45

A Functional Model for Mobile Commerce

Reinhard Riedl
Department of Information Technology, University of Zurich

Abstract: In this paper we shall introduce a feasible functional model for mobile commerce, which meets the basic user requirements. First, we shall analyse these requirements and we shall give an overview on the interplay of disciplines in the design of successful mobile commerce applications. And we shall explain the core results of interstate e-government research on information relevance management, as they apply to mobile commerce. Second, we shall define and discuss the functional model for the mobile end-user devices. Third, we shall discuss various non-standard mobile commerce scenarios, which might help to bootstrap mobile commerce in the large.

1. INTRODUCTION

In this section, we shall present some basic considerations on mobile commerce. We shall first give an overview on basic success requirements and we shall depict the various tasks, which are part of the design process. Then, we shall discuss the key issue of information relevance management. Hereby, we shall rely on recent research results in interstate e-government. And, finally we shall various conclusions for the risk handling in mobile commerce.

1.1 Mobile Commerce

In the following the term mobile commerce will describe transactions with a monetary value that is conducted via mobile telecommunications networks ([2]). In [11] a list of emerging applications is depicted, including mobile inventory management, product location, proactive service management, wireless engineering, mobile auction and reverse auction, mobile distance education, wireless data centre, and mobile music and music on demand.

When we compare the requirements for these applications with usual requirements for e-commerce applications, we may identify various differences. As it has been pointed out in [11], we need a wireless user infrastructure - that is a mobile end-user device with sufficient memory, an appropriate display, and communication functionalities, plus an appropriate operating system with a small footprint fulfilling real-time requirements – wireless and mobile Middleware, and wireless networking infrastructure. In particular, location management, reliable and survivable networks, and roaming across multiple, heterogeneous networks are essential for successful mobile e-commerce, and the wireless quality of service sets the constraints for application scenarios and system design.

The restrictions on performance and dealing with a heterogeneous distritibuted system are two major challenges for mobile commerce, while the location services are a major, novel opportunity for mobile e-commerce.

Our approach in this paper is partially orthogonal. It stems from our interdisciplinary research on interstate e-government ([6] and [8]), and it is based on our prototyping experience with inter-organisational document services for e-government [9]. We have not implemented mobile access, but access with Javacards and stationary kiosks. However our analyses of scalability issues generalise to mobile commerce.

On the one hand, interviews with European citizens and with civil servants have stressed the issue of trust and confidence for all kinds of e-government services, which are accessed with Smartcards. We put forward the thesis, that trust and confidence requirements for mobile commerce will have to fulfil comparable if not more strict requirements than e-government. On the other hand, the heterogeneity Europe with respect to processess, ontology, and culture for e-government renders global services difficult challenge and it makes homogeneous solutions impossible to achieve (compare [5] and [7]). Part of this heterogeneity is typical for the governmental context, but the heterogeneity of user requirements with respect to usability an acceptance of technological solutions, constitutes a challenge for all kinds of services, which should be universally accessible.

From an analytic point of view, all forms of e-commerce require a clear concept of digital identity and a clear concept for data protection. In practice, these requirements are often ignored, and attempts to provide adequate concepts (as in [1]) are rare and still lack implementation. However, due to an increased uncertainty about the identity of customers, and due to the increased possibilities for customer profiling, once this uncertainty is resolved, on mobile commerce convincing concepts for digital identity are essential, both for legal reasons and for achieving customers' trust and confidence. Implementations of mobile commerce must be globally usable, but the stated heterogeneity of cultures makes it impossible to create one solution for all. If we want to achieve scalability, digital identity has to be separated from service access functionality. While it is possible to provide local solutions for digital identity, interoperability will only be achieved with a global

solution, which has to provided by e-government. On the contrary, in many application scenarios, global service functionality is impossible to achieve.

Thus we identify trust and confidence and universally accepted digital identity as two further major challenges for mobile commerce. Further, intercultural usability may be considered as another challenge, but further basic research will be needed, in order gain better insight into what can be achieved, and what should be achieved.

In [11], the main issues for developers are identified as network processing and storage requirements, application development, compatibility and interoperability, and the procurement of desirable features such as easy upgrades. The authors conclude that the development of the next frontier of e-commerce will require the active participation of economists, computer and telecommunication experts, social scientists and business strategists.

Our research approach is similar. Our interdisciplinary research team consists of computer scientists, social scientists, economic scientists, psychologists, mathematicians, application experts, and business consultants. Our experience has shown that this type of interdisciplinary co-operation is difficult to manage, but it is a conditio sine qua non for research progress.

1.2 SUCCESS FACTORS

Successful mobile commerce results from the combination of five different expertises:

1. Distributed computing with mobile access
2. User-friendly human-system interaction design
3. Information and knowledge mining and management
4. Transparent security technology
5. Business processes based on clear value net models

The relevance of 1, 2 and 4 is quite obvious, and it complies with folklore engineering standards. 3 addresses both the exploitation of data about user-behaviour and the exchange of information between different organisations. Mobile phones and other mobile devices offer physical localisation, which opens new possibilities for electronic customer relationship management. Future business models will be based on the co-operation between different players, as the business as whole is too complex that single providers can efficiently offer total service. This stresses the need for IT systems enabling information exchange between different organisations. Finally, when different partners cooperate, clear models are needed where and how value is generated in this co-operation, that is in distributed workflows, or sets of loosely coupled independent workflows.

A carefully engineering of the interplay of the above factors is a conditio sine qua non for a successful development of mobile commerce solutions. Success and failure are essentially determined by user acceptance, which in turn, is very much influenced by four key factors:

1. Trust and confidence
2.-4. Universal access for many or all
2.-4. Usability
2.-4. Services which address customer needs

Our interviews with European citizens have stressed the criticality of trust and confidence, while the ranking of the other four factors is unclear so far, and we hereby have to rely primarily on business experience for similar scenarios.

Trust and confidence (T&C) is different from pure security. It means security PLUS the acceptance of/belief in its trustworthiness by the customers. T&C addresses technical, commercial, psychological, social, and cultural issues. T&C may come along without proper security underneath. Moreover, clearly there will never be something like 100% security. However, in the long run, customers will require a common sense amount of security plus add-ons, which depend on the local culture.

Universal access for all means access transparency with respect to time, place, and particular features of a type of accepted access devices – hereby, transparency is used in the sense of distributed systems – AND it means availability of proper access devices for all people, independent of social status or personal handicaps. Cultures differ with respect to the emphasis of this issue though. In some major market places in Europe, for example in the UK, access facilities for handicapped people are an absolute requirement for political acceptance of digital services.

Usability is another major issue: Care has to be taken that indeed no special skills and experiences in interaction with computing systems are required for the access to the commercial services. If the listed first three pre-requisites are fulfilled, then finally the services decide whether a particular mobile commerce application is accepted. Both choosing suitable trust and confidence guarantees and selecting the right services, requires market research on user needs, part of which can be done in the markets themselves with the evaluation of customer traces [8].

T&C, access, usability, and services are the qualities of a mobile commerce solution, as customers perceive them. Considering mobile commerce from the perspective of system designers as a special form of distributed computing, it is a distinctive feature of mobile commerce, that, once again, special attention has to be given to the communication and distribution models.

A clear separation of the layers in the communication protocols, flexible quality of services implemented with selectable protocol modules, and total transparency are essential quality criteria. The same is true for the event model, the monitoring, and the rules for the evaluation of traces. Once such a Middleware is available, an advanced distribution of application logic is possible, whereby the restricted resources in mobile devices pose new requirements for performance engineering (while the costs for the infrastructure set the constraints for the scalability-engineering task). Economic issues will drive the actual distribution. Thus, the distribution of processing capacity, workload, control, and intelligence is finally

governed by the interplay of performance and economic issues, and the constraints are set by the objective security requirements and the subjective user perception of trust and confidence guarantees.

The customer-to-system interaction requires both user-friendly design, which is easily understood, and it must fit with the requirements for the market research and customer profiling. The interaction of users with the system tells us a lot about their needs, likes and dislikes. If we really want to exploit that implicit generation of knowledge, we have to design the events of the customer-to-system interaction in such a way that the event mining for knowledge on customers provides optimal results ([10])

The bottom line of all design is making profit. Profit requires that value is generated and risk is properly handled. This in turn requires a sound management of information relevance, since the trustworthiness of the information exchange, or the handling of untrustworthy or partially trustworthy information, respectively, is the basic requirement for any successful commerce.

1.2.1 MANAGEMENT OF INFORMATION RELEVANCE

The key inequality for relevance management reads:

Relevance = Correctness (with respect to a given content context) + Authenticity (of the origin) + (possibly) Validation (of relevance by human or non-human relevance agents) + Actuality (of the contents) + History (as it is relevant for the creation process) + Role of the producer (as an individual or as a member of an organisation) + Quality guarantees (provided by the producer) + Validation estimation by the receiver (who makes the final decision)

Clearly, correctness and authenticity are necessary on the left-hand side. The necessity to integrate the history stems from causality problems in distributed computing due to the lack of global time. Case studies in e-government and in e-business reveal the necessity to support validating statements, e.g. when statements with respect to the living place have to be verified by the police, which eventually requires that digital statements on digital statements are made. As it is common practice in non-digitised scenarios only to accept information of a decent age, actuality is a necessity on the left-hand side, too. Similarly, the role of the producer and the quality he guarantees determine the relevance of information. (For a case study on the social impact on the relevance of information see [4].) Finally, the decision on the relevance of a document has to be made by the receiver of information. It can be outsourced, but then this has to be implemented as the decision rule, that statements of a selected partner have to be considered as fully relevant. Thus, in general, the factors on the right hand side are necessary, although the corresponding attributes may become void in a particular scenario.

Whether the list of factors is indeed complete is difficult to verify. We have checked the completeness with respect to various e-government applications, which

yielded some evidence that it is indeed sufficient for inter-organisational information exchange.

The critical concept for the implementation of relevance management is that of context procurement. The application logic should not attempt to deal with distributed, consistent, actually correct data, as it is never possible to achieve total consistency, and even restricted consistency is very expensive. Instead, electronic documents should be exchanged, which provide data plus a definition of the data context. This context consists of the following components

- Content definition (what is described by data, and what is not described by data)
- Time and circumstances of creation (when and how was the document created, which enables the receiver to decide on the history, the actuality, and quality)
- Role and identity of the person and/or system component confirming the data (verified by a digital signature)
- Purpose of the document (who is addressed and what is the addressee allowed to do with the data)

The latter is of particular importance in Europe, where rather restrictive data protection laws apply. Documents thus have to be digitally signed, and possibly, they have to be encrypted afterwards, in order to guarantee that only the addressee will be able to read them. The appropriate formats for content definition are RDF and XML. However, a standard or a negotiated intermediary XML representation scheme is required.

Once such a context scheme is defined, the signing instance takes the responsibility for the correctness of the data with respect to the content context, the computing system takes the responsibility for the authenticity of the origin, and the receiver/consumer of information decides on the relevance of the content. The latter decision may be based on the content description, the time stamp, the trustworthiness of the role of the signing instance, and possibly additional statements by validation agents. Thus, the relevance of an electronic document is defined as the infimum of the relevance of the content, the trustworthiness of the signing role, the acceptability of the ‘age’ of the document, and the meaning of validating statements.

That context procurement scheme was developed in the interstate e-government project "FASME – Facilitating Administrative Services for Mobile Europeans". There, the originally intended approach of creating personal documents by handling states representing European citizens, had to be exchanged with the alternative approach of creating personal documents by shipping information with a given time stamp and an appropriate context definition.

Although this might appear a rather philosophical issue, it is a major concern for practical purposes. The originally intended approach in FASME would have created many problems for the organisational implementation and it would have provided significantly less useful services for the citizens than the current solution provides. The heart of the problem lies in the high costs of consistency management, which

are avoided with the alternative system design (which constitutes a complete digital realisation of traditional services).

In FASME, all documents shipped through the system are time-stamped and signed by the provider of the information. The signature assures the correctness of the document with respect to its explicitly stated context and the time-stamp of the document. The FASME-system guarantees the authenticity of the origin of information. Possible validation agents may annotate document meta-information on the relevance of the document. The FASME application also decides on the actual relevance of the document with respect to the administrative service requested by the citizen. This example (including its prototypical implementation) demonstrates the feasibility of the concepts introduced above. And it may be transferred to mobile commerce, as we shall depict in the following.

1.2.2 RISK HANDLING

There are various risks in mobile commerce, which we have to handle:

- Project risk
- Operational risk, namely
  - Risk of information relevance
  - Risk of attacks and misuse
  - Risk of system failure

Failure-Risk and project risk are classical issues in distributed computing and software engineering, and in e-business project management, respectively. The best way to handle the risk of information relevance is to mimic existing procedures and to confine oneself to security standards, which are better than security standards provided by existing practice. The critical two problems, which are known in e-commerce, but which are the more challenging in mobile commerce are faked digital identity and data protection. One customer can act in the name of others, and in fact he can let a computer act in the name of others, and an organisation may ignore data protection rules and use the data submitted by the customer and the data created by mobile service access without the customer's authorisation.

Risk handling thus requires the capabilities for authenticity management and the capability for the supervision of the information exchange and information usage, in order to guarantee non-repudiation and to avoid identity fakes, and in order to trace non-authorised intrusion into the system and lawfully behaviour of system insiders such as system administrators. Important examples of services for risk management are payment services, trust centres validating digital signatures and certificates, and certification services for the trustworthiness of providers or customers.

2. THE FUNCTIONAL SPECIFICATION

In this chapter, we shall define and explain those core functional components for mobile devices, which provide mobile communication between the customer and the virtual market. Further, we shall shortly discuss the feasibility of their implementation. The key component for mobile commerce is a mobile device for service access of the customer. This device speaks in effigy of the customer with the services provided in the virtual market. On the one hand, it plays the role of a legal representative, while on the other hand it has to protect the customer against various forms of fraud achieved through faked authenticity. Furthermore, it may provide agent functionalities to the customer interacting with a virtual market place.

The trustworthiness of mobile commerce essentially depends on the specification of guarantees provided by the mobile device and on their correct implementation. Guarantees have to be given in both directions, to the customer, who wants be sure that the services in the market are trustworthy, and to the services in the virtual market, which have an authenticated identity of the customer or non-repudiable proof of the possibly anonymous right of the customer to access certain services. In principle, that type of functionality can be separated from agent functionality. There are five basic functions of such a component:

1. Establishing secure and trustworthy communication channels with partners
2. Providing (limited) e-broker functionality
3. Providing limited workflow functionality
4. Providing a trustworthy, personalised graphical user interface
5. Providing authentication services with biometric tools

The basic idea hereby is that any negotiation or deal, and the corresponding relevance management, respectively, is based on the following scheme: One partner makes a statement by delivering a signed digital document with proper context specification. Part of this context specification may be a pointer to a validating agent, or a certificate, respectively. Then the other partner validates the statement, whereby he contacts one or various service providers for risk management. That is, the other partner always contacts a trust centre for the validation of the digital signature (except in cases of recent caching of that information), but possible he also contacts further partners, e.g. for the validation of certificates on the commercial or technical (IT-) trustworthiness of the first partner.

In order to be able to trust in the contacted centres themselves, the second partner always contacts trust centres of his choice, which negotiate with the trust centres chosen by the first partner in order to validate signatures and certificates. Further, in order that this works economically, the trust centre of the choice of the second partner has to bear the risk of wrong validation, as the certification services have to bear the risk of wrong certification. And the whole application system must provide non-repudiation in a legally relevant way. These procedures may be implemented with secure and trustworthy customer-to-one-partner communication

channels plus a non-repudiation monitoring. Please note that this generic scheme equally applies to digital payment services.

Thus, the secure and trustworthy communication with a partner is established by exchanging time-stamped, signed, and encrypted documents with a proper content definition.

E-broker functionality may be either provided by the access device or by a virtual extension of the access devices (cp.[3]), that is a secure and trustworthy channel to a remote e-broker, which may either be a service provider or a private application. E-brokers support the matching process between customers and suppliers. For instance, they contact different providers and they compare their offers. In case of standardised XML-specifications of products, that comparison will soon become feasible for mobile computing devices. Again, the risk of the trustworthiness of XML-descriptions of products arises, and a proper commercial management is both necessary and possible.

Contrary to the optional e-broker functionality, minimal workflow management functionality is mandatory in mobile access devices, which supports the procedures for deals depicted above. Further workflow management facilities may again be outsourced to some virtual extension of the device.

Finally a visual user interface (or an appropriate equivalent for handiicapped persons) and an authentication facility are needed. Traditional authentication is based on PIN numbers, but this does not suffice higher T&C standards. Instead, biometric authentication ought to be performed, which cannot be repudiated, such as it is provided by fingerprint sensors or by iris scanners (with a high degree of trustworthiness in the case of iris scanners). This can further be used for the authenticated confirmation of commands for digital signature of documents by the access device in effigy of the customer.

While communication and authentication are comparably secure if state of the art technology is used, the GUI might turn out as a Trojan horse. The access component acts as a representative of the customer and it is thus supposed to perform exactly what the customer wants it to perform. If the principle is violated in any way harm may be done to the customer. The customer thus needs an interface to the access device, which is both user-friendly and trustworthy.

This completes the description of the functionality of the access device. So far, we have indicated various other components in the system. However, they are rather one-to-one analogues of the corresponding components for e-commerce, except that they have to be capable of communication with the mobile devices.

Note that the functional model defines an open and flexible framework, since any e-commerce provider may be contact with the access devices defined, if he fulfils the basic communication requirements, and new trust centres may be added as confidence partners in a completely flexible way. Our prototyping with Javacard technology has confirmed this approach.

2.1 NON-STANDARD APPLICATION AREAS

In this chapter we shall discuss various non-standard application areas for mobile commerce. Right now, two main non-standard application areas of interest are e-government and virtual co-operations. Particular examples of promising applications are paid A2C (authority-to-citizen) e-government services and platforms for secure and trustworthy information exchange in virtual enterprises and in strategic co-operations in supply chains, and mobile access to trustworthy information services.

Interstate A2C e-government means the digital procurement of civil services. In order to bridge national, social, cultural, language and skills gaps, boundary objects for information brokerage are needed, and we have to implement inter-organisational, administrative workflows, which connect non-interoperable systems with incompatible ontologies, processes, and legacies. There are lots of local A2C e-government solutions being developed, but so far the main problem of inter-connecting authorities (in a way which respects the European data protection regulations) has not been addressed seriously. However, in the future, 'intelligent', digital ID-Cards, will enable the flexible and secure uploading of additional, commercial services, including services from direct competitors.

Future successful virtual enterprises and strategic co-operations in supply chains will have to rely on platforms for universal, mobile access to secure and trustworthy exchange of information among non-interoperable systems. In addition, an increasing public awareness of the importance of trust and confidence might nurture niche markets for the digital procurement of trustworthy documents (personal documents and expertises). Again mobile access will be mandatory for wide user acceptance and the bridging of ontological gaps will be a key success factors.

Mobile access devices similar to those developed for e-government and for future enterprise information management will then serve as carriers for standard mobile commerce applications. In parts, access devices disseminated for e-government will be capable of providing commercial services. A simple realisation of this concept (with pure access functionality) is already available with the Fin-ID card. Thus, e-government and mobile commerce will benefit from each other, and the same is true for enterprise information management and internal, mobile commerce.

However, this is only one side of our vision that could be described as ubiquitous information and knowledge management in the whole. This vision requires mobile ad hoc networking of information systems as depicted above, in order to gain universal access for delivery and usage of information and knowledge, but it also requests for the exploitation of implicit knowledge collected in mobile commerce and information exchange. Obviously, this need competes with the legal and ethic requirements for data protections and thus trustworthy knowledge digging solutions are needed which inter-operate smoothly with the ubiquitous knowledge

management. The rise of mobile commerce will rake this political and ethic conflict and compromises will have to be agreed upon.

3. CONCLUSION

We have presented a functional model for end-user devices in mobile commerce. This model is based on recent findings in interstate e-government, where the feasibility of the core functionality has already been demonstrated, although the interaction and communication model is less complex than in mobile commerce. Our model supplies the basic framework for future mobile commerce applications for various reasons: One access device can be used to access competing service providers in a secure and trustworthy way. Complex e-brokering facilities can be built on top of it due to an inherent and clear context procurement scheme. Services may be added ad hoc in a flexible way. Further, it will be possible to integrate mobile commerce with digital ID-Cards. And finally, the basic user requirements concerning trust and confidence are fulfilled.

4. REFERENCES

[1] Cap, C.H., Maibaum, N., Digital Identity and ist Implications for Electronic Government, Proceedings of the 1st IFIP Conference on E-Business, E-Commerce, and E-Government, Zurich 2001

[2] Durlacher, Mobile Commerce report, 1101010, www.durlacher.com/downloads/Mcomreport.pdf,

[3] Maibaum, N, Cap, C.H. Javacards as Ubiquituous, Mobile, and Multiservice Cards, PACT 2000, Proceedings of the International Conference on Parallel Architecture and Compilation Techniques, Workshop on Ubiquituous Computing, Philadelphia, PA 2000

[4] R.H.R. Harper, Information that counts: A sociological view of information navigation, in A.J. Munro, K. Höök, D. Benyon, editors, Social Navigation of Information Space, Springer, London 1101010

[5] A.-M. Oostveen, P. van Besselaar, Linking Databases and linking structures: The complexity of concepts in international e-government, Proceedings of the 1st IFIP Conference on E-Business, E-Commerce, and E-Government, Zurich 2001

[6] R. Riedl, Applicability of Modern KM Concepts for the Specific Requirements of Public Administration and e-Government., to appear in the Proceedings of the International Workshop on Distributed Knowledge and e-Government, Siena 2001

[7] R. Riedl, Information Brokerage in E-Government and in Interdisciplinary Research and Development Projects, to appear in Proceedings of the DEXA Workshop on e-Government 2001, Munich 2001

[8] R. Riedl, Interdisciplinary Engineering of Interstate E-Government Solutions, to appear in Proceedings of the Fourth International Conference on Cognition Technology: Instruments of Mind, Warwick 2001

[9] R. Riedl, Document-based Interorganisational Information Exchange, accepted for Proceedings of SIGDOC 2001, Santa Fe 2001
[10] R. Riedl, Event Mining in Virtual Markets: Market Research, Knowledge Engineering, Information Agents, and Social Role Structures, to appear in Proceedings of the IFIP Working Conference on e-Commerce / e-Business, Salzburg 2001, Kluwer Publishing
[11] U. Varsheney, R.J. Vetter, R. Kalakota, Mobile Commerce: A New Frontier, IEEE Computer, Vol 33, No 10
[12] M. Wenderoth, D. Wörmann, Development of an European-Wide Citizen Javacard to Support Administrative Processes by the Usae of Electronic Signature and the Fingerprint Sensor: A Case Study of Legal Implications, Proceedings of the 1st IFIP Conference on E-Business, E-Commerce, and E-Government, Zurich 2001