and Privacy

Both the payment information on the payment device and information about payment habits must be secured and protected along the whole value chain. This is an opportunity for financial institutes as customers already entrust their financial information to them. The implementation of the demonstrators showed that there are certain security mechanisms such as challenge-response-algorithms, which allow protecting data on software and hardware level. The data connection between the payment device and the RFID reader must also be ensured for RFID applications. The demonstrators used Bluetooth encryption features and application based security implemented through Java components.

Conclusion

The requirements for u-payment and m-payment are basically the same: the PPA requirements integrate the views from all value chain partners and from the basis for the key success factors: customer perception of the payment instrument, merchant or value chain partner acceptance, and technology as necessary catalyst to achieve or improve certain business processes. As the payment procedures are still processed via existing financial networks, the main difference lies in the interfaces to payment: payment devices in m-payment are often mobile phones or personal digital assistants whereas u-payment can use unobtrusive technologies like RFID transponders.

On the adoption path from m-payment to u-payment there are already many applications on their way such as Speedpass. The demonstrators based on BluePay illustrate that technical feasibility must always be regarded in the real world environment, for example to test the automatic and unobtrusively identification of a payer. The test platform showed that in order to secure a success of the u-payment system the payment system provider should offer secure, transparent and simple payment procedures. Also, merchants have to be involved from the beginning, as their support is essential.

We see the future of u-payment not only in business-to-consumer sector, but also in the sector of business-to-business: Payment scenarios (e.g. in the supply chain) could gain more importance with the development of object-to-object payments with low or no human interaction. This implies that products trigger payments in real-time and based on context dependent business rules. Further research should concentrate on the evaluation of requirements and technologies, enabling business models such as pay per use, pay per damage, or pay per risk. In each case the principle applies that the customer is liable for the actual used amount of service respectively damage.

Literature

[Acce02] Accenture: Ubiquitous Commerce - Autonomous Purchasing Object. www.accenture.com/xd/xd.asp?it=enweb&xd=services\technology\tech_autopurchase.xml, Visited the 2003-06-17

[Dahl02] Dahlberg, T.; Mallat, N.: Mobile payment service development - managerial implications of consumer value conceptions. European Conference on Information Systems (ECIS), 2002

[DSta01] DStar - Accenture Lab works on "object-to-object" Internet Commerce: www.hpcwire.com/dsstar/01/1120/103711.html, Visited the 2003-03-17

[Exxo02]ExxonMobile: Hard-to-Shop-for People on Your Holiday List? How about an Electronic Wallet for Their Wrists?. www.exxonmobil.com/Corporate/Newsroom/Newsreleases/xom_nr_041202.asp, Visited the 2003-03-17

[Fore01] Forrester: European Mobile Payments: Can't pay, won't pay, says Forrester, 2001, www.forrester.com/ER/Press/Release/0,1769,562,00.html, Visited the 2003-11-17

[Heis03a] Heise online: Paybox stellt Endkunden-Geschäft in Deutschland ein. www.heise.de/newsticker/data/uma-23.01.03-000/, Visited the 2003-07-04

[Heis03b] Heise online: Paybox meldet sich mit neuem Partner zurück. www.heise.de/newsticker/result.xhtml?url=/newsticker/data/psz-28.06.03-002/de, Visited the 2003-07-04

[ITWo02] ITWorld Study: M-Commerce to be $25B Market by 2006. www.itworld.com/nl/ebus_insights/04042002/, Visited the 2003-08-04

[IWW02] IWW: Zahlungssysteme im Internet - eine Übersicht. Institut für Wirtschaftspolitik und Wirtschaftsforschung der Universität Karlsruhe, 2002

[Krey02] Kreyer, N.; Pousttchi, K.; Turowski, K.: Characteristics of Mobile Payment Procedures. In: Proceedings of the ISMIS 2002 Workshop on M-Services (2002)

[Krue01] Krueger, M.: The future of M-Payments - Business Optionsand Policy Issues. Institute for Prospective Technological Studies (European Commission), 2001

[Mobe00] Mobey Forum: Mobile Financial Services (White Paper), 2000

[Mobe02] Mobey Forum: Preferred Payment Architecture: Local Payment (White Paper). 2002

[Mobi02] Mobile CommerceNet (2002) Mobile payments to reach USD 25 billion in 2006, www.mobile.commerce.net/story.php?story_id=1458, Visited the 2003-11-17

[Reut01] Reuters (2001) Yankee Group: Mobile Commerce market to be Worth over $50 Billion in Europe by 2006. In: Investors and Media information

[Sieg03] Siegemund, F.; Rohs, M.: Rendezvous Layer Protocols for Bluetooth-Enabled Smart Devices. To be published: Journal for Personal and Ubiquitous Computing (PUC), 2003

[Thin03] Thing, L.; Rouse, M. (o.J.): M-payment. http://searchbusiness.techtarget.com/sDefinitions/0,,sid19_gci772807,00.html, Visited the 2003-11-12

[Weis99] Weiser, M.; Gold, R.; Brown, J.S.: The origins of ubiquitous computing research at PARC in the late 1980s. In: IBM Systems Journal (1999) 4: pp. 693-696