EPCiR Technical Report

An Evaluation of an OSGi-Based Residential Pervasive Computing Platform

Klaus Marius Hansen[1], Simon Bo Larsen[1],
Jakob Illeborg Pagter[2], Michael Østergaard Pedersen[1], and Jonas Thomsen[1]

[1] Computer Science Department, University of Aarhus,
Aabogade 34, 8200 Aarhus N, Denmark
{klaus.m.hansen,simonbl,michael,jones}@daimi.au.dk
[2] The Alexandra Institute's Centre for IT Security (AICIS),
Aabogade 34, 8200 Aarhus N, Denmark
jakob.pagter@alexandra.dk

Abstract. Residential applications including home control, alarm systems, and monitoring services is an area in which pervasive computing systems are currently emerging. One problem facing technology and service providers is getting a view on and analysis of technological and commercial problems and opportunities. As a step towards that, we present an analysis and evaluation of a widely-used setup for residential pervasive computing applications, viz., a setup based on a residential gateway with an Open Services Gateway Initiative (OSGi) implementation. The analysis is anchored in *use*, through scenarios and prototyping, and employs architectural, security, and business perspectives. Furthermore, we present challenges to be met to enhance technological and commercial opportunities for this platform.

Keywords. Evaluation and assessment, ubiquitous/pervasive computing, architecture, security, business analysis.

1 Introduction

As the realization of the vision of pervasive computing spreads [Green et al., 2001], [Moravec, 2003], [Starner, 2002], residential gateways represent a serious contender for bringing pervasive computing to the mass-consumer market. Residental gateways are typically small computers running an embedded operating system and equipped with Internet routers, firewalls, and support for various communication protocols such as Wi-Fi and Bluetooth. Prior to bringing such technology to market, there is, however, a need for a combined understanding of resulting technical and commercial consequences. We present an evaluation of a concrete solution for enabling pervasive computing in private homes using a residential gateway.

The evaluation was carried out during the "Enabling Pervasive Computing in Reality (EPCIR; `http://www.ooss.net/ecpir`) project. The EPCiR project involved scenario, business, architecture, and security experts from both research and industry, with the driver for the evaluation being a large european telecommunications company. A major factor in shaping the project was that the telecommunications company has an interest in potentially becoming a gateway operator in a residential pervasive computing market, complementing a number of service and equipment providers. One consequence of this was that the focus in the EPCiR Project, was on use and technology which was expected to be commercially viable in 2005.

The overall purpose of the project was two-fold: 1) to develop an approach for evaluating pervasive computing technologies, and 2) to use this approach on concrete residential gateway technology to answer whether the technology is appropriate for real-life applications? Section 1.1 summarizes the approach, Pervasive Scenario Evaluations [Hansen et al., 2003], and the rest of the paper desribes the results of the actual evaluation[1].

[1] Working notes describing the evaluation more fully are available from the EPCiR web site (`http://www.ooss.net/epcir`). The business analysis is partially specific to the Danish market

1.1 Pervasive Scenario Evaluations

Our approach is centered around *use* since we are interested in practical implications of introducing the evaluated technology. This focus is realized by rooting our activities in *scenarios* describing expected use of the technology, and by implementing *prototypes* based on these scenarios. Scenarios enable us to to explore unknown futures and share visions between stakeholders [Rosson and Carroll, 2003]; and prototyping allows us to experiment with these visions [Floyd, 1984]. Furthermore, we iteratively analyze the technology from separate views grounded in use; the views in EPCiR being 1) architecture, 2) business, and 3) security. The activities of the three views were mainly tied together through the shared focus on use, but joint workshops involving participants doing different kinds of analyses were also instrumental in this.

The *architecture analysis* describes and evaluates the overall structures of the technology in terms of components, their externally visible properties, and the interconnections between them in terms of connectors [Bass et al., 2003]. To describe and evaluate architectures that are not fully specified, as in the EPCiR case, we use the Unified Modeling Language (UML; [OMG, 2003]) for architectural descriptions, and Quality Attribute Workshops (QAWs; [Barbacci et al., 2002]) for architectural evaluations based on these descriptions.

The goal of the *security evaluation* is to identify a specification of suitable security mechanisms for the scenarios, and to use this to assess the security of the evaluated platform, security being crucial in user acceptance for a large number of pervasive computing technology [Stajano, 2002]. In order to do this, the platform is analyzed to identify weaknesses with respect to confidentiality, integrity, and availability. Our approach takes its starting point in the e-Pasta project (`www.e-pasta.org`), which in turn is inspired by the Common Criteria standard for product and system security evaluation (`www.commoncriteria.org`). A key element of our approach is to let users, domain experts, and security experts jointly and actively determine trust levels, i.e., *how* secure they want solutions to be. To this end the approach uses an iterative approach based on interviews, workshops, experiments with the prototypes etc.

Since the market for pervasive computing is still emerging, the roles of businesses have not settled yet. Partners and competitors have not been defined and neither has the value associated with the pervasive computing. The key element in our *business analysis* is *added value* through *complementors* [Brandenburger and Nalebuff, 1997]. In an emerging market, most actors are complementors and not competitors. Complementors are actors which add value to the market by combining their products.

The result of the evaluation is an analysis containing: choice of technology, a description of scenarios, evaluations of the platform based on each view, a prototype, and finally a overall assessment of the platform.

2 Overview of the Evaluated Platform

Part of the EPCiR project was to identify technology suitable for realizing residential pervasive computing in 2005. Residential gateways based on the emerging Open Services Gateway Initiative (OSGi; `http://www.osgi.org`) standard was chosen due to its versatility, availability of implementations including management solutions, and adherence to standards. Concretely, we investigated a Metavector Pylix gateway (`http://www.metavectortech.com`) and Prosyst OSGi software (`http://www.prosyst.com`) as a platform for realizing residential pervasive computing.

A simplified view of the overall architecture of the platform is shown in Figure 1 using a combination of UML deployment and component diagrams. The three-dimensional boxes show hardware hardware components and lines between boxes show protocol connectors. The following components are of primary interest:

- *Residential Gateway.* In this case a Pylix gateway that runs ProSyst's Embbeded Server (mBS) OSGi implementation. It is a gateway between residential equipment and the Internet.
- *Residential Equipment.* Sensors, actuators, and alarms that are connected to the residential gateway and can be controlled, administered or monitored by the residential gateway.

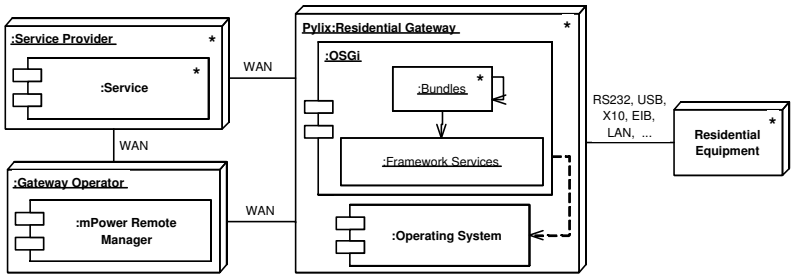

Fig. 1. Part of execution view of the evaluated technology

- *Gateway Operator.* The gateway operator monitors and maintains gateways using ProSyst's mPower Remote Manager (mPRM). It handles administration of software installed on gateways also for service providers. This includes initial bootstrapping of gateways.
- *Service Provider.* Provides services of value to a residential user. The initial contact between a service provider and a residential gateway goes through the gateway operator.

The evaluation results should not be taken as a complete evaluation of these technologies, but as an evaluation in the context of the scenarios of the EPCiR project.

3 Evaluation Results

3.1 Anchoring in Use

A number of future scenarios of residential pervasive computing use in the year 2005 were developed based on the IDON method [Galt et al., 1997]. In general the scenarios take place in two different futures — one in which a wide range of pervasive computing technologies are commercially available, and another in which the pervasive computing technology adoption is still at a rather premature level. In the scenarios, named persons in concrete situations use pervasive computing technology to, e.g., obtain security and safety; efficiency; and convenience. In the advanced scenarios, technologies such as micro-payments, application roaming, speech recognition, and web-enabled products play essential roles.

To enable prototyping and analysis within the resource constraints of the EPCiR project (see Section 4), the IDON scenarios were *refined* to scenarios including specific technology and solutions. The refined scenarios were useful as a common resource during prototyping and analysis. The following is two excerpts of refined scenarios from EPCiR:

- *Home care.* An elderly woman is treated for a diabetic foot ulcer in her home. Daily, she makes personal observations and stores these in an information system. Continuous measurements are made by an "active bandage" that she brought back from her latest hospital visit; and these are sent to the electronic health records at the hospital. Every week, the visiting nurse helps rinsing the wound, and on these occasions an online video conference are established with the expert doctor at the hospital to discuss the treatment plan.
- *Alarm.* A resident leaves home, heading for the library. Out of the house, he sends an SMS in order to activate the alarm of the house. The platform handles this, but senses that he forgot to turn off the light, which according to the configuration initiates an alarm. This alarm is caught by a service provider that automatically judges that this is not a serious alarm, and that no action is needed except notifying the user. The user receives the warning as an SMS, and from the library's public computer, he is able to access the residential gateway and turn off the light.

The scenarios mainly focuses on use involving the residential gateway, the residential equipment, and service providers (cf. Figure 1). This has meant that in particular prototyping has not experimented with the gateway operator component of the architecture. Most of the refined scenarios have been implemented, in a proof-of-concept-sense, the alarm scenario most fully. For the scenario realization, the residential equipment we experimented with includes X10 equipment (`http://www.x10.org`) for home control and simple alarms, Smart-Its (`http://www.smart-its.org`) for the active bandage, a thermoter, web and wireless cameras, and an SMS box.

3.2 Architecture Analysis

Architectural Test Cases. Architectures need to balance a large number of potentially contradicting architectural quality attributes. In the EPCiR setup, the *critical* architectural qualities were judged to be *availability*, *security*, and *usability*. In this analysis, the critical architectural qualities are critical from a technical as well as a commercial perspective.

Based on among others scenarios, critical qualities, and prototyping, *architectural test cases* are developed. In conjunction with an architectural description, these allow to make assessment of the evaluated architecture [Barbacci et al., 2002]. As an example the ECPiR project has a "self-configuration" test case, describing how installation of new applications should be a simple procedure not compromising security, safety, or correctness of installation. Examples of tests connected to this description is whether initial configuration can be done without intervention, how the gateway will detect new equipment, and how drivers, gateway software components ("bundles") etc. will be provided for new residential equipment.

Results. The proposed architecture supports the requirements put forth by the scenarios and to a large extent also the architectural test cases. There is, however, a number of areas in which substantial work is required to fulfill the architectural test cases. Identified issues include:

- *Device description.* There is no agreed-upon or standardized way of describing properties of residential equipment such as type, state, and capabilities. This is needed for in particular for self-configuration and is strongly connected to usability. For open-ended descriptions, technologies such as the XML Resource Description Framework (RDF; `http://www.w3.org/RDF/`) may be suitable, but agreement on specific formats for device description is needed.
- *Gateway and service monitoring.* For availability reasons, remote monitoring of gateways and services is needed. There is no specific provision for this in OSGi, but mPRM enables gateway operators to create scripts that may run periodically to check the status of residential gateways and connected residential equipment. This, however, requires that residential equipment and bundles running at residential gateways are monitorable in a standard way. Furthermore, there are potential privacy concequences that need to be handled if gateway operators, service providers or both should be able to remotely monitor most activity of bundles and equipment (see Section 3.3).
- *Runtime placement of data and computation.* To support long term availability and performance there is a need to be able to potentially place data and computation for applications dynamically at any component in the architecture of Figure 1. There is probably no smooth way of doing this since there is little architectural overlap between OSGi bundles and typical backend architectures such as J2EE (`http://java.sun.com/j2ee/`)

Each of these may be solved specifically and technically, e.g., by a gateway operator in the form of custom development

3.3 Security Analysis

The security analysis is built upon the refined scenarios, which means that focus in on the security issues related to the gateway and devices. That we do not focus on the backend (gateway to providers), is justified

by the fact we believe that this part contains nothing novel and can be handled using off-the-shelf security solutions.

The first key ingredient of our efforts is a security analysis resulting in a description of the functional and trust requirements for the *context*[2] we are studying. The functional requirements are basically — and not surprisingly — the well-known cornerstones of security: authentication, integrity and confidentiality. Another fundamental issue is that the system should be able to dynamically discover, enroll, and revole devices, i.e. life cycle management.

In the determination of trust levels, we primarily used workshops with domain experts in the EPCiR project group as time was short. The overall results were that alarms required a very high level of security (even the mere existence of an alarm must be kept secret), personal data involved in the health care scenario requires a reasonable trust level, but not at the expense of ease-of-use, and controlling light, ventilators etc. in the home requires little trust.

Security Architecture. To realize these requirements, we developed the following *idealized security architecture*, which is based on the assumption that devices only communicate via the gateway, i.e., we have a centralized setting.

The need for device security is divided into three categories: *low*, *medium*, and *high*. Lighting control is, e.g., in the low category; alarms, e.g., in the high category, and the remaining residential equipment from the refined scenarios is in the medium category. Briefly, security for each of these categories is realized as follows:

- In the low category it is sufficient for each device to claim an ID.
- In the medium category each device must use symmetric cryptography (AES or similar) to identify itself and to protect communication.
- In the high category each device must have a heart-beat (i.e. send a fixed length message with regular time intervals) and use asymmetric cryptography (RSA or similar) to identify itself and to protect communication. If one is willing to sacrifice non-repudiation, symmetric methods will suffice.

Realizing lifecycle management basically involves key management — in particular key exchange — preferably in an easy-to-use fashion. Unfortunately, traditional key exhange protocols do not meet this criterion, and during the short lifespan of the project we were not able to come up with good solutions to this end. Still, it is a requirement of our idealized security architecture.

Evaluation. Based on the security architecture we can evaluate the proposed platform. Among the conclusions are:

- The OSGi platform is a good choice for realizing the security architecture
- X10 equipment is not suited for alarms — or medium/high security in general. On the other hand, X10 is in principle appropriate for lighting control and similar
- Smart-Its can be used to realize a medium level of security, but this requires some implementation effort
- Some easy-to-use protocols for life cycle management in particular enrolment of new devices must be developed

Overall, the chosen technology will allow a proper level of security, albeit some development effort can be expected. The only exception being that X10 is not appropriate for realizing medium/high security. Finally — pending studies of user requirements — good solutions must be developed for enrolment as a part of life cycle management; however this is not specific to OSGi-based platforms, but applies to any platform.

[2] A security context consist of a scenario description together with an architectural description of the technology to be used to realize the scenario

3.4 Business Analysis

The change drivers are the environmental changes needed to push pervasive computing technology into the market. This includes a wish for privacy, safety/security, availability of micro payments, and use of high-speed Internet access for video and music on demand. If new technology is to enter the market, the pushed technology needs to be connected to user needs such as safety/security, entertainment, cost reduction (e.g. energy saving), and comfort.

From the point of view of business, the big step in adding value comes with complementors. Complementors engage in *value nets* which are the combination of existing and emerging independent value chains in the market, and describes the entire market as a whole. Figure 2 shows the value nets for the business model in the EPCiR case. Compared to Figure 1, the value nets defines which *roles* are connected to the architectural components, the Content Providers (CPs) and Service Provider roles, e.g., operating Service Provider components. Based on the value net business model, it is estimated that added value is

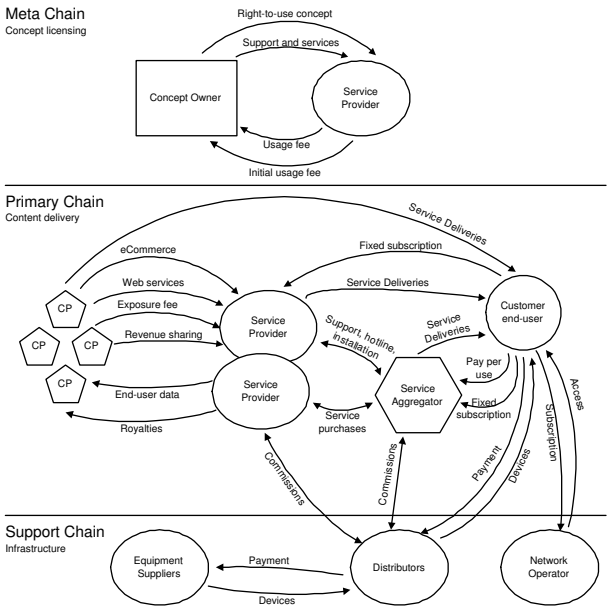

Fig. 2. Value nets in EPCiR. (Adapted from a figure ©Ericsson 2000)

distributed between the different roles with 60% to service providers, 35% to content providers, and 5% to the distributor role.

Benchmark of Business Model. The benchmark on the business model deals with comparing identified business opportunities of the value nets with the investigated technology. This first of all points to a number of areas that technology could be improved in order to enhance business opportunities. These include:

- *Standards.* Hardware — including descriptions of it — should be standardized in order to ensure interoperability
- *Actors.* One or more of the major telecommunications or network operator companies should enter the market and put the needed resources into development
- *Development horizon.* Different companies operates with different time horizons of varying lenghts. Actors bringing the technology to the market, should aggree on common development horizons

Taking this into account, we attempt to populate the roles in the value nets with existing companies. This part is specific to the market in question (here the Danish market) and not related here.

Based on this, we estimate that the market will be in its beginning in 2005. The major companies are expected to start investing and preparing for entrance to the market, but there will only be very little revenue at this early stage. By 2010, however, we expect the market to be increasing dramatically, because of several companies are working in the area, thus complementing each other and collectively adding value to users.

3.5 Overall Conclusions

The presented OSGi-based technology suffices for implementing the scenarios; part of this claim has been validated through experimental prototyping.

From the perspective of architecture, there are a number of areas in which custom development is needed. This development includes reflection capabilities (for self-description and efficient monitoring), better support for configuration and constraints, and support for moving OSGi services between nodes. From a security perspective, the OSGi platform provides flexible support for varying security requirements. The concrete security level of an application depends on its context of use, and the equipment deployed in the application must be appropriate for this level. This implies that there should be an way of assessing and certifying bundles and connected equipment introduced into the system. Moreover, the analysis points to a need for highly usable protocols for introducing devices into an existing system. And, finally, from a business perspective, the projected initial value in the value nets created by an introduction of a large OSGi infrastructure is relatively small in a local market as the Danish.

The issues mentioned here are not prohibitive for the implementation of the scenarios, but the combination of the three perspectives magnifies the problems. If efficient value nets of gateway operators, service providers, and providers of residential equipment has to be created, the individual value chains needs to be well integrated. This has implications for how important it is, e.g., to have standardized, self-describing bundles and equipment in the system. If this exists, services from different providers may potentially co-exist and co-operate, and if it does not exist, services such as remote monitoring of residential applications become difficult to create in general. Also, the importance of the usability architectural attribute may have large implications for the adoption of the technology and also — particularly combined with security issues — for long-term acceptance of the technology.

The evaluation as such does not point to whether a real-world implementation of the presented technology should be attempted or avoided. Rather, a natural next step would be to create exploratory prototypes based on a design of resolutions of the identified technological issues in order to assess the implications on the value chains.

4 Discussion

This paper has presented the results of an analysis and evaluation of a *specific* OSGi platform for a *specific* set of scenarios. This raises the question of whether and how the evaluation generalizes to other pervasive computing platforms and other applications. Most of the analyses are not specific to the chosen OSGi implementation, but primarily depends on properties of OSGi specification. We are currently evaluating different gateways and a different OSGi implementation for those gateways combined with different management solutions. We expect to find the same results for this setup. The analysis is, on the other hand, specific to OSGi-based platforms whereas the analysis approach would be usable for other types of pervasive computing platforms.

The scenarios represent a specific set of interactions with a future system. They of course do not cover all types of future emerging residential pervasive computing applications, but the specific scenario generation approach used ensures that a large number of environmental factors (such as available technology, emerging lifestyle, and politics) are taken into account and that fairly general scenarios are created. We also do not claim that the situations in the scenarios *will* come true, rather we take scenarios as given and

use well-known evaluation techniques for these assumed situations. Scenarios in various forms are, however, generally regarded as effective way of envisioning, designing, and discussing future systems across stakeholders [Rosson and Carroll, 2003].

The scenarios are independent of the evaluated platform in that they are created without assumptions of which type of platform or middleware that they will eventually be realized on. This means that they may be reused across evaluations of different pervasive computing platforms. The *refined* scenarios are, however, connected to an OSGi-based platform, but again independent of a specific implementation of that platform. And for a chosen technology, the refined scenarios tries to balance the need for evaluating detailed scenarios with resource constraints of an evaluation project. In the EPCiR project, the evaluations was to be done over a course of a few months and was estimated to use less than 20 man weeks for the evaluation part. This puts tight constraints on the amount of time available for each part of the evaluation — and in particular on prototyping. The refined scenarios represented, however, a reasonable balance between scope and available resources in that they cover much of the original scenarios and in that we were able to finish prototyping and analysis on time.

5 Summary

We have presented and discussed an evaluation of emerging, residential pervasive computing applications based on OSGi with a potential gateway operator as major stakeholder. The evaluation approach, *Pervasive Scenario Evaluations*, is multiperspective and anchored in future use through the application of use scenarios and experimental prototyping. The perspective employed are *architectural*, *security*, and *business* perspectives. We try to balance technological, social, and commercial issues in the evaluation through the specific approaches employed within the perspectives and through the combination of perspectives.

The main result of the evaluation is that the OSGi-based platform is indeed technically usable for a variety of residential pervasive computing applications, but that there are a number of technological and commercial challenges that need to be met. The commercial opportunities centers around the emergence and cooperation in *value nets* — connected value chains — which need to be supported by technology. This requires improvements in among other standardization of device description, monitoring capabilities, and usability of security measures of OSGi platforms.

References

[Barbacci et al., 2002] Barbacci, M. R., Ellison, R., Stafford, J. A., Weinstock, C. B., and Wood, W. G. (2002). Quality Attribute Workshops, 2nd edition. Technical Report CMU/SEI-2002-TR-019, Carnegie Mellon Software Engineering Institute.

[Bass et al., 2003] Bass, L., Clements, P., and Kazman, R. (2003). *Software Architecture in Practice*. Addison-Wesley, 2 edition.

[Brandenburger and Nalebuff, 1997] Brandenburger, A. M. and Nalebuff, B. J. (1997). *Co-Opetition: 1. A Revolutionary Mindset That Redefines Competition and Cooperation; 2. the Game Theory Strategy That's Changing the Game of Business*. Doubleday.

[Floyd, 1984] Floyd, C. (1984). A systematic look at prototyping. In Budde, R., Kuhlenkamp, K., Mathiassen, L., and Züllighoven, H., editors, *Approaches to Prototyping*, pages 1–18. Springer Verlag.

[Galt et al., 1997] Galt, Chicoine-Piper, and Hodgson (1997). *IDON Scenario Thinking: How to Navigate the Uncertainties of Unknown Futures.* IDON Ltd.

[Green et al., 2001] Green, P., Flynn, M., Vanderhagen, G., Ziiomek, J., Ullman, E., and Mayer, K. (2001). Automotive industry trends in electronics: Year 2000 survey of senior executives. Technical Report UMTRI report 2001-15, Ann Arbor, MI: University of Michigan Transport Research Institute.

[Hansen et al., 2003] Hansen, K. M., Larsen, S. B., Pagter, J. I., Østergaard Pedersen, M., and Thomsen, J. (2003). Pervasive scenario evaluations: A multiperspective approach for evaluating emerging pervasive computing technologies. Technical report, ISIS Katrinebjerg. `http://www.ooss.net/epcir/`.

[Moravec, 2003] Moravec, H. (2003). Robots, after all. *Communications of the ACM*, 46(10):90–97.

[OMG, 2003] OMG (2003). Unified Modeling Language specification 1.5. Technical Report formal/2003-03-01, Object Management Group.

[Rosson and Carroll, 2003] Rosson, M. B. and Carroll, J. M. (2003). Scenario-based design. In Jacko, J. A. and Sears, A., editors, *The Human-Computer Interaction Handbook. Fundamentals, Evolving Technologies and Emerging Applications*, pages 1032–1050. Lawrence Erlbaum Associates.

[Stajano, 2002] Stajano, F. (2002). *Security for Ubiquitous Computing*. John Wiley & Sons.

[Starner, 2002] Starner, T. E. (2002). Wearable computers: No longer science fiction. *IEEE Pervasive Computing*, 1(1):86–88.