



**Project no:** IST - 5 – 033563  
**Project acronym:** SMEPP  
**Project title:** Secure Middleware for Embedded Peer-to-Peer Systems

## Periodic Activity Report Year 2

Period covered: from M12 to M24 Date of preparation: 10/2007

Start date of project: September 2006 Duration: 3 years

Project coordinator name: Manuel Díaz  
Project coordinator organisation name: UMA Revision: 4<sup>th</sup> review



### Project Participants

Participant no.	Participant name	Participant short name	Country
1 (Coordinator)	Universidad de Málaga	UMA	Spain
2	Tecnomat, S. A.	TEC	Spain
3	Technische Universität Graz	TUG	Austria
4	Siemens AG	SIEM	Germany
5	Valtion Teknillinen Tutkimuskeskus	VTT	Finland
6	Università di Pisa	UPI	Italy
7	Telefónica I+D	TID	Spain
8	Institute for Infocomm Research	I2R	Singapore

### Coordinator Contact Details

The Project Coordinator is:

Dr Manuel Díaz  
 ETSI Informática  
 Universidad de Málaga  
 Málaga, 29071, Spain.  
 email [mdr@lcc.uma.es](mailto:mdr@lcc.uma.es);  
 tel +34 952131394; fax +34 952131397

### Web Site

The project website is available at <http://www.smepp.org/>

## Executive Summary

### Work Performed

The main efforts in the project during this second year have been devoted to producing a first running prototype of the SMEPP middleware. In order to achieve this, a previous phase of refinement of the software architecture and security concepts and algorithms was carried out.

The definition of the software architecture has required more effort than expected, because of the lack of understanding of the QADA methodology from some of the partners and some initial coordination problems in the group that had to carry out the main role in this task. After the first year review, the consortium as a whole took the necessary measures to overcome this initial problem, increasing the effort initially planned for this task. A meeting focused on software architecture was held in Pisa, involving the main stakeholders, to review the initial proposal presented in the deliverables of the first year. In this meeting, the methodology was clarified and a reviewed version of the initial conceptual software architecture was proposed. In addition, the main blocks of this conceptual architecture were assigned to the different groups of the project, depending on their expertise. The work on the architecture was coordinated by UMA and VTT and reviewed versions of the deliverables were presented on the intermediate review meeting held on Brussels on April 2008. After this intermediate review meeting, the task on evaluation of the software architecture was cancelled and a minor modification to the contract Annex I, including a reallocation and re-scheduling of the work was made. This modification is included as an Annex in this deliverable.

From the implementation point of view, the first step was the design of the Component Model and Run-time Component Framework. A first version of the model, its mapping to Java and the initial design of the framework were presented in deliverable D5.2.1, which was accepted in the intermediate review. The model is based on UM\_RTCOM, a generic model for embedded systems developed by the UMA group, although it has been thoroughly modified to cope with the particularities of a middleware component model and, more precisely, to the SMEPP software architecture.

In addition to the component framework, we have also worked on the design and implementation of the main building blocks of the middleware architecture. In this sense, we have analyzed the requirements related to the protocol design and a first version for the basic protocols needed in the middleware has been produced. The analysis and design of these protocols are described in deliverable D5.3.1 and D5.3.2.

A first integrated version of all the middleware components is now running on T3 devices, as part of the work of WP5.2. The implementation adaptation to T2 devices is near to its completion. The deliverable 5.2.2 includes the current state of the implementations as source and binary code and a report where the main implementation details of the different components are included. An important coordination effort has been achieved in order to produce this implementation. Each of the partners involved in WP5.2 has separately implemented one or more components based on the description provided in the concrete architecture deliverable. The components only interact through the predefined interfaces and by means of the run-time component framework. It is important to highlight that the security components were also integrated in this first version of the middleware (group management security services and secure routing).

The final integration work was carried out at the end of September in a meeting in Málaga. After this meeting, some modifications have been carried out to the different components in order to correct some bugs, but the final integration effort has not been very high, demonstrating that the proposed approach in the software architecture definition was appropriate for the type of project.

In the case of the security WPs, they have evolved as expected during this year producing both, theoretical and practical advances. In the case of Elliptic curve algorithms, a first implementation of the concepts developed in this task has been finished and is under evaluation. First tests showed that arithmetic on this curve can be implemented easily and efficiently on 16-bit devices (whereat long integer arithmetic is not necessary).

The work in *Secure Instruction set extensions* to improve the power- and energy efficiency of lightweight cryptographic devices was finished and the main results are described in the final version of D5.1.1.

The rest of the security related work has been focused on the implementation of the first version of the algorithms. For SMEPP light, a special interface was designed by I2R (*ICryptographicServices*) to get access to micaZ-implementations of AES and SHA1. The underlying implementation of AES is thereby based on an implementation of TUG. In addition, the proposed secure routing algorithms and the integration of these algorithms into the SMEPP Component Framework. Supported protocols are: OLSR, AODV, DSR and ARIADNE. Additionally to the PC-based version of all routing protocols, a PDA-based implementation was realized on a HP iPAQ hx4700. The components implementing the security services for groups have also been developed and integrated in the current implementation.

Finally, the work on the design of the validation applications has also started and a first version of the deliverables D6.1 and D6.2 has been released, even if the corresponding tasks started with some delay, due to the dependencies with WP3 and WP5.\* tasks. Some initial work on middleware validation has been achieved based on the TID prototype for the validation application.

## **Main results during the period**

- Refined version of the conceptual and concrete software architecture of the middleware.
- An adaptation of the generic software architecture to T1 devices (sensor networks) named SMEPP light
- Secure Instruction set extensions for T1 devices and demonstration of its use on an open controller platform (LEON).
- Elliptic curve algorithm implementation and validation
- Study of the requirements and design of the basic common protocols for SMEPP (service management, routing, group management, overlay management,...). This includes the development of some prototypes for the evaluation of the studied protocols (for instance as Secure Lime proof of concept prototype for the service management protocol)
- Implementation of symmetric and asymmetric cryptography primitives, including its integration in the corresponding implementations.
- Design and implementation of the middleware component framework
- Design and implementation of the first running SMEPP standard prototype, including the implementation of all the basic components (API, Routing, Overlay network, Service Management,...)
- Design and implementation of SMEPP light.
- Design and implementation of the middleware debugging and monitoring tool

## **Expected end results**

By the end of the project we expect to have:

- A new abstract model for EP2P systems and support tools for the analysis of the specifications from the first stages of the development (simulation, validation, ...)
- Tools for quality analysis methods that facilitate the selection and instantiation of a concrete software architecture depending on the types of devices and domain and on the specific quality of service requirements for the application.
- Design and implementation of a Component Based Framework to support the abstract service model
- Design and implementation of a set of components implementing the most important aspects of EP2P systems including, at least, security, reconfiguration and mobility.
- Design and implementation of a security infrastructure for EP2P systems.
- Integration of this infrastructure in the SMEPP middleware.
- Design and implementation of secure routing protocols.
- Design and implementation of cryptographic protocols and security primitives for EP2P systems.
- Implementation based on SMEPP of a set of P2P services on the existing Seguitel social and health care application
- Implementation based on SMEPP of a radiation monitoring application based on fixed and mobile sensors

**Plan for Using and Disseminating Knowledge**

The dissemination activities during this second year have continued as planned. The dissemination Plan/Report has been updated with the results of this second year and with the planned activities for the final year. We have obtained positive feedback from different industries and universities that have know about the SMEPP project.

## Table of Contents

1. Project Objectives and Major Achievements.....	9
1.1. Project Objectives.....	9
1.2. Recommendations from Previous Reviews .....	10
1.3. Work Performed, contractors involved and main achievements .....	12
2. Workpackage Progress.....	16
2.1. WP0: Management .....	16
2.2. WP1: EP2P Middleware and Applications Requirements .....	18
2.3. WP2: Abstract Service and Interaction Model.....	20
2.4. WP3: Software Architecture.....	23
2.5. WP4: Security Services .....	26
2.6. WP5.0: Implementation Coordination.....	28
2.7. WP5.1: Security Services Implementation.....	30
2.8. WP5.2: Middleware Framework Implementation.....	34
2.9. WP5.3: Network Specific Protocols and Infrastructure .....	38
2.10. WP6: Applications and Validation.....	40
2.11. WP7: Dissemination and Exploitation .....	42
3. Consortium Management .....	44
3.1. Project Status .....	44
3.2. Workplanning and timetable* .....	45
3.3. Overall Status of Deliverables .....	47
3.4. Progress towards Year 3 Objectives and Deliverables .....	48
3.5. Advisory Board .....	48
4. Annex I: Effort Table .....	50
5. Annex II: Changes to the DoW.....	54



# 1. Project Objectives and Major Achievements

## 1.1. Project Objectives

The main objective of this project is to develop a new middleware, based on a new network centric abstract model, specially designed for EP2P applications, and trying to overcome the main problems of the currently existing domain specific middleware proposals. The middleware will be secure, generic and highly customizable, allowing for its adaptation to different devices (from PDAs and new generation mobile phones to embedded sensor actuator systems) and domains (from critical systems to consumer entertainment or communication). Its suitability will be demonstrated by the development of two different innovative real-life applications in the domains of Context Aware Mobile Telephony and Environmental Monitoring in Industrial Plants

- **Objective 1. Abstract Service and Interaction Model** The aim is to provide a service oriented abstract model to program the interaction among peers, which hides low-level details treated by the support infrastructure. More specific objectives are:
  - The development of a quality oriented P2P service architecture that supports
    - self-configurable services of P2P environment
    - reconfigurable quality properties of services, and
    - scalability from tiny embedded devices with wireless connections to heterogeneous P2P networked systems.
  - To develop support for embedded P2P networking with
    - mechanisms that guarantee quality properties of services especially for the execution qualities such as reliability, performance and adaptability
    - communication services with special focus on self-organisation, mobility and service discovery and delivery, and
    - security services, that provide tools for the secure interaction between peers.
- **Objective 2 . Middleware Architecture and Infrastructure** . Design an implementation of a Component Framework, based on the abstract execution model for EP2P systems .The specific objectives in this area can be summarized in the following points:
  - Development of tools for quality analysis methods that facilitate the selection and instantiation of a concrete architecture depending on the types of devices and domain and on the specific quality of service requirements for the application.
  - Design and implementation of a set of components implementing the most important aspects of EP2P systems including, at least, security, reconfiguration and mobility.
- **Objective 3 . Security** . Traditional security infrastructures cannot easily be adapted to EP2P systems, since most of them are based on trustable servers that provide authentication and authorization. The goal is to develop security services for the middleware taking into the characteristics of this systems into account. More specific objectives in this area are:
  - Design and implementation of a security infrastructure for EP2P systems.

- Integration of this infrastructure in the SMEPP middleware.
  - Design and implementation of secure routing protocols.
  - Design and implementation of cryptographic protocols and security primitives for EP2P systems.
- **Objective 4 . Applications .** The goal of this task is the validation of proposals developed in the other activities which will be carried out in the context of the project. Chosen applications represent very different scenarios and will enable us to evaluate to what extent the proposals made in the project context are appropriate. Two validation applications will be developed:
    - A context aware mobile telephony base system on the field of telecare.
    - An environmental monitoring application in the context of nuclear power plants.

## 1.2. Recommendations from Previous Reviews

In this section we summarize the main recommendations of the two reviews held after the first year and the measures taken by the consortium to follow them:

From the first review the comments and measures taken by the consortium to cope with them can be summarized as follow:

- **R2.1:** Thoroughly review the architecture of the SMEPP middleware and comprehensively investigate related implementation. This includes extensive revision of WP3 deliverables D3.1 to D3.4.
  - ✓ The conceptual architecture was re-defined in a meeting in Pisa, just after the review. In this meeting, some problems related to the methodology were clarified and an initial partition of the work was carried out.
  - ✓ Each partner provided a revised version of the structural and behavioural models that were refined and integrated by UMA and VTT
  - ✓ A new version of the conceptual architecture was frozen and the work was concentrated on the concrete architecture.
  - ✓ The deliverables were nearly re-written in the exception of D3.4, where limited advances were achieved.
  - ✓ The results of the work carried out by the consortium were presented in the intermediate review.
- **R2.2:** Closely integrate the work carried out by each partner, in particular making sure that there is a sufficient level of collaboration. Integration should be mainly worked around the middleware architecture definition.
  - ✓ The consortium has worked as a whole in the development of the software architecture and implementation. Each partner has been in charge of defining its corresponding component in terms of its interaction with the rest of the components and has had to check the consistency of all the provided and used interfaces. This checking was carried out iteratively through all the definition of the middleware and finalized in the different coordination meeting held during this year (see description in WP0 activities).
- **R2.3:** Work actively towards the implementation of the SMEPP tools, middleware and security solutions.
  - ✓ Most of the effort of the entire consortium has been devoted to implementation (123 pm just in implementation, in addition to 56pm devoted to the re-definition of the architecture). At the end of the second year a first

- version of the SMEPP standard and light version was running. Both version incorporate the results from the security work-packages.
- **R2.4:** Clearly stress the contribution of the SMEPP project compared to state of the art in M12 and forthcoming deliverables. This in particular applies to WP4 deliverables.
    - ✓ We have tried to take into account this issue in all the deliverables. Moreover, the deliverables of WP4 were revised to include a new section at beginning of the document where the contributions are analyzed.
  - **R2.5:** Present more concisely the achievement of the project in forthcoming project reviews, avoiding repeating the content of the deliverables but rather highlighting key results and contributions.

The results and recommendations from the intermediate review for WP3 and the measures taken are the following:

- **R3.1:** The differentiation of the SMEPP middleware with respect to other related middleware should be put forward. Therefore, the architecture definition should exhaustively specify the role of the differentiating aspects (security mechanisms and processes, etc.) in its different components and layers.
  - ✓ The differences of the middleware approaches are discussed in each of the components of the middleware and in the component framework deliverable. The component model in which the middleware is based is very innovative, since it allows building and integrating different adaptation and monitoring tools, without affecting to the middleware components. This is an added value with respect to other existing middleware solutions. On the other hand, the architecture has demonstrated to be innovative, by permitting a smooth integration of the security aspects at the group and routing level without major impacts on the rest of the middleware components.
  - ✓ During these last months, the role of the software architecture has been re-defined. Since the task on software architecture analysis was stopped, the focus has been put in providing useful reference documents for the implementation. Changes in the interfaces and interaction have been incorporated to D3.3. The high-level behavioural description of deliverable 3.2 has been frozen in the M18 version. It will be updated once the first version of the implementation is running.
- **R3.2:** Work actively towards the implementation of the SMEPP middleware and security solutions; this will allow to progress also at architectural level.
  - ✓ See comment to recommendation 2.3.
- **R3.3:** The work on architecture evaluation (D3.4) is not considered to be neither at a satisfactory level nor key for achieving SMEPP main goals, and therefore it should be stopped. In its current state after half of the project, it remains a rather general work not specifically designed for this particular middleware. Initially planned resources for architecture evaluation, which is work of VTT partner, should be reallocated to the rest of activities of WP3 or even to other work packages **as requested by the project coordinator**.
- **R3.4:** Clear human resource commitment of all partners will be expected for the rest of the project. For next review, all partners will have to offer sufficient evidence of such commitment by producing the expected results as planned in the DoW. **This is specially requested for VTT partner.** After the project running for half of its duration, constant personnel resource reallocations have taken place in VTT, which has had a negative impact in the timeliness of results delivered by the activities, in

particular of WP3 and also a negative impact on the extra effort that other partners have had to allocate to such work. As reported by the VTT representative, the person with the appropriate expertise for the architecture evaluation work moved out of the project in the days previous to the review. In the light of the above recommendations, VTT should provide appropriate personnel resources with expertise to support the work in WP3 or other work packages **as requested by the project coordinator** (and not in architecture evaluation as this task is stopped).

- ✓ All the effort remaining effort from the work on architecture evaluation has been moved to WP5.2, where VTT has implemented the event management component and has worked towards the final implementation of the extension management.
- ✓ The rest of the effort will be devoted to the implementation of monitoring tools and OSGi integration.
- ✓ With respect to human resources, a new member from VTT has been working on the implementation of these components

### **1.3. Work Performed, contractors involved and main achievements**

**WP0 (UMA, UPI, TEC, TID, TUG).** During this period all the planned activities were carried out, including the steering committee meetings, the advisory board meeting and the review meetings. Several other internal meetings for the coordination of the work in software architecture and implementation were also organized. The effort spent by each partner was monitored during the all the year and reported in a task and person basis format, in addition to the WP effort consumption at month 20 and 24. The Management and Activity reports were delivered on time.

**WP1 (UMA, TEC, TID, VTT, TUG).** The deliverable D1.3 was revised to take into account the final requirements of the applications after the revision of the architectural drivers in deliverable 3.1 and their impact on the application requirements.

**WP2 (UPI, UMA).** A meticulous revision process of the service interaction model has been achieved. This work led to the specification of a new (refined) version of both the SMEPP primitives and of the format of the SMEPP service contracts. The main modifications are related to a stronger distinction between peers and services behaviour and the inclusion of a new asynchronous primitive for the reception of service invocation results. Both modifications came after a deep analysis of the examples, that was helped by the support tools. UPI also worked on the design of a service discovery architecture for embedded P2P systems. The discovery architecture builds on top of the DHT (Distributed Hash Table) technology and it adapts to varying network configuration. Both contribution have been reflected in the software architecture and in the implementation.

**WP3 (VTT, UMA, UPI, TEC).** The architecture has been fully revised. New versions of all the deliverables were produced in month 15 and 20, following the recommendations of the reviewers. In deliverable 3.1 the architectural requirements were refined and the methodology was clarified. Also the requirements were traced back to the ones produced in WP1. The conceptual architecture was collaboratively re-defined, providing a first step for the division of the work. The deliverable M15 version of deliverable D3.2 include all the views (structural, dynamic, deployment,...) required by the methodology. With respect to deliverable 3.3, in the version of M15 we provide a structural description of the components and component

framework. This view was completed in the M20 version, including a refined version of the dynamic view of D3.2. This was the starting point and architectural references for the first version of the implementation. These documents will be updated once the first version has been validated.

**WP4 (UMA, TUG, SIEM, I2R).** During this second year of the project, and focusing on D4.2 and D4.3, we have analyzed the suitability of security primitives for constrained devices and have discovered that the lowest device (sensor nodes) can support the necessary security primitives required by SMEPP. UMA also studied the key management protocols for high security protocols that should be used on SMEPP. Finally, public Key Cryptography has been the technique selected for SMEPP. New revised versions of D4.2 and D4.3 were produced on time. Key-management for groups intending to use cryptographic keys has been studied. The requirements and goals were defined and the “distributed” vs. the “centralized” approaches were compared. Furthermore the results of the standardizations groups of the IETF were studied and taken into account. The proposed key-management for groups is a scheme using a centralized approach (tree structure) and is based on the GSAKMP standard instead of the IETF (Group Secure Association Key Management Protocol, Internet Standard RFC4535). D4.4 was also produced in this period, providing power estimation-methodologies and the corresponding estimation tools.

**WP 5.0 (UMA, TEC, TID).** As the architecture work-package was finishing their tasks and implementation started, more and more interaction among component developers has taken place. Cooperation has taken place mostly through e-mail, but also the use of source code repository (Subversion) has been increasing constantly during this second year and is now a key tool for the implementation effort. Two implementation meetings that have taken place during this period: where we have tried to define those very concrete aspects of the implementation that are difficult to manage remotely. An *implementation integration* meeting is planned for the end of September. All the groups participating in implementation WPs are planned to work together during one week towards the validation and testing of the first prototypes. The deliverables corresponding to this WP were produced on time.

**WP 5.1 (UMA, TUG, SIEM, I2R).** This WP has been very active during this second year. In the field of *Secure Instruction set extensions for EP2P lightweight devices* we investigate into the field of instruction set extension to improve the power- and energy efficiency of lightweight cryptographic devices. The research was focused on a small set of strong cryptographic primitives. The results in this field have been presented in the revised version of D5.1.1 in M15.

With respect to the hardware support for asymmetric cryptography, we have developed the estimation tools proposed in WP4.

We have also worked on the design of new asymmetric cryptographic primitives, taking into account the limitations the hardware platforms. The focus was on scalable asymmetric cryptographic schemes to avoid complex long integer arithmetic. The chosen approach is based on elliptic curves over binary fields  $GF(2^n)$  and finite extension fields  $GF(p^n)$  where  $p$  needed to be optimized for the word length of the used processor platform.

The rest of the work has been focused on the implementation of the first version of the algorithms. For SMEPP light, a special interface was designed by I2R (*ICryptographicServices*) to get access to micaZ-implementations of AES and SHA1. The underlying implementation of AES is thereby based on an implementation of TUG. In addition, the proposed secure routing algorithms and the integration of these algorithms into the SMEPP Component Framework. Supported protocols are: OLSR, AODV, DSR and

ARIADNE. Additionally to the PC-based version of all routing protocols, a PDA-based implementation was realized on a HP iPAQ hx4700.

The components implementing the security services for groups have also been developed and integrated in the current implementation.

**WP 5.2 (UMA, VTT, UPI, TUG, TID).** The first step in the implementation was the adaptation of the UM-RTCOM model to the specific needs of a reconfigurable middleware. As a result a new component model, named SMCOM, was designed and implemented. This first implementation was the starting point for the integration of the different middleware components. The following step was to adapt the different components to the model. This task included the definition of the interfaces following SMCOM and the implementation of the component containers and interaction points. After the first iteration, the component model implementation and the mapping to Java has been modified.

In addition to the component framework, this work-package also includes the implementation of the main building blocks of the middleware architecture. A first integrated version of all these components is now a running on T3 devices. The implementation adaptation to T2 devices is near to its completion, since it is based on the optimization of the current implementation for the Java version of PDAs. The deliverable 5.2.2 includes the current state of the implementations as source and binary code and a report where the main implementation details of the different components are included.

Some work has also been achieved in the context of task 5.2.4 (Upgrading and Extension Support). A specific component of the middleware has been designed to allow extending the functionalities of the SMEPP Middleware by adding components to the Common Services-level of the architecture. The component basically acts as a bridge between the SMCOM and Extension frameworks. The integration of SMEPP and OSGi is also considered in the context of this task. Different possible integration alternatives have been analyzed in WP5.3 and the final adopted approach is being implemented and will be used in the final TID validation application.

With respect to *extra-functional support*, the focus of the work has been on the integration of security services and energy efficiency management in SMEPP light. This aspect has been thoroughly investigated in the security related WPs, since security encryption techniques may greatly affect energy consumption in sensor networks. The current implementation in the SMEPP light version incorporates some of the results of this research (see WP5.1). In addition, SMEPP Light includes an Energy Efficiency module that is responsible of turning off the radio when the node does not expect to send or receive data.

**WP 5.3 (UMA, TEC, TID, I2R).** We have analyzed the communication requirements of the two validation applications. In the case of the Home Systems and Mobile Telephony application, we assume that most users of the application will get connectivity through a residential gateway. SMEPP and OSGi integration has been studied and will be the basic solution to the interoperability problem. The residential gateway will behave as a common SMEPP node acting as gateway between home networks and external networks.

For the environmental monitoring application, SMEPP Light will be used on motes and other constrained devices. These devices would need to be connected to more resourceful nodes that would act as gateways, acting in behalf of the reduced devices and connecting them with the rest of the SMEPP network. More precisely, sensor nodes and, quite probably, worker nodes would be SMEPP Light nodes. Their gateways would be installed at the wireless routers and other network infrastructure devices that give them connectivity.

In the context of this WP we have also characterized the most usual protocols that will be used by the applications considering the requirements. We have also analyzed the availability of the different protocols on the devices considered for SMEPP. We distinguish between the different node types and the possible operating systems of each one. All the results of this initial step are summarized in D5.3.1.

The rest of the work carried out in the context of this WP during this second year has been devoted to the analysis and design of the basic supporting protocols of the SMEPP infrastructure. The results are all included in D5.3.2.

**WP6 (UMA, TEC, TID).** Most of the effort in this WP was devoted to the design of the validation applications that is included in the deliverable D6.1 and D6.2. This work has strong dependencies with the results of WP3 and WP5.\*. Even if some of the results of these WPs was delayed, the impact on the design was not too high due to the extra-effort that was put in the design of the requirement elicitation prototypes (see Year 1 Activity Report ).

The first version of the deliverables was ready on time, including the high level design of both applications. Some prototyping based on the current SMEPP implementation has also been carried out in order to test the initial version of SMEPP.

Another major contribution of this WP is the design and manufacturing of the new sensor board card that will be used in the prototype. This new card includes the radiation sensor, avoiding the necessity of the connection to a dosimeter, improving the range of application and deployment of the sensors.

**WP7 (UMA, TEC, TUG, SIEM, VTT, UPI, TID, I2R).** Most partners have contributed to scientific dissemination through publications in International Conferences and Journals. A total of 22 conference papers and 4 journals and book chapters has been published during this second year. The collaboration inside the consortium has been increased, with joint publications with UPI, TID, TEC and I2R. On the other hand, the major event during this year was the organization of the MIMES workshop in Dublin as an associated workshop to the Ubiquitous 2008 International Conference. The workshop was organized by UMA and UPI and all the papers were refereed by at least two relevant researchers in the field. Most of the partner presented some paper in this workshop.

We have obtained some feedback on the general impact of the project. For instance, SMEPP and its radiation monitoring application is referenced in the Crossbow page as a relevant application of their technology <http://blog.xbow.com/xblog/2007/12/radmote---mobil.html>. This page had a very large number of visits and since its publication we have received a lot of mails asking for details about the SMEPP project. The industrial partners have also increased their effort in dissemination in their fields, inside and outside the companies.

## 2. Workpackage Progress

### 2.1. WP0: Management

#### Workpackage Objectives

- The aim of this WP is to guarantee effective progress of the project, ensuring the correct development of the work-plan and providing the necessary liaisons between the consortium and the EU and controlling the quality of the work and deliverables. It will coordinate the rest of the control WPs, paying special attention to Exploitation and Dissemination activities and risk control.
- All the administrative and financial management, including conflict resolution will also be included in this WP

#### Starting Point

The requirements of the middleware and applications were established during the first year. Also the abstract interaction model and associated tools were finished on time. The basic security requirements and threat models were also ready. An initial software architecture was ready at the beginning of the year, but there was a delay in the WP3 tasks. The inputs from the reviewers about the work in the first year was positive, except with respect to the advance of this WP. The Advisory Board also provided positive inputs about the scope and overall status of the project.

#### Progress on WP0 in Year 2

The work devoted to coordination has been higher than planned during this second year. The main reason has been the extra-work required to produce the SMEPP software architecture. Following the recommendations of the reviewers after the first year review, the initial software architecture was fully revised. This required an extra meeting, which was held in Pisa (November 2007), just after the first year review, and where a re-assignment of the work to the partners involved in the definition of the software architecture was achieved. As this activity was recognized as a critical one for the project evolution, an important effort in the coordination of the work of the different partners was required during the following months. This effort included a leading role in the re-edition of the deliverables that were not accepted in the first year review and the preparation of the intermediate review that was held in Brussels in April 2008. Most of the partners collaborated in the re-definition of the software architecture, increasing their allocated effort. After the intermediate review meeting, the task on evaluation of the software architecture was cancelled and a minor modification to the contract Annex I, including a reallocation and re-scheduling of the work was made.

In addition, the originally planned meetings of the steering committee and technical/scientific coordination meeting were organized in Málaga (January 2008), Madrid (June 2008) and Dublin (July 2008). This last meeting was held jointly with the MIMES Workshop, which was organized by the groups of Málaga and Pisa as a main dissemination activity.

The first meeting of the advisory board was also held during this first year. The preliminary conclusions were presented during the first year review, but a deeper analysis based on anonymous questionnaires was carried out. The result of this meeting was very satisfactory and the main recommendations given by the board have been taken into account during this period. The next advisory board meeting is planned for December 2008, just after the second year review

**Deviations from project workprogramme for WP0**

No important deviation in this WP occurred during this first year, except some extra effort on the coordination of WP3 and WP5.2.

**List of Deliverables (WP0)**

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Estimated indicative person-months</b>	<b>Used indicative person-months</b>	<b>Lead contractor</b>
D0.2	Annual Management Report	0	M24	M25	3	3	1
D0.5	Annual Activity Report	0	M24	M25	3	3	1

**List of Milestones (WP0)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM0/24	Annual Management and Activity Reports	0	M24	M24	UMA
WM 0/18	Intermediate Activity Reports	0	M6	M6	UMA

## **2.2. WP1: EP2P Middleware and Applications Requirements**

### **Workpackage Objectives**

- This WP is in charge of collecting the middleware requirements, taking into account generic EP2P characteristics and the validation applications.
- The generic requirements will be obtained from a deep study of the state of the art on middleware for EP2P systems and from the analysis of the applications. The concrete application requirements will also be specified in this WP. Particular attention will be paid to extra functional requirements that will be derived from the type of devices and networks considered.
- As mentioned in section 7.1.1, an iterative incremental approach to project development will be followed. This will allow better adaptation to imprecise or changing requirements. As P2P technology and applications are in continuous evolution we think that this approach is the most appropriate for this type of project.
- The requirements WP will therefore span during most of the project duration, although with much more effort in the initial phases of the project.

### **Starting Point**

From the 1<sup>st</sup> year Activity Report:

“All three tasks in the work package have performed most of their expected work in this this period. The expected deliverables have been produced and prototypes have been built. Some additional effort is expected during the first months of second year in order to update the deliverables with the information obtained from other work-packages.”

### **Progress on WP1 in Year 2**

As the main versions of all three deliverables were accepted in the first year, only minor work has taken place in this work-package. Final versions of the three deliverables are now available and no more work is expected in this work-package.

The main work this workpackage has been focused on the review of the revised version of deliverable D1.3 and more concretely on checking the consistency of the requirement mapping between the software architecture and the global SMEPP requirements, including those related to security and generic middleware requirements. TID analyzed the expected services and the possibilities of the defined SMEPP architecture middleware in order to refine the application requirements. Moreover, with respect to the application itself, Telefonica's interests were revised in order to check that the proposed services match the future perspectives in the eHealth area.

The work-package is considered finished now.

### **Deviations from project workprogramme for WP1**

No significant deviations have taken place in this work-package during this second year.

**List of Deliverables (WP1)**

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Estimated indicative person-months</b>	<b>Used indicative person-months</b>	<b>Lead contractor</b>
D1.3	Application Requirements Final Version	1	M12	M21	4	3,5	TEC

**List of Milestones (WP1)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM1/15	Revised versions of middleware and security requirements	1	M15	M15	TEC
WM1/18	Application requirements defined	1	M18	M18	TEC

## 2.3. WP2: Abstract Service and Interaction Model

### Workpackage Objectives

The aim of this WP is to define an abstract service model, on top of which EP2P applications will be developed. The abstract model establishes how to discover and interact with (available) services. A specific objective of the service model is to provide a suitable level of abstraction to application developers, hiding the details concerning all the supporting implementation (including the underlying software architecture).

### Starting Point

#### Workpackage Objectives

In period M12-M24, the principal aim of WP2 was to define the way in which peers can locate the services (i.e., service instances) available. A major issue was to design a service discovery mechanisms able to deal with situations typically related to embedded P2P systems, such as, e.g., continuous connections and (unanticipated) disconnections of devices and availability of limited resources.

### Starting Point

At the end of M12, the first version of the service interaction model – identifying primitives for group, service and event management – was defined (D2.1). A first version of the format of SMEPP service contracts was also available, including a compositional language (SMoL) for the specification of peers and services behaviour. Software and concrete architecture of the SMEPP middleware (D3.2, D3.3) were in the early stages.

### Progress on WP2 in Year 2

At M13, UPI started a meticulous revision process of the work on WP2 achieved in the first year of the project (viz., the definition of the (first version of the) service interaction model), which led to the specification of a new (refined) version of both the SMEPP primitives and of the format of the SMEPP service contracts.

As far as the SMEPP primitives are concerned, two main novelties are:

- a stronger distinction between peers and services behaviour. Peers manage groups, and (un)publish services, services provide operations, while both discover and invoke services, and manage events. The SMEPP primitives can be hence classified in three separate groups: primitives available to peers only (viz., `createGroup`, `getGroups`, `joinGroup`, `leaveGroup`, `getGroupDescription`, `getIncludingGroups`, `getPublishingGroup`, `publish`, and `unpublish`), primitives available to services only (viz., `receiveMessage` and `reply`), and primitives available to both peers and services (viz., the rest of the SMEPP primitives).
- a new `ReceiveResponse(id, operationName)` primitive, needed to introduce the non-blocking invocation of *request-response* operations. A `returnResult` boolean parameter of the `invoke` primitive allows to specify the `invoke` behaviour: blocking,

if `returnResult` is true, non-blocking if `returnResult` is false (as default). In the latter case (viz., `returnResult` set to false or not specified), the `invoke` caller unlocks just after the provider invokes the `receiveMessage` primitive, and it can later retrieve the response by invoking the new `receiveResponse` primitive.

Note that the strong distinction between peers and services behaviour introduced in the service model required a careful revision of the specification of (pre-defined) exceptions (e.g., an `invalidCall` exception is raised whenever a service invokes an operation available to peers only) and input parameters (e.g., a services is not be able to specify a group identifier, since it implicitly refers the group it is published in) of the SMEPP primitives.

As far as the SMEPP service contracts are concerned, two major novelties are:

- removal of the service grounding from service contracts (groundings are now only available to providers, which are in charge of actually invoking the service operations).
- new (revised) XML schemas, providing a better support for ontologies and SMoL behaviour specifications.

In the period M13-M24, UPI also worked on the design of a service discovery architecture for embedded P2P systems. The discovery architecture builds on top of the DHT (Distributed Hash Table) technology and it adapts to varying network configuration, indeed dealing with connections and (unanticipated) disconnections of devices. Briefly, within each group, peers are organized into a DHT. Service contracts are distributed among peers w.r.t. their hash value, which is computed by taking into account a set of basic parameters (viz., service name, service category and the identifier of the group where the services is going to be published). A TTL-based mechanisms is employed to renew service contracts and to remove the contracts of those services whose providers are no more available. Services are discovered in two steps. First, all the services whose hash value is equals to the hash value of a given contract template (i.e., a (partially specified) service contract) are retrieved. Then, a syntactic or enhanced (i.e., ontology and/or behaviour-based) matching algorithm is to be run to filter those service contracts which (fully) matches the required constraints. A general description of the discovery architecture has been presented in the MIMES 2008 workshop.

### List of Deliverables (WP2)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D2.1	Service model description	2	M15	M15	9	7.9	UPI
D2.2	Tool Support for the service model	2	M15	M15	2	1.5	UMA

**List of Milestones (WP2)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM2/16	Service model description and updated tool support	2	15	16	UPI

## **2.4. WP3: Software Architecture**

### **Workpackage Objectives**

The objectives were to continue defining the conceptual EP2P middleware architecture (D3.2) and concrete architecture for an extended set of middleware services (D3.3), and their evaluation (D3.4)(V2)

### **Starting Point**

First versions of Architecture specific requirements (D3.1) had been proposed, Conceptual EP2P middleware architecture (D3.2) and concrete architecture for a selected set of middleware services (D3.3) and their evaluation (D3.4) (V1) had been proposed.

### **Progress on WP3 in Year 2**

The architecture requirements deliverable D3.1 was refined to more clearly identify the architectural drivers of SMEPP middleware, and to show how the SMEPP requirements were reflected in the proposed architecture. The structure of deliverable was also revised.

A workshop to refining the conceptual architecture was held in November 2007 and the partners responsible for implementing various architecture components worked scenarios related to the components. The inconsistencies between scenarios were checked and Conceptual architecture model and deliverable was compiled by VTT and UMA based on refined versions of the proposed scenarios provided by the different partners.

In the evaluation task, the requirements were classified and analysed in order to recognize which of them were the most important from the perspective of various quality attributes analysed, and preliminary analysis of conceptual architecture performed for those quality attributes.

A workshop was held in January 2008 in which the abstract SMCOM component model proposed by UMA was accepted as base of defining the concrete interfaces. Based on the scenarios in conceptual architecture, each responsible partner proposed the concrete interfaces for the components they were responsible and the results were gathered into revised concrete architecture document edited by VTT.

The iterated deliverables were presented in architecture review meeting in April in Brussels.

After the review the work on new iteration of architectural interfaces was started in order to propose refinements to the component interfaces and their required and provided functionalities, and to find out the inconsistencies between components.

An implementation workshop was held in Madrid in May 2008 in which the architecture descriptions were updated according to changing requirements coming from the

implementations. Updated versions of the Conceptual Architecture (D3.2) and the Concrete Architecture (D3.3) were proposed to reflect the changed requirements. The consortium also agreed on the re-structuring of the deliverables to make them easier to read and maintain. In this sense, the behavioural description of the architecture was further refined and included in D3.3, as the main reference component interaction. This will be the reference behavioural description of the architecture during the implementation. The conceptual dynamic view of the architecture will be updated once the final concrete architecture description has been frozen.

### Deviations from project workprogramme for WP3

The work on evaluation task WP3.4 was stopped after the architecture review meeting in Brussels at 9 of April and the work on deliverable D3.4 was frozen

### List of Deliverables (WP3)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D3.2	Conceptual architecture of secure EP2P middleware	3	M12/M20	M15/M20	12	15,3	VTT
D3.3	Concrete architecture of secure EP2P middleware services	3	M12/M20	M15/M20	26	29,3	VTT
D3.4	Evaluation results of EP2P middleware arch. and service model	3	M12/M20	M18/ Cancelled	9	6,2	VTT

**List of Milestones (WP3)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM3/8	Architecture specific requirements (D3.1) and conceptual EP2P middleware (D3.2)	3	8	15	VTT
WM3/12	Conceptual EP2P middleware architecture (D3.2), a specific architecture for a selected set of middleware services (D3.3) and their evaluation (D3.4) (V1)	3	M12/20	M15/M20	VTT
WM3/20	Conceptual EP2P middleware architecture (D3.2), a specific architecture for a selected set of middleware services (D3.3) and their evaluation (D3.4) (V1)	3	M2/20	15-Cancelled	VTT

## **WP4: Security Services**

### **Workpackage Objectives**

This WP is in charge of defining new security services for EP2P. Its primary objective is to design new non-centralized authentication and authorization mechanisms. Authentication will be based on self-signed certificates and grouping. Grouping is the basic technique used in serverless environments for certificate management. Group security services will also be included in this WP.

The main objective for this period was to use the existing research already made public in tasks 4.2 and 4.3 to justify security design decisions such as using public key cryptography and developing a transversal layer for the SMEPP architecture. Besides, we needed to investigate a power estimation methodology for secure algorithms and protocols in embedded networks (Task 4.4). Note that we also needed to revise the first version of D4.2 and D4.3 according to the requirements of the commission.

### **Starting Point**

As a starting point, we used the finished (revised) versions of D4.2 and D4.3.

### **Progress on WP4 in Year 1**

During this second year of the project, and focusing on D4.2 and D4.3, we have analyzed the suitability of security primitives for constrained devices and have discovered that the lowest device (sensor nodes) can support the necessary security primitives required by SMEPP. UMA also studied the key management protocols that should be used on SMEPP, based on previous analyses and it was established that public Key Cryptography is a good candidate for high security levels. Furthermore the integration of the security mechanisms inside software and network architectures was analyzed. As a result of this analysis it was concluded that it would be advantageous to use a transversal layer for containing the security components in the SMEPP architecture.

Task 4.4 is strongly related to task 5.1.2, since both tasks deal with the design of power estimation methodologies and the corresponding estimation tools. From the design perspective, T5.1.2 and T4.4 cannot be clearly separated. Thus, TUG carried out some work during T5.1.2, which was actually more related to WP4. Results of this “additional” work and methods to evaluate power- and energy estimation were presented in D4.4. Task 5.1.2. is therefore the practical counterpart to 4.4, and deals with the practical application of the power estimation methodologies. Practical results achieved so far have also been included in D4.4. While work on software-based approaches in this context was more or less done from scratch, TUG could also profit from prior knowledge (generated in the EU-funded project SCARD) in the field of energy and power estimation for hardware-based solutions.

The main effort from SIEM in this WP was focused on task 4.3 (Key-Management for groups). Siemens developed a key-management for groups intending to use

cryptographic keys. In the document produced they compared first a key-management referring to only 2 parties with a key-management referring to a dynamic group of at least 3 members and pointed out the significant differences which are the scalability of the group and the optimal key update within the frame of an effective “Join-and-Leave”-Policy. The requirements and goals were defined and the “distributed” vs. the “centralized” approaches were compared. Furthermore the results of the standardizations groups of the IETF were studied and taken into account. The proposed key-management for groups is a scheme using a centralized approach (tree structure) and is based on the GSAKMP standard instead of the IETF (Group Secure Association Key Management Protocol, Internet Standard RFC4535)

#### Deviations from project workprogramme for WP4

None.

#### List of Deliverables (WP4)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D4.3	Security Protocols for EP2P systems	4	M24	M9	9	8,8	1
D4.4	Power estimation methodology for secure algorithms and protocols in embedded networks	4	M18 M24	M18 M24	6	6	1

#### List of Milestones (WP4)

Milestone no.	Milestone name	Workpackage no.	Date due	Actual/Forecast delivery date	Lead contractor
WM4/10	Basic security services and protocols defined	4	M4/24	24	UMA

## 2.5. WP5.0: Implementation Coordination

### Workpackage Objectives

- This WP will be in charge of the coordination of the three implementation WPs. Its main function will be to elaborate and monitor the detailed iteration work-plans for each of the implementation WPs, including version planning and control.
- The plans will try to prevent any duplication of work, detecting common components in the different sub-packages and allocating the requirements to the sub-packages in a coordinated manner.
- The risks analysis derived from the implementation and the coordination between the middleware development teams and the validation and application teams will also be a task of this WP.

### Starting Point

From the Activity Report of 1<sup>st</sup> year:

“In this year, the Configuration Management and Version Planning Deliverable has been produced and the initial infrastructure for the Configuration Management System has been installed. This consists of a Version Control System for source code (CVS) and a Cooperative Work support tool (BSCW) for documents.

These tools have been installed at the facilities of University of Málaga.”

### Progress on WP5.0 in Year 2

As the architecture work-package was finishing their tasks and implementation started more and more interaction among component developers has taken place. Cooperation has taken place mostly through e-mail, but also the use of source code repository (Subversion) has been increasing constantly during this second year and is now a key tool for the implementation effort.

It is also important to mention the two implementation meetings that have taken place during this period:

- Madrid (May 2008)
- Dublin (July 2008)

In this implementation meeting we have tried to define those very concrete aspects of the implementation that are difficult to manage remotely. The meetings followed a very similar structure, with an overall presentation of the status of the implementation work and main issues identified. Then each of the components responsible presented the status and the component and a more detailed description of existing issues. After these presentations, different work-groups were defined with a concrete agenda for the whole meeting. Each of these groups presented their conclusions and results in the second day of the meeting, with a concrete planning for the next iteration.

An *implementation integration* meeting is planned for the end of September. All the groups participating in implementation WPs are planned to work together during one week towards the validation and testing of the first prototypes.

**Deviations from project workprogramme for WP5.0**

Although a slight delay exists for implementation due to late finish of preceding work-package (WP3: Architecture) no major deviations are foreseen as first version of middleware is already available.

**List of Deliverables (WP5)**

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Estimated indicative person-months</b>	<b>Used indicative person-months</b>	<b>Lead contractor</b>
D5.0.2	Implementation Progress Plan	5.0	M18-M24	M18-M24	2	2,5	2

**List of Milestones (WP5)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM5/18/24	Implementation Progress Reports.	5	M5/18-M5/24	M18-M24	TEC

## 2.6. WP5.1: Security Services Implementation

### Workpackage Objectives

This WP is in charge of the implementation of the security infrastructure including, authentication mechanisms, secure routing protocols, key distribution algorithms and cryptographic protocols. All these developments must finally be integrated in the middleware implementation. This WP will also analyze the design of secure hardware modules for those cryptographic operations with heavy computing requirements.

### Starting Point

For this second year the starting point for the different sub-objectives are the following:

#### T5.1.1. Secure Instruction set extensions for EP2P lightweight devices

In T5.1.1. we started with some prior knowledge about instruction set extension carried out at TUG by Stefan Tillich, Johann Großschädl, and Alexander Szekely as well as work by other research groups. Some prior papers presented in this field of research are:

- Johann Großschädl and Erkey Savas. Instruction Set Extensions for Fast Arithmetic in Finite Fields  $GF(p)$  and  $GF(2^m)$ . In Cryptographic Hardware and Embedded Systems — CHES 2004, vol. 3156 of Lecture Notes in Computer Science, pp. 133–147. Springer Verlag, 2004.
- Stefan Tillich and Johann Großschädl. Instruction Set Extensions for Efficient AES Implementation on 32-bit Processors. In Cryptographic Hardware and Embedded Systems — CHES 2006, vol. 4249 of Lecture Notes in Computer Science, pp. 270–284. Springer Verlag, 2006.
- Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta. Architectural Extensions for Elliptic Curve Cryptography over  $GF(2^m)$  on 8-bit Microprocessors. In Proceedings of the 16<sup>th</sup> IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2005), pp. 343-349. IEEE Computer Society, 2005.
- Stefan Tillich and Christoph Herbst. Boosting AES Performance on a Tiny Processor Core. In Topics in Cryptology - CT-RSA 2008, Proceedings of the Cryptographers' Track at the RSA Conference 2008, vol. 4964 of Lecture Notes in Computer Science, pp. 170–186. Springer Verlag, 2008.

#### T5.1.2. Secure HW-module for asymmetric cryptography

This task is mainly the practical counterpart to T4.4 of WP4, and deals with the practical application of the power estimation methodologies described in D4.4. The practical results achieved so far have also been included in D4.4 to serve as a validation of the introduced methodologies. While the work on software-based approaches was more or less done from scratch, TUG had some prior knowledge in the field of energy and power estimation for hardware-based solutions in the context of the EU-funded project SCARD.

#### T5.1.3. Design of new asymmetric cryptographic primitives

Siemens had some prior knowledge in this field of research - gained during prior activities.

#### T5.1.4. Implementation of symmetric and asymmetric algorithms

This task started in month 19. Thus, the amount of new achievements in the case of LEON-based processor platforms is limited. But especially in this task, we can fall back onto prior knowledge on cryptography processor extensions, mostly gained during the nationally-funded ISEC project (Austrian FWF):

- ISEC Project Website: <http://www.iaik.tugraz.at/content/research/vlsi/isec/>

Furthermore, TUG has also extensive prior knowledge regarding side-channel attacks and countermeasures both for software-based and hardware-based solutions:

- TUG IAIK's SCA Laboratory website:  
[http://www.iaik.tugraz.at/content/research/implementation\\_attacks/](http://www.iaik.tugraz.at/content/research/implementation_attacks/)

In the field of P2P routing protocols, we did not have any noteworthy expertise. Actually, we started from scratch – but we started very early in the project to have a prototype available in M19 which is the actual starting point for T5.1.4.

#### T5.1.5 Elliptic curve construction algorithm

Siemens had some prior knowledge in this field of research - gained during prior activities.

### Progress on WP5.1 in Year 2

The WP5.1 objectives for the period M12 – M24 can be divided into 5 sub-objectives according to the corresponding tasks in this work package:

#### T5.1.1. Secure Instruction set extensions for EP2P lightweight devices (M13 – M15)

This task was a short task in time with the intention to investigate into the field of instruction set extension (ISE) to improve the power- and energy efficiency of lightweight cryptographic devices.

The main idea was to accelerate the computing of cryptographic processes by keeping the flexibility of the implementation (e.g. in the case of using different key sizes or different modes of operation).

Since time for this task was limited (only 3 months) the investigations were limited to a small set of strong cryptographic primitives:

- ECC for asymmetric crypto: *both  $GF(p)$  and  $GF(2^m)$*
- AES for symmetric crypto

Results of T5.1.1. have been presented in D5.1.1., which was already delivered in M12 (Rev.1) and M15 (final Rev.).

#### T5.1.2. Secure HW-module for asymmetric cryptography (M15 – M24)

The objective of this task was to develop an estimation tool, which allows an accurate power- and energy estimation on all levels of the design process. While T5.1.2 is responsible for the development of such a tool, T5.1.2 is highly related to T4.4, which deals with the design of estimation-methodologies. But since T5.1.2. and T4.4 can not be clearly separated, TUG carried out some work which is related to WP4. Results of this work and methods to evaluate power- and energy estimation were presented in D4.4.

#### T5.1.3. Design of new asymmetric cryptographic primitives (M13 – M20)

The objective of T5.1.3. was to develop cryptographic protocols taking into account the limitation of heterogeneous platforms (e.g. 8-bit vs. 16-bit processors). The focus

was on scalable asymmetric cryptographic schemes to avoid complex long integer arithmetic. The chosen approach is based on elliptic curves over binary fields  $GF(2^n)$  and finite extension fields  $GF(p^n)$  where  $p$  needed to be optimized for the word length of the used processor platform.

#### T5.1.4 Implementation of symmetric and asymmetric algorithms (M19 – M24)

The objective of T5.1.4 was the efficient implementation of ECC and AES. One main objective in the time period M12 – M24 was the use of instruction set extensions (ISE) on an open controller platform (LEON). Based on this platform, the capability of ISE was demonstrated.

A special interface was designed by I2R (*ICryptographicServices*) to get access to micaZ-implementations of AES and SHA1. The underlying implementation of AES is thereby based on an implementation of TUG.

The second part of T5.1.4 was devoted to:

- The design of secure routing algorithms and the integration of these algorithms into the SMEPP Component Framework (SMCOM). Beside a permanent adopting process (*since SMCOM and other middleware components changed very frequently*), the integration of all supported routing algorithms were completed. Supported protocols are: OLSR, AODV, DSR and ARIADNE. Additionally to the PC-based version of all routing protocols, a PDA-based implementation was realized on a HP iPAQ hx4700.
- Implementation of other security components of the architecture (group services and communication services):
  - The first set of protocols that are needed are the authenticated key exchange (AKE) protocols, where a certain peer (client) authenticates itself to another peer (server) and obtains the session key of the group. We have developed an AKE protocol for the security level 1 (authentication through shared symmetric key) based on the ISO 9798-2 protocol.
  - For the encryption and decryption of messages, we have implemented mechanisms for the security layer 2 (authentication and confidentiality/integrity).

#### T5.1.5 Elliptic curve construction algorithm (M3 – M24)

While the objective of T5.1.3 was to design new cryptographic primitives, this task starts from the assumption that an EC-based scheme (defined over  $GF(p^n)$ ) can be a promising solution. Based on this assumption, the objective of T5.1.5 was to develop an algorithm to classify curves in  $GF(p^n)$ . A first result of T5.1.5 was the decision to chose a Koblitz-type curve where  $p$  is in the range  $2^{15} < p < 2^{16}$ .

The idea was to get an adequate first solution for this problem and to start with benchmark testing very early.

For this first solution, an elliptic curve  $E: Y^2 = X^3 + aX + b$  (with  $a = 0x5348$  and  $b = 0x2ebe$ ) was chosen. First tests showed, that arithmetic on this curve can be implemented easily and efficiently on 16-bit devices (whereat long integer arithmetic is not necessary).

### Deviations from project workprogramme for WP5.1

Up to now, there are no notable delays from the project work planning and timetable. The only notable deviation is that some additional work in WP3 was done (T3.1, T3.2, T3.3) to define the specific requirements of the EP2P architecture as well as to define the specific architecture of a secure EP2P middleware. Results left its mark in contributions to D3.1 (M8), D3.2 (M8, M12) and D3.3 (M12).

### Deviations from project workprogramme for WP5.1

Some of the work of WP 5.1 has been carried out earlier than planned in order to support the research effort of WP 4 (“Security Services”).

### List of Deliverables (WP5.1)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D5.1.1	Spec. of Secure Instruction Sets fpr EP2P Devices	5.1	M12	M15	14	15	TUG

### List of Milestones (WP5.1)

Milestone no.	Milestone name	Workpackage no.	Date due	Actual/Forecast delivery date	Lead contractor
WM51/15	Specification of Secure Instruction Sets	5.1	15	12	TUG

## **2.7. WP5.2: Middleware Framework Implementation**

### **Workpackage Objectives**

#### **Objectives**

This is devoted to the design and implementation of a component framework to support the software architectures developed in WP3. It must not be seen as a closed middleware implementation, but as a highly customizable framework integrating a minimal set of component concepts (containers and ports for component interaction, support for dynamic deployment and binding of components, packaging and distribution, etc.) with a very small software footprint. This framework will be initially based on the results of the RUNES project, but it will require an adaptation to the P2P service interaction model defined in WP2.

#### **Starting Point**

The SMEPP software architecture deliverables and the study and evaluation of different component frameworks carried out in D1.1 and the initial analysis tasks carried out in this WP during the first year of the project.

After this study, the use of RUNES results was shown to be very difficult and the consortium decided to build a specific framework for SMEPP. This framework is based on UM-RTCOM, a previous work of the UMA on a generic component model for embedded systems.

#### **Progress on WP5.2 in Year 2**

Due to the fact of the limited reuse of other results, the scope of this WP was redefined, and it now includes the development of the framework and tools, in addition to the basic components of the middleware (i.e. those not directly related to security, which are implemented in WP5.1, and the those heavily dependent on the type of device or network used, implemented in WP5.3).

The first step in the implementation was the adaptation of the UM-RTCOM model to the specific needs of a reconfigurable middleware. Some basic model concepts had to be re-defined to cope with the particularities of a middleware component model and, more precisely, to the SMEPP software architecture. As a result a new component model, named SMCOM, was designed and implemented. The initial design and implementation and the model mapping to the Java language were presented in the first version of D5.2.1, which was accepted in the April review meeting.

This first implementation was the starting point for the integration of the different middleware components. The first step was to adapt the different components to the model. This task included the definition of the interfaces following SMCOM and the implementation of the component containers and interaction points. This was a difficult and time consuming task due to the constraints imposed in the communication and synchronization of the component threads. These constraints are basic to allow for the latter analysis of non-functional properties, although they make it more difficult the implementation in some cases.

During the first iterations, several proposals were made by different component implementers in order to make it easier and/or more efficient the framework. These proposals were discussed and a lot of them were included, leading mainly to the modification of the Java

mapping, providing more powerful primitives and to a better implementation. Of course, these first iterations were also very useful to debug the run-time system. As a result, the component framework implementation is quite stable and all the components are now interconnected through the framework. The new version of deliverable 5.2.1 includes all the modifications to the component framework and analysis tools up to the end of September 2008. No major modifications of the framework implementation are foreseen, at least in the case of T3 devices.

In addition to the component framework, this work-package also includes the implementation of the main building blocks of the middleware architecture. A first integrated version of all these components is now running on T3 devices. The implementation adaptation to T2 devices is near to its completion, since it is based on the optimization of the current implementation for the Java version of PDAs. The deliverable 5.2.2 includes the current state of the implementations as source and binary code and a report where the main implementation details of the different components are included.

Besides the tasks devoted to the implementation of the basic components of the middleware, this WP also includes other tasks related to *extra-functional properties support, extension support* and the *associated tools*.

In the case of task 5.2.4 (Upgrading and Extension Support), a specific component of the middleware has been designed to allow extending the functionalities of the SMEPP Middleware by adding components to the Common Services-level of the architecture. A modified component framework is implemented for the extension components to allow dynamic and late binding of interfaces and flexible declaration of events. The component basically acts as a bridge between the SMCOM and Extension frameworks.

The integration of SMEPP and OSGi is also considered in the context of this task. Different possible integration alternatives have been analyzed in WP5.3 and the final adopted approach is being implemented and will be used in the final TID validation application.

With respect to *extra-functional support*, the focus of the SMEPP proposal was on the integration of security services and network quality. From the security point of view, security was taken into approach from the very beginning of the project and it is now integrated into the current SMEPP and SMEPP light versions of the middleware. Quality of service has also been taken into account in the design. The specification can be achieved in terms of service contracts and the component model has been designed to be able to analyze and monitor the real-time behaviour of all the components, including those related to basic communication support (adaptation layer, routing and SHLC). The activities related to the integration of quality of service aware protocols in the middleware are planned for the final year (from a more theoretical point of view in WP5.3 and from the implementation point of view in this WP).

Another important aspect related to extra-functional support that has been considered in SMEPP is energy efficiency management. This aspect has been thoroughly investigated in the security related WPs, since security encryption techniques may greatly affect energy consumption in sensor networks. The current implementation in the SMEPP light version incorporates some of the results of this research (see WP5.1). In addition, SMEPP Light includes an Energy Efficiency module that is responsible of turning off the radio when the node does not expect to send or receive data. The main activities that can be executed in SMEPP Light are group operations (discovery existing groups, join or leave a group, and

subscription/event operations (receive the values corresponding to subscribed events, unsubscribe events). All the group support algorithms for SMEPP light interact with this module in order to minimize energy consumption.

The implementations of these concepts are already available in the SMEPP light implementation. With respect to deliverable D5.2.3, which is identified as a prototype in the DoW, the current efforts corresponding to this deliverable are integrated in the SMCOM prototype and the SMEPP light implementation. Even if there is no report associated to this deliverable, the details are explained in the rest of the reports of this WP. It is expected to provide a report by the end on the project summarizing the main SMEPP innovations in this area.

### **Deviations from project workprogramme for WP5.2**

The first version of the implementation was finished with a delay of ~ 1 month.

**List of Deliverables (WP5.2)**

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Estimated indicative person-months</b>	<b>Used indicative person-months</b>	<b>Lead contractor</b>
D5.2.1	Component and Infrastructure design	5.2	M18 M24	M18 M24	6	8	UMA
D5.2.2	Component Infrastructure and Tool Implementation	5.2	M24	M24	10	20	UMA
D5.2.3	Implementation of Extra Functional Properties support	5.2	M24	M24	6	8	UMA

**List of Milestones (WP5.2)**

<b>Milestone no.</b>	<b>Milestone name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Lead contractor</b>
WM52/18	Revised version of the design and first version of the basic infrastructure implementation	5.2	M18	M18	UMA
WM52/24	Component Infrastructure and Tool Implementation and first version of the Extra-functional support	5.2	M24	M24	UMA

## **2.8. WP5.3: Network Specific Protocols and Infrastructure**

### **Workpackage Objectives**

This WP was originally thought of to cope with the analysis the implementation of the components and protocols that are network and device specific. The components and protocols implemented in this WP are determined by the application environments and must be designed and implemented to be easily integrated in the middleware (following the component model established in WP5.2).

### **Starting Point**

The main inputs for this WP are:

- The state of the art, security requirements and application specific requirements of WP1
- The SMCOM and associated component framework

### **Progress on WP5.3 in Year 1**

The first step in this WP was the study of the network protocols that will be used to connect SMEPP nodes and to perform routing functions. The selection has been done on the basis of a preliminary design of the way that the applications use SMEPP. In particular, the use of sensor networks and mobile telephones determines the study of different wireless communication protocols.

We have analyzed the communication requirements of the two validation applications. In the case of the Home Systems and Mobile Telephony application, we assume that most users of the application will get connectivity through a residential gateway. One possible solution to the interoperability problem could consist of a special OSGi bundle deployed in the residential gateway that would act as a bridge between OSGi and SMEPP. The residential gateway will behave as a common SMEPP node acting as gateway between home networks and external networks. Also, every device participating in SeguiTel could be connected to the SMEPP network, either directly, through its nearest residential gateway or through SeguiTel provider servers, assuming they are also running these OSGi/SMEPP bridges. Likewise, acting the residential gateway as a bridge between OSGi and SMEPP, let other services or devices controlled by the residential gateway (UPnP devices, home automation devices...) be published as SMEPP services.

For the environmental monitoring application, SMEPP Light will be used on motes and other constrained devices. These devices would need to be connected to more resourceful nodes that would act as gateways, acting in behalf of the reduced devices and connecting them with the rest of the SMEPP network. More precisely, sensor nodes and, quite probably, worker nodes would be SMEPP Light nodes. Their gateways would be installed at the wireless routers and other network infrastructure devices that give them connectivity.

After the analysis of the requirements, in section we have characterized the most usual protocols that will be used by the applications considering the requirements. We have also analyzed the availability of the different protocols on the devices considered for SMEPP. We distinguish between the different node types and the possible operating systems of each one. All the results of this initial step are summarized in D5.3.1.

The rest of the work carried out in the context of this WP during this second year has been devoted to the analysis and design of the basic supporting protocols of the SMEPP infrastructure. In this sense, we have provided initial solutions for all the protocols needed in the current basic common infrastructure including:

- Secure routing in ad-hoc networks
- Service discovery
- Overlay management
- Group management
- Event management

During the next year we plan to improve some of the protocols. In the case of groups, the use the overlay network to improve the efficiency of broadcasting has been studied.

### Deviations from project workprogramme for WP5.3

There have not been major deviations during this year

### List of Deliverables (WP5.3)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D5.3.1	Analysis and Ev. of network specific EP2P protocols	5.3	M12 M18	M15 M18	6	6	I2R
D5.3.2	Network and device specific protocols design	5.3	M21	M24	8	6	I2R

### List of Milestones (WP5.3)

Milestone no.	Milestone name	Workpackage no.	Date due	Actual/Forecast delivery date	Lead contractor
WM53/18	Analysis and Evaluation of network specific protocols for EP2P	5.3	M18	M18	I2R
WM53/24	Network and device specific protocols design	5.3	M24	M24	I2R

## **2.9. WP6: Applications and Validation**

### **Workpackage Objectives**

The main objective of the WP during the second year of the project is to *first define and specify the two applications that were considered in the Dow:*

- a) One related to two specific areas: Home and Mobile systems which implied the realisation of Mobile Personal Context Aware Communication Services. The service chosen in WP1 is, as mentioned above, centred on an e-Health service which takes into consideration what benefits EP2P systems can bring into the field for group based communications and information sharing.
- b) The other one implements the monitoring of effects (Radiation) of industrial plants on the environment in the field of nuclear energy, where the security and reliability aspects of SMEPP middleware can be validated and how valuable is the implementation of a Middleware solution running on the sensor networks themselves without using bridges for instance.

Moreover an evaluation of the capacity of the SMEPP designed Middleware to implement the designed scenarios was to be monitored closely to identify the parts of the applications that could suffer modifications. Also the security mechanisms and threats had to be analyzed.

### **Starting Point**

The requirements and prototypes developed in WP1, the concrete middleware software architecture (WP3), the component framework (WP5.2) and the study on the protocols of D5.3.1, including SMEPP and OSGi interaction and SMEPP standard – AMEPP light integration.

### **Progress on WP6 in Year 1**

Most of the effort in this WP was devoted to the design of the validation applications that is included in the deliverable D6.1 and D6.2. This work has strong dependencies with the results of WP3 and WP5.\*. Even if some of the results of these WPs was delayed, the impact on the design was not too high due to the extra-effort that was put in the design of the requirement elicitation prototypes (see Year 1 Activity Report ).

A first detailed specification and preliminary design work on Environmental monitoring application has been produced. TEC has also redesigned the electronics associated to the prototype that will be developed during the next year. A new board with an integrated radiation sensor is ready for the development of this prototype, reducing the problems with the interaction of the external dosimeters that were presented in the prototypes developed during the first year.

The second validation application is related to the tele-assistance platform of Seguitel and to the services requirements and scenarios specified in D1.3. The service is about the generation and handling of alarms. This year TID has improved the JXTA prototype to include several functionalities such as VOIP and Video streaming. Continuous feedback to WP5 is being

provided to ensure that the applications requirements are met by the envisaged and designed middleware.

### Deviations from project workprogramme for WP6

There have been no significant deviations from the planned workprogramme, but a short delay in the design work caused by its dependencies of WP3 and WP5 is recognized. We expect that this delay will not impact the final result of this WP.

### List of Deliverables (WP6)

Del. no.	Deliverable name	Workpackage no.	Date due	Actual/Forecast delivery date	Estimated indicative person-months	Used indicative person-months	Lead contractor
D6.1	Design and Implementation of environmental monitoring app	6	M24	M24	36	7,2	2
D6.2	Design and Imp. of telephony services and applications	6	M24	M24	34	8,1	7

### List of Milestones (WP6)

Milestone no.	Milestone name	Workpackage no.	Date due	Actual/Forecast delivery date	Lead contractor
WM6/24	Design of both validation applications	6	M24	M24	TID

## **2.10. WP7: Dissemination and Exploitation**

### **Workpackage Objectives**

The main objective of this WP is to disseminate and exploit the SMEPP results from the scientific and industrial point of view. In this sense, we target a broad audience

### **Starting Point**

The dissemination activities have basically followed the plan presented in deliverable D7.1, that was accepted in the first year review.

### **Progress on WP7 in Year 1**

Most partners have contributed to scientific dissemination through publications in International Conferences and Journals. A total of 22 conference papers and 4 journals and book chapters has been published during this second year. The collaboration inside the consortium has been increased, with joint publications with UPI, TID, TEC and I2R. On the other hand, the major event during this year was the organization of the MIMES workshop in Dublin as an associated workshop to the Mobiquitous 2008 International Conference. The workshop was organized by UMA and UPI and all the papers were refereed by at least two relevant researchers in the field.

During this first year, we obtained some feedback on the general impact of the project. For instance, SMEPP and its radiation monitoring application is referenced in the Crossbow page as a relevant application of their technology <http://blog.xbow.com/xblog/2007/12/radmote---mobil.html>. This page had a very large number of visits and since its publication we have received a lot of mails asking for information about SMEPP from companies and universities (University of Sydney,...). More detailed information is included in the second version of the dissemination deliverable.

Overall, perhaps the most relevant success has come from the industrial impact, in the case of UMA and SMEPP initial contact has been established with Entergy Nuclear Incorporated, in the USA. This company has shown their interest in the SMEPP technology and a meeting with this company is planned for next December

In the case of the industrial partners they have also carried out an important effort on dissemination and initial exploitation plans. TID presented a paper in Telecom I+D 2008 ("Middleware seguro EP2P: un desafío para las redes sociales"), written by Telefónica, Tecnom and UMA about the SMEPP validation applications. This conference has a significant impact on the ICT companies in Spain, since it has a long track and most of the main players in this field regularly assist yearly.

Telefónica, Tecnom and UMA have also collaborated in another paper for the Blog of the Technological Observatory (La Cofa: <http://www.lacofa.es>), that has also a significant impact on the TIC area. Other different articles have been published on the intranets of the Telefónica Group (SIMTID and Diario Telefónica). Internal dissemination within Telefonica

Investigación y Desarrollo has been promoted and an internal workshop was held on the 1<sup>st</sup> of April 2008 for the whole Digital Home organisation (about 60 attendees). The event was broadcasted to our premises in Huesca- Spain, Valladolid-Spain and Sao Paulo Brasil.

Tecnatom has also worked on the internal an external dissemination in its area. The main activities can be summarized as:

- Internal dissemination through presentations to different departments in the company and paper on the impact of the SMEPP results that was distributed via the Tecnatom Intranet.
- A paper presented in the technological bulletin of the *Comunidad de Madrid*.
- Different contacts with potential partners and clients for the exploitation of the technology (Nuclear Central Plants, MGPI – that is a world-wide manufacturer/provider of radiological equipment -, Entergy, Thermo, etc.)

#### **Deviations from project workprogramme for WP7**

No significant deviations from the workplan

#### **List of Deliverables (WP7)**

<b>Del. no.</b>	<b>Deliverable name</b>	<b>Workpackage no.</b>	<b>Date due</b>	<b>Actual/Forecast delivery date</b>	<b>Estimated indicative person-months</b>	<b>Used indicative person-months</b>	<b>Lead contractor</b>
D7.1	Dissemination Plan	7	M18	M18	6	4,00	SIEM

#### **List of Milestones (WP7)**

No milestones in this WP during the second year

## **3. Consortium Management**

### **3.1. *Project Status***

During this second year the project continued as planned, although some extra-work was required for the development of the software architecture. This also produced a delay in the implementation and some extra-work to prepare an intermediate review that was held in Brussels in April 2008.

As a consequence of this review, task 3.4 was cancelled, and the resources devoted to that task were re-allocated to WP 5.2, where a significant effort increment was needed due to the limited re-usability of the results of other projects.

In general, the work on all the WPs devoted to implementation (WP5.\*) was delayed as a consequence of the late delivery of the WP3 results, but the extra effort of the consortium has partially overcome this, and only a small delay in the T2 implementation of the middleware exist (~1 month).

The rest of the activities related to coordination (steering committee meetings, advisory board, dissemination, etc) are going as planned. More details on these issues can be found in the description of the work of WP0 and on the management report.

### 3.2. Workplanning and timetable\*

Task Name	First Year									Second Year									Third Year																
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
<b>WP0 Project Management</b>																																			
<b>WP1 Middleware and Application Requirements</b>																																			
T1.1 Generic Middleware Requirements	█																																		
T1.2 Security Requirements	█			█																															
T1.3 Application Requirements	█			█																															
<b>WP2 Abstract Service and Interaction Model</b>																																			
T2.1 Service Discovery	█			█						█																									
T2.2 Service Interaction	█			█						█																									
T2.3 Secure Service Providing	█			█																															
<b>WP3 Software Architecture</b>																																			
T3.1 Architecture Specific Requirementst	█			█																															
T3.2 Conceptual Architecture	█			█						█																									
T3.3 Service Components	█			█						█																									
T3.4 Architecture Evaluation	█			█						█									█																
<b>WP4 Security Services</b>																																			
T4.1 Threat Models	█			█																															
T4.2 Security Foundations	█			█																															
T4.3 Security Protocols	█			█						█																									
T4.4 Power Estimation Methodology	█			█																															
<b>WP5 Implementation Coordination</b>																																			
T5.1 Configuration Management and Version P.	█			█																															
T5.2 Middleware Implementation Coordination	█			█						█									█																
T5.3 Applications and Validation Support	█			█						█									█																
<b>WP5.1 Security Services Implementation</b>																																			
T5.1.1 Secure Instruction set extensions	█			█						█																									
T5.1.2 Secure HW Modules for asymmetric cryp.	█			█						█																									
T5.1.3 Design of new asymmetric cryp. primitives	█			█						█																									
T5.1.4 Imp. of symmetric and asymmetric algorithms	█			█						█									█																
T5.1.5 Elliptic curve construction algorithm	█			█						█																									
T5.1.6 Implementation of Security Protocols	█			█						█									█																
<b>WP5.2 Middleware Framework Implementation</b>																																			
T5.2.1 Basic Component Infrastructure Development	█			█						█									█																
T5.2.2 Component and Application Development Tools	█			█						█									█																
T5.2.3 Extra Functional Properties Support	█			█						█									█																
T5.2.4 Upgrading and Extension Support	█			█						█									█																
<b>WP5.3 Network Specific Protocols and Infrastructure</b>																																			
T5.3.1 Analysis of Specific Protocols and Infrastructures	█			█						█																									
T5.3.2 Evaluation of Specific Protocols	█			█						█																									

Milestone MIL1

T5.3.3 Implementation and Int. of Selected Protocols																																					
Task Name	First Year												Second Year												Third Year												
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
<b>WP6 Applications and Validation</b>	Milestone MIL2																																				
T6.1 Environmental Monitoring Application																																					
T6.2 Mobile Telephony Applications																																					
T6.3 Middleware Validation																																					
T6.4 Security evaluation																																					
<b>WP7 Dissemination and Exploitation</b>																																					
T7.1 Academic Dissemination and Exploitation																																					
T7.2 Industrial Dissemination and Exploitation																																					



**\*The tasks in red reflect the proposed changes to the workplan for year 1**

**\*The tasks in blue reflect the proposed changes to the workplan for year 2, as requested in the intermediate review of April 2008**

### 3.3. Overall Status of Deliverables

The deliverables produced during this second year are shown below.

Delilverable	WP	Title	Partner	Due
D0.1-D0.3	0	Annual Management Reports	UMA	M24
D0.4-D0.6	0	Annual Activity Reports	UMA	M24
D1.1	1	State of the art and generic middleware requirements	TEC	M15
D1.2	1	Security requirements of EP2P Applications	TEC	M15
D1.3	1	Application Requirements	TEC	M18
D2.1	2	Service Model Description	UPI	M15
D2.2	2	Tool support for the service model	UPI	M15
D3.2	3	Conceptual architecture of secure EP2P middleware	VTT	M20
D3.3	3	Concrete architecture of secure EP2P middleware	VTT	M20
D3.4	3	Evaluation results of EP2P middleware and service model	VTT	M20
D4.3	4	Security Protocols for EP2P networks	UMA	M24
D4.4	4	Power estimation methodology	UMA	M18-24
D5.0.2	5.0	Implementation progress reports	TEC	M18-24
D5.1.1	5.1	Spec of Secure Instruction Sets for EP2P Devices	TUG	M15
D5.1.3 <sup>1</sup>	5.1	Design and Imp of symmetric/asymmetric algorithm	TUG	M30
D5.2.1	5.2	Component Infrastructure and Tool Design	UMA	M15-M24
D5.2.2	5.2	Component Infrastructure and Tool Implementation	UMA	M15- M18-M24
D5.2.3 <sup>2</sup>	5.2	Implementation of Extra Functional Properties support	UMA	M24
D5.3.1	5.3	Analysis and Ev. Of network specific EP2P protocols	I2R	M15-M18-M24
D5.3.2	5.3	Network and device specific protocols design	I2R	M21
D6.1	6	Design and Imp. of environmental monitoring app.	TID	M24
D6.2	6	Design and Imp. of telephony services and applications	TID	M24
D7.1	7	Dissemination Plan	SIEM	M24

<sup>1</sup> Note that this deliverable was delayed with respect to the original WP (see Activity report year 1)

<sup>2</sup> This deliverable is a prototype, without associated report. See discussion on WP5.3 in this repor

### **3.4. Progress towards Year 3 Objectives and Deliverables**

The final year of the project will be devoted to the refinement of the current implementations and the development of the final validation prototypes. The main risk at this moment is the efficiency of the T2 implementation. In this sense, a specific task on optimization is for the next months and some initial results have been produced. The component model and the underlying routing services are now running on Microsoft based PDAs. The rest of the components are now been migrated, and only some efficiency problems have been found in the case of service implementation, that is too time and memory consuming. Several optimizations have been studied and will be implemented in the next months. In addition to concrete optimizations, other general optimization strategies have been studied and are planned to be used. Concretely code shrinking and obfuscators have been tested, with good results. Although its applicability is not immediate due to the use of reflection in the run time component framework, there are some techniques that could overcome this problem and that currently under test.

Other important point is the optimization of some of the protocols. The current version of some of the protocols can be improved. For instance, in the case of group management, the use of the overlay network component for optimizing broadcasting is planned as an immediate step.

With respect to security, new protocols will be implemented and tested during the next year. Special attention will be paid to the integration of the elliptic curve based algorithms that are currently finished and are being integrated in SMEPP light.

The validation of the implementation has already started. In this sense a set of test has been developed and will be conveniently updated during all the year. The idea is to run all these tests after each modification of the middleware.

The rest of the activities will follow the initial work-plan, with the modifications proposed in the first year for WP 5.3 and the ones included in WP3 and WP5.2 for this year. In this sense, The deliverables for the next year are the one planned in Dow.

An increment in the dissemination and exploitation activities is also planned, with the organization of the second edition of the MIMES workshop, where an especial track on demonstration will be organized. We also plan to attend to other meetings to carry out demonstration activities, after the first prototypes are finished.

### **3.5. Advisory Board**

The Advisory Board is comprised of the following members; Joaquin Torrecillas, Head of the Research Department on Wireless Technology in AT4, Robert H. Deng, Singapore Management University, Alex Wolf, Imperial College London, Eduardo Sollet, head of the Nuclear Power Plant in Confrontes (Spain), and Michael Gonzalez Harbour, Project Coordinator of the Frescor STREP project. Following the recommendations of the reviewers a member of the MORE project has been incorporated to the Advisory board.

The first meeting of the Advisory Board was held on Madrid on October 17<sup>th</sup>. After the meeting a questionnaire was provided for all the participants and some conclusions from these questionnaires were summarized, in order to ask for an agreement of the board. The preliminary conclusions agreed for this meeting can be summarized in the following points:

- The project was found very interesting and with clear scientific and technological challenges.
- The workplan and the development during the first year were recognized as appropriate, although a major effort on prototyping was suggested.
- The link between the demos/applications and the SMEPP middleware should be highlighted.

- Quality of service should be tackled in the same (transversal) way as security issues have been.
- Necessary to focus on specific security services and threats as it would not be feasible to address all those considered, i.e. *prioritize*.
- Necessary to demonstrate the coordination through the realization of joint publications and presentations.

All these points have been taken into account, and the members of the board have been informed about the progress on the report through an e-mail list. The next meeting is planned to December 2008, after the second year review.

## **4. Annex I: Effort Table**

## 1.4.1 Person Month Distribution

		Person months											Funded Totals		
		UMA		TEC	TUG		SIEM	VTT	UPI		TID	I2R			
		Funded	Non-funded		Funded	Non-funded			Funded	Non-funded		Funded		Non-funded	
WP0	Effort Spent M6	6		0	0		0	0	0,3	0	0,125	0	0	12,765	
	Effort Spent M9	9		0,33	0,5		0	0	0,5	0	0	0	0		
	Effort M12	9,5	2,5	0,33	0	1	0,3	0	0,1	0,6	0,375	0	0,3		
	M12-M24	12	2	0,33	0	1	0,31	0	0	0,25	0,125	0	0,2		
	Effort spent up to M24	21,5	4,5	0,66	0	2	0,61	0	0,1	0,85	0,5	0	0,5		23,37
	Total Effort Allocated	26	6	1	1	1	1	1	1	1	1	0	1		32
WP1	Effort Spent M6	4		5,9	1,5		0	1,5	2,1	0	4	0	0	2,51	
	Effort Spent M9	8		7,03	3		3,72		3,1	0	0	0	1		
	Effort M12	7,5	2,75	7,41	1	2	3,72	2,5	1,3	2,5	4,625	0	1		
	M12-M24	0	0,5	0,11	1	0,5	0	0	1,4	0	0	0	0		
	Effort spent up to M24	7,5	3,25	7,52	2	2,5	3,72	2,5	2,7	2,5	4,625	0	1		30,565
	Total Effort Allocated	6	3	6	2	3	3	3	3	2	4	0	0		27
WP2	Effort Spent M6	3		0	0	0	0	2	6	0	0	0	0	5,1	
	Effort Spent M9	6		0	0	0	0		15	0	0	0	0		
	Effort M12	9,5	5,5	0	0	0	0	3,5	7,9	15,6	0	0	0		
	M12-M24	0	1,5	0	0	0	0	0	5,1	2,8	0	0	0		
	Effort spent up to M24	9,5	7	0	0	0	0	3,5	13	18,4	0	0	0		26
	Total Effort Allocated	9	4	0	0	0	0	10	25	6	0	0	0		44
WP3	Effort Spent M6	0,36		0	0	0	0	3	0,1	0	1	0	0		
	Effort Spent M9	3		0,9	0	0	0		0,1	0		0	0		
	Effort M12	4,3	1,95	1,52	0	0	0	15,76	1,1	1	1	0	0		

	M12-M24	4,5	5,45	1,47	5	0	0	15,862	15	4	4,825	0	0	46,657
	Effort spent up to M24	8,8	7,4	2,99	5	0	0	31,622	16,1	5	5,825	0	0	70,337
	<b>Total Effort Allocated</b>	<b>12</b>	<b>5</b>	<b>5</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>33</b>	<b>20</b>	<b>6</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>73</b>
<b>WP4</b>	Effort Spent M6	10,86		0	3,5		2,63	0	0	0	0	0	9,64	
	Effort Spent M9			0	6		7,06	0	0	0	0	0	11	
	Effort t M12	5	6,15	0	10	2	7,06	0	0	0	1	0	12	
	M12-M24	0,5	1,9	0	2,5	2	3,53	0	0	0	0,875	0	3,5	7,405
	Effort spent up to M24	5,5	1,9	0	12,5	4	10,59	0	0	0	1,875	0	15,5	30,465
	<b>Total Effort Allocated</b>	<b>12</b>	<b>5</b>	<b>0</b>	<b>8</b>	<b>6</b>	<b>9</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>12</b>
<b>WP5</b>	Effort Spent M6	0		1,24	0	0	0	0	0	0	0	0	0	
	Effort Spent M9	0,5			0	0	0	0	0	0		0	0	
	Effort M12	1	0	1,56	0	0	0	0	0	0	1	0	0	
	M12-M24	3	3	0,99	0	0	0	0	0	0	1,655	0	0	5,645
	Effort spent up to M24	4	3	2,56	0	0	0	0	0	0	2,655	0	0	9,215
	<b>Total Effort Allocated</b>	<b>9</b>	<b>3</b>	<b>4</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>0</b>
<b>WP5.1</b>	Effort Spent M6	0		0	6,5		0	0	0	0	0	0	0	
	Effort Spent M9	0		0	8		2,9	0	0	0	0	0	0	
	Effort M12	0	0	0	10	5	3,76	0	0	0	0	0	2	
	M12-M24	6	0,5	0	11	2	13,46	0	0	0	0	0	10	30,46
	Effort spent up to M24	6	0,5	0	21	7	17,22	0	0	0	0	0	12	44,22
	<b>Total Effort Allocated</b>	<b>15</b>	<b>4</b>	<b>0</b>	<b>28</b>	<b>12</b>	<b>31</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>20</b>
<b>WP5.2</b>	Effort Spent M6	0		0	0	0	0	0	0	0	0	0	0	
	Effort Spent M9	0		0	0	0	0	0	0	0	0	0	0	
	Effort SM12	1,36	0	0	0	0	0	0	0	0,5	0	0	0	
	M12-M24	17,5	0,25	0	0	0	0	4,346	4,25	4,15	4,3875	0	0,5	30,4835

	Effort spent up to M24	18,86	0,25	0	0	0	0	4,346	4,25	4,65	4,3875	0	0,5	31,8435
	<b>Total Effort Allocated</b>	<b>9</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>10</b>	<b>10</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>29</b>
<b>WP5.3</b>	Effort Spent M6	0		0	0	0	0	0	0	0	0	0	0	
	Effort Spent M9	0		0	0	0	0	0	0	0	0	0	0	
	Effort M12	0	0	0	0	0	0	0	0	0	0,125	0	0	
	M12-M24	6,5	1,5	1,55	0	0	0	0	2,5	0	3,690	0	0,1	14,240
	Effort spent up to M24	6,5	1,5	1,55	0	0	0	0	2,5	0	3,815	0	0,1	14,365
	<b>Total Effort Allocated</b>	<b>14</b>	<b>6</b>	<b>8</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>5</b>
<b>WP6</b>	Effort Spent M6	0		0	0	0	0	0	0	0	0	0	0	
	Effort Spent M9	0		0	0	0	0,6	0	0	0	0	0	0	
	Effort M12	0,5	0	0	0	0	1,76	0	0	0	0	0	1	
	M12-M24	1	2	6,2	8,5	3	4,85	0	0	0	8,10625	0	0	28,65625
	Effort spent up to M24	1,5	2	6,2	8,5	3	6,61	0	0	0	8,10625	0	1	30,91625
	<b>Total Effort Allocated</b>	<b>17</b>	<b>7</b>	<b>36</b>	<b>10</b>	<b>5</b>	<b>8</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>29</b>	<b>0</b>	<b>0</b>
<b>WP7</b>	Effort Spent M6	0,25		0	0	0	0	0	0	0	0,625	0	0	
	Effort Spent M9	2		2,9	1	0	0,4	0	0,7	0	0	0	0	
	Effort M12	1,25	2	3,07	1	0	0,79	0	0,6	0,5	0,9375	0	1	11,1475
	M12-M24	0	4	2,73	0,5	0,5	1,17	1,655	1,25	0,5	2,255	0	0,2	9,56
	Effort spent up to M24	1,25	6	5,8	1,5	0,5	1,96	1,655	1,85	1	3,1925	0	1,2	17,2075
	<b>Total Effort Allocated</b>	<b>6</b>	<b>4</b>	<b>9</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>6</b>	<b>3</b>	<b>1</b>	<b>5</b>	<b>0</b>	<b>3</b>	<b>35</b>
	Effort M0-M12	39,91	20,85	13,89	22	10	18,71	21,22	11	20,7	9,063	0	17,3	204,6425
	Effort M12-M24	51	22,6	13,38	28,5	9	23,32	21,863	29,5	11,7	25,919	0	14,5	193,482
	<b>TOTAL effort spent to M24</b>	<b>90,91</b>	<b>37,3</b>	<b>27,28</b>	<b>50,5</b>	<b>19</b>	<b>40,71</b>	<b>43,623</b>	<b>40,5</b>	<b>32,4</b>	<b>34,981</b>	<b>0</b>	<b>31,8</b>	<b>328,504</b>
	<b>TOTAL EFFORT ALLOCATED</b>	<b>135</b>	<b>50</b>	<b>69</b>	<b>51</b>	<b>30</b>	<b>56</b>	<b>63</b>	<b>62</b>	<b>17</b>	<b>54</b>	<b>0</b>	<b>41</b>	<b>490</b>

Comentario [a1]: Funded + Non funded

## **5. Annex II: Changes to the DoW**

The changes to the DoW are minor. We have just allocated the remaining effort from task 3.4 to WP 5.2 and mainly to the tasks related to tool implementation. The work achieved by VTT in the WP has previously been described in this document. The changes on the time table are reflected in section 3.2.

<b>Workpackage number</b>	3			<b>Start date or starting event:</b>				Month 3		
<b>Workpackage title</b>	<b>Software Architecture</b>									
<b>Participant id</b>	UMA	TEC	TUG	SIEM	VTT	UPI	TID	I2R		
<b>Person-months participan</b>	12	5	5		0	27 <sup>4</sup>	20	6	3	

### Objectives

The aim of work package 3 is to define a distributed software architecture for reconfigurable middleware that supports the new interaction model (developed in WP2) and the special security and adaptability requirements of EP2P. The goal of the architecture is to ensure both quality of service and ease of development of the middleware. Consequently, the architecture provides a design of a Component Based Framework for the development of self-configurable services. The work package is related to WP2 and WP4.

The main contribution of WP3 is the software architecture description of secure EP2P middleware. WP3 is carried out in an incremental and iterative way and it produces 3 versions of the main deliverables (V1, V2 and V3). Each increment is validated by service development activities in WP5 and application development in WP6.

### Description of work

#### Task 3.1: Architecture specific requirements

In this task the functional and non-functional requirements for secure EP2P middleware will be (re)defined starting from the application and business requirements defined in WP1. Technological constraints (e.g. standards and other regulations) and quality criteria for secure P2P middleware are defined for selecting middleware technologies and 3<sup>rd</sup> party components.

The tasks results in the architecture specific requirements of secure EP2P middleware.

#### Task 3.2. Conceptual architecture

This task divides the functional and non-functional responsibilities of the middleware into layers to provide separation of concerns to different service levels. Each layer is further clustered to meaningful sub-domains according to the purpose of use. The services provided by the different layers and sub-domains are defined at the conceptual level. The service interaction model developed in WP2 is taken into account in architecture definition. Special attention is paid to the security issues defined in WP4.

The outcome of the task is the conceptual architecture of the secure middleware of EP2P systems.

#### Task 3.3: Service components

This task focuses on the specification and design of the service components for the secure EP2P middleware. Special attention is paid to interfaces and mechanisms that allow reliable self-configuration of real-time applications and run-time adaptation of middleware services. Service contracts have a strong influence on the service components of EP2P middleware and therefore the work in service components is defined in conjunction with WP2. The specific architecture of the service components of the secure EP2P middleware is the outcome of this task.

<sup>3</sup> The shaded columns indicate effort of permanent staff for partners with additional cost model

<sup>4</sup> Modified from the initial 33 pm

<b>Deliverables</b>	<b>Delivery Date</b>
D3.1 Architectural specific requirements of secure EP2P middleware	M8
D3.2 Conceptual architecture of secure EP2P middleware	M8-M12-M20-M30-M35
D3.3 Specific architecture of secure EP2P middleware	M12-M20-M30-M35

<b>Milestones<sup>5</sup> and expected result</b>	
WM3/8	Architecture specific requirements (D3.1) and conceptual EP2P middleware architecture (D3.2) (V1)
WM3/12 (V1)	Conceptual EP2P middleware architecture (D3.2), a specific architecture for a selected set of middleware services (D3.3) and their evaluation (D3.4)
WM3/20	Conceptual EP2P middleware architecture (D3.2), a specific architecture for an extended set of middleware services (D3.3)
WM3/30	Validated conceptual (D3.2) and specific architecture (D3.3) for EP2P middleware
WM3/30	Final version of all the WP deliverables

---

<sup>5</sup> Milestones in workpackages are identified as **WM**[WPnumber]/month corresponding to the milestone

<b>Workpackage number</b>	5.2		<b>Start date or starting event:</b>				Month 10			
<b>Workpackage title</b>	<b>Middleware Framework Implementation</b>									
<b>Participant id</b>	UMA	TEC	TUG	SIEM	VTT	UPI	TID	I2R		
<b>Person-months participan</b>	9	3				16 <sup>6</sup>	10	1		

### Objectives

This WP will be devoted to the design and implementation of a component frame work to support the software architectures developed in WP3. It must not be seen as a closed middleware implementation, but as a highly customizable framework integrating a minimal set of component concepts (containers and ports for component interaction, support for dynamic deployment and binding of components, packaging and distribution, etc.) with a very small software footprint. This framework will be initially based on the results of the RUNES project, but it will require an adaptation to the P2P service interaction model defined in WP2.

### Description of work

#### Task 5.2.1. Basic Component Infrastructure Development

With the term infrastructure we mean mechanisms for component instantiation, binding, communication, distribution of components over hardware, announcing capabilities of components and discovery of desired components. This task will carry out the design and implementation of the basic infrastructure based on the inputs for WP1 and WP3.

The basic mechanisms included in the SMEPP component infrastructure are:

- *Instantiation and binding.* A Component Instance is the instantiation of a Component implementation at a specific location in the device memory. Once in operation, each component instance may create and manage its own data and can be bound to other components instances by creating links. A link between component instances may be used for communication and navigation. In the case of EP2P systems we need to provide support for dynamic binding. Instantiation and binding mechanisms will be determined by the selected software architecture (WP3).
- *Communication:* The infrastructure must implement the interaction mechanisms defined in WP2, using the architecture provided by WP3.
- *Discovery.* Every component framework needs to define a mechanism by which the presence of components in the system can be discovered. Such a Discovery mechanism is needed to support late and dynamic binding. The discovery mechanism in SMEPP will be determined by the service model defined in WP2.
- *Self configuration and run-time adaptation.* These features are specific to EP2P and will probably consume most of the development efforts. The basic mechanisms for self configuration are defined in Task 3.3, but the framework must allow the integration of domain specific algorithms (as those defined in WP 5.3).

<sup>6</sup> The dark columns indicate effort of permanent staff for partners with additional cost model

<sup>7</sup> Modified from the initial 10 pm

**Task 5.2.2. Component and Application Development Tools**

This task will be devoted to the design and implementation of a set of tools to support component and application development on top of the Component Infrastructure. The tools that will constitute the development environment will be decided after the design of the basic component infrastructure. New tools will be added during the development of task 5.2.3 and 5.2.4. We will pay special attention to analysis tools for Extra Functional Properties.

**Task 5.2.3. Extra Functional Properties Support**

This task has the purpose of extending the basic infrastructure to provide support for extra functional properties. We will concentrate the development efforts mainly on the integration of security services and network quality of service. This task is strongly linked with the previous task, since the support of extra functional properties will require the development of associated tools. The specific properties supported by the middleware will be determined during the requirement analysis phase in WP1.

**Task 5.2.4. Upgrading and Extension Support**

Improvements in software are developed in rapid succession. To extend the economic lifetime of devices, they should be able to upgrade software components with improved versions. In addition to upgradeability, there is a need to be able to add new functionality to a device. The mechanism needed for uploading a new functionality can be largely shared with that for upgrading. This task will be devoted to extending the framework to support the upgrading and extension of applications and the middleware itself.

Network specific protocols and algorithms developed in WP 5.3 will be integrated by means of the functionality developed in this WP.

<b>Deliverables</b>	<b>Delivery Date</b>
D5.2.1 Component Infrastructure and Tool Design	M12-M18-M35
D5.2.2 Component Infrastructure and Tool Implementation	M24-M36
D5.2.3 Implementation of Extra Functional Properties Support	M24-M32
D5.2.4 Implementation of Upgrading and Extension Support	M30-M36

**Milestones<sup>8</sup> and expected result**

WM52/12	First stable version of Component Infrastructure design
WM52/18	Revised version of the design and first version of the basic infrastructure implementation
WM52/24	Component Infrastructure and Tool Implementation and first version of the Extra-functional support
WM52/30	Upgrading and Extension support implemented

<sup>8</sup> Milestones in workpackages are identified as **WM**[WPnumber]/month corresponding to the milestone

