

INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME

Project n°: FP6-IST-033563



SMEPP

Secure Middleware for Embedded Peer-to-Peer systems

WP5.0

D5.0.2 Implementation Progress Report

Author(s):	J. Serrano (TEC), S. Tillich (TUG), M. Diaz (UMA)
Status -Version:	Third release – 2.0
Date:	15 September 2008
Distribution – Confidentiality:	Public
Code:	D5.0.2-ImplementationProgressReport.doc

Disclaimer

This document contains material, which is the copyright of certain SMEPP contractors, and may not be reproduced or copied without permission. All SMEPP consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The SMEPP Consortium consists of the following companies:

Participant no.	Participant name	Participant short name	Country
1 (Co-ordinator)	Universidad de Málaga	UMA	Spain
2	Tecnatom, 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

The information in this document is provided “as is” and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Document Revision History

Date	Issue	Author/Editor/Contributor	Summary of main changes
25 Sep 2007	0.0	José Serrano (TEC)	Initial draft
3 Oct 2007	0.1	Jose Serrano (TEC) Stefan Tillich (TUG)	Rearrangement of actual effort section. Description of progress in WP5.1
5 Oct 2007	0.2	Manuel Diaz (UMA)	Description of progress in WO5.2
4 April 2008	1.0	José Serrano (TEC)	Second release: First draft
25 June 2008	1.1	José Serrano (TEC) D. Garrido, R. Roman (UMA) F. Benigni (UPI) E. Hess (SIE) T. Paaso (VTT) J. Zhou (I2R) U. Payer (TUG)	Partner Inputs
15 September 2008	2.0	José Serrano (TEC)	3 rd release

Table of Contents

1	Introduction	5
1.1	Purpose.....	5
1.2	Audience	5
2	Scope	6
3	Expected and actual progress	7
3.1	Expected Progress.....	7
3.2	Actual Progress	8
3.2.1	WP5 Implementation Coordination	9
3.2.2	WP5.1 Security Services Implementation	9
3.2.3	WP5.2 Middleware Framework Implementation	10
3.2.4	WP5.3 Network Specific Protocols and Infrastructure	13
4	Version Plan	14
4.1	Milestones.....	14
4.1.1	Versions	14

1 Introduction

1.1 Purpose

Implementation inside SMEPP project is divided in three work-packages:

- 5.1 Security Services Implementation
- 5.2 Middleware Framework Implementation
- 5.3 Network Specific Protocols

As stated in the Description of Work, work package 5 (Implementation Coordination) is responsible for monitoring the work plans for each implementation WP.

A new version of Deliverable 5.0.2 is released every six months. This version describes the progress of implementation from month 18 to month 24.

1.2 Audience

The audience for this document includes the project management, system analysts, system designers and testers.

2 Scope

This report covers the implementation progress for all the software development produced from month 18 until month 24 in the SMEPP work-packages 5.1 (Security Services Implementation), 5.2 (Middleware Framework Implementation) and 5.3 (Network Specific Protocols and Infrastructure)

3 Expected and actual progress

3.1 Expected Progress

According to the plans described in the Description of Work and the Initial Version Plan described in deliverable 5.0.1 (Configuration Management Plan) the implementation should be working towards the milestone of version 0.1, expected initially for month 24.

The version plan was updated in the last release of this Implementation Progress report (March 2008). In this update, version 0.0 was delayed to month 22. This version should include Basic Component Infrastructure:

- Instantiation and binding
- Communication
- Discovery
- Self-configuration and run-time adaptation.

According to this last update, the following version of the middleware (0.1) is expected for month 28. This next version will include:

- Component Infrastructure & Tools
- Extra functional properties support: Integration of security services & network QoS.
- Cryptographic algorithms and protocols

According to the Description of Work, most tasks related to Implementation should be active. Namely,

- WP5
 - Task 5.1 Configuration Management and Version Planning
 - Task 5.2 Middleware Implementation Coordination
 - Task 5.3 Application and Validation Support
- WP5.1
 - Task 5.1.1 Secure Instruction Set Extensions
 - Task 5.1.2 Secure HW modules for asymmetric cryptography
 - Task 5.1.3 Design of new asymmetric cryptography primitives
 - Task 5.1.4 Implementation of symmetric and asymmetric algorithms

- Task 5.1.5 Elliptic curve construction algorithm
- WP5.2
 - Task 5.2.1 Basic Component Infrastructure Development
 - Task 5.2.2 Component and application Development Tools
 - Task 5.2.3 Extra functional Properties Support
- WP5.3
 - Task 5.3.1 Analysis of Specific Protocols and Infrastructures
 - Task 5.3.2 Evaluation of Specific Protocols
 - Task 5.3.3 Implementation and Integration of selected protocols

3.2 Actual Progress

At end of month 24, the following tasks are active:

- WP5 Implementation Coordination
 - Task 5.0.1 Configuration Management and Version Planning
 - Task 5.0.2 Middleware Implementation Coordination
- WP5.1 Security Services Implementation
 - Task 5.1.1 Secure Instruction Set extensions for EP2P lightweight devices
 - Task 5.1.3 Design of new asymmetric cryptographic primitives
 - Task 5.1.4 Implementation of Symmetric and asymmetric algorithms
 - Task 5.1.5 Elliptic curve construction algorithm
 - Task 5.1.6 Implementation of Security Protocols
- WP5.2 Middleware Framework Implementation
 - Task 5.2.1 Basic Component Infrastructure Development
 - Task 5.2.2 Component and application Development Tools
 - Task 5.2.3 Extra functional Properties Support
- WP5.3
 - Task 5.3.1 Analysis of Specific Protocols and Infrastructures

- Task 5.3.2 Evaluation of Specific Protocols

A first version of the middleware (0.0) is available as expected. This version incorporates all features planned for this release as well as other features not planned for this date, such as:

- Component Framework Monitorization Tool
- Smepp Light extension
- Secure routing
- Extension support

Description of actual progress in each work-package is described below:

3.2.1 WP5 Implementation Coordination

3.2.1.1 Task 5.1 Configuration Management & Version Planning

The Configuration Management System is been actively used by implementation tasks. The last update of the version plan is still valid.

Also the mailing lists have been very active with information exchange among the software engineers of the different components.

3.2.1.2 Task 5.2 Middleware Implementation Coordination

As a result of the architecture work-package each component of the middleware was assigned to a partner.

Several meetings have taken place to co-ordinate implementation tasks, namely:

- Madrid, April
- Dublin, July

At the moment of writing this report, all components have been finished in their first version and are available for the validation applications.

3.2.2 WP5.1 Security Services Implementation

Work has been very active in this work-package in following areas:

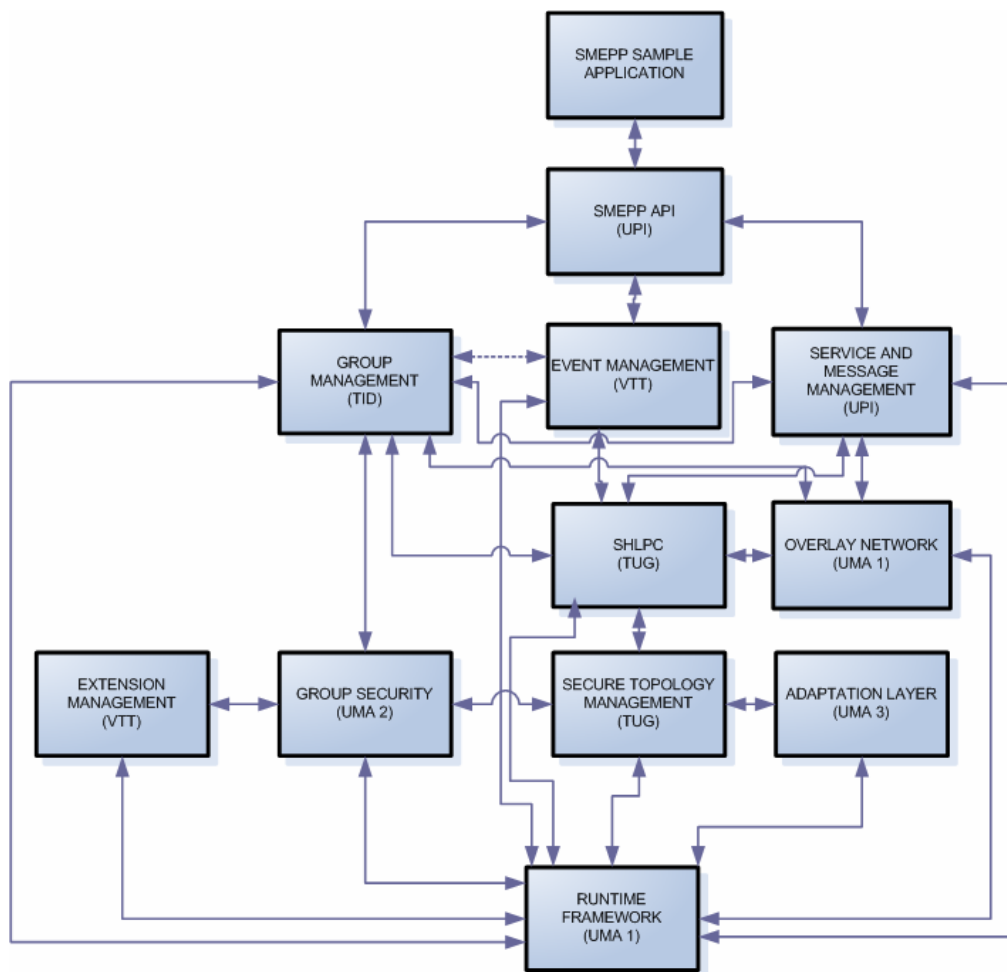
- Power estimation algorithms have been implemented and tested in several scenarios
- The following secure routing algorithms have been implemented and tested: OLSR, AODV, DSR, Ariadne. These algorithms have been implemented on a PDA HP IPaq X4700.

- Several crypto-systems based on ECC have been implemented for the ATMega128 chip, which is the processor of the wireless sensor nodes chosen for this project (MicaZ).

3.2.3 WP5.2 Middleware Framework Implementation

The middleware framework implementation is the core of the implementation tasks.

Thanks to the effort of all partners, a first version of middleware is available now that allows for application developers to start connecting to SMEPP middleware. This version is made up of the following blocks:



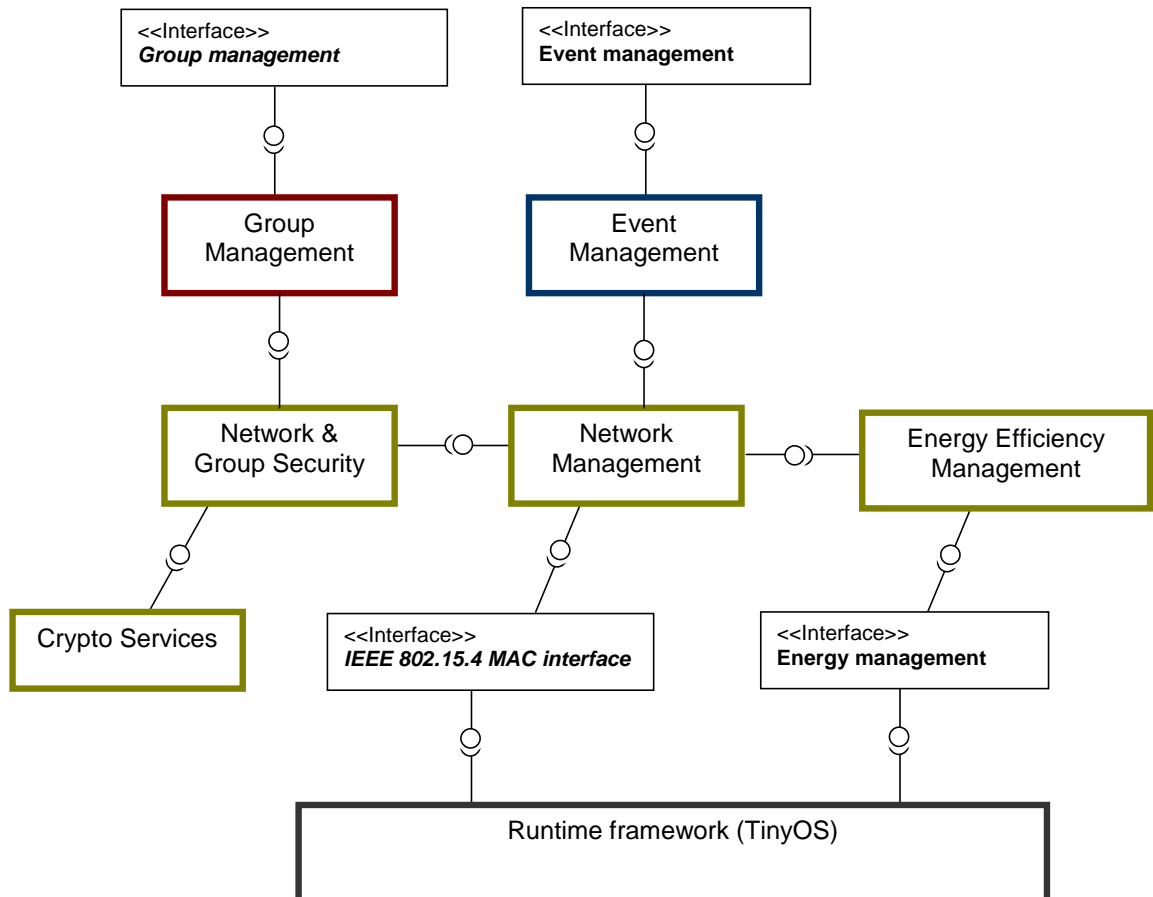
- **API:** This layer provides interaction with the upper-layer applications. A first version of this component is also finished. The current version of the SMEPP_API component is suitable for a prototype of the whole middleware, since it allows prototype applications to be run and it fully uses its SMCOM interfaces.
- **Service & Message Management:** The Service and Message Management component (SMM, for short) is responsible for service publishing/unpublishing, service discovery, contract management, service invocation, and session management. A first basic version of this component has been developed with a simple service discovery mechanism.

- **Overlay Network:** This component represents a virtual network of nodes and logical links that is built on top of the existing network. A first version has been developed that allows for group and peer communication.
- **Event Management:** This component is responsible for handling events inside a peer. This component is fully implemented.
- **Group management:** The Group Management (GM) component is responsible for maintaining the group structure of the SMEPP network. A simplified version of this component is available.
- **Group Security and Cryptographic Services Component:** Group Security is concerned with the security related aspects of group establishment and maintenance. This component is also available in a first version that will be improved in following releases.
- **Secure High Level Peer Communication:** The *Secure High Level Peer Communication Component* is the gateway between the *SMEPP Common Services* and the *SMEPP Enabling Services*. This component is fully implemented and only modifications resulting of application development are expected.
- **Secure Topology Management Component:** The main function of the STM is to provide peer communication capabilities to the higher layer components and also manages the admission to the SMEPP network and performs many tasks necessary for keeping the SMEPP network running. This component is implemented, but has not been integrated in this version.
- **Adaptation Layer Component.** This component provides an abstract interface to the underlying execution platform by supplying uniform primitives to access the network, the file system and context data of the device on which is running. Adaptation Layer has been built and tested in isolation but it has not been integrated with the rest of the components yet.
- **Extension Management Component.** This component allows extending the functionalities of the SMEPP Middleware by adding components to the Common Services –level. This component has also been fully implemented and is available in the first version of SMEPP middleware.
- **Runtime Component Framework.** This is the underlying system that provides basic functionality to all of the SMEPP middleware components. This Component framework and several tools, like a debugger, have been developed to help SMEPP implementation team to validate the behaviour of their components.

The version is running fully on T3 devices (WiFi-enabled laptops) and partially on T2 devices (PDA).

3.2.3.1 Smepp Light

The version for T1 devices (wireless sensor boards) is known as “Smepp Light” and is also available as a prototype that incorporates cryptographic algorithms. This version allows applications to communicate with T3 peers using events and groups. It incorporates the following components:



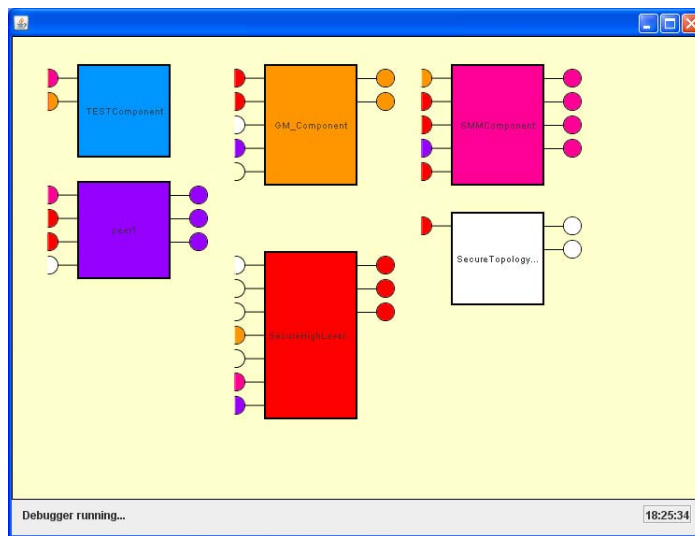
- **Group Management.** The Group Management component manages the peers of each group and the topology of the groups, and maps to the group management and peer initialization primitives.
- **Event Management.** The Event Management component maps to the event management primitives and it is in charge of subscription and event management.
- **Network & Group Security component.** The Network & Group Security component manages the keys for all the security issues related to the network and to the group layers, and provides commands to encrypt/decrypt messages.
- **Network Management component.** The Network Management component implements the communication between peers.

- Energy Efficiency Management. The Energy Efficiency Management component manages the duty cycles of the peer.

“SMEPP Light” is implemented and ready to be used from user's application code, but it has got some limitations due both to its early age and the innovations that are contained in it, that have to live a period of use and debugging to reach a mature state of development.

3.2.3.2 Tools

At the moment a monitorization tool has been implemented to help developers of SMEPP components and applications called “SMCOM Monitorization Tool”. The goal of this tool is to become a fully interactive debugger for SMCOM-based applications.



3.2.4 WP5.3 Network Specific Protocols and Infrastructure

This work-package has been very active in the analysis and evaluation of specific protocols. Although this is not an implementation-specific task it has a strong relationship with implementation.

OSGi has been selected as one of the specific protocols that must extend SMEPP middleware. This is known as SMEPP “extensions”. OSGi extension has been developed during this 6-month period and is now been integrated with the core of SMEPP middleware.

SmeppLite is the extension of SMEPP to wireless sensor nodes and is also available now in a first version.

4 Version Plan

As mentioned in the DoW, the project will follow an iterative approach and will therefore produce incremental versions of the middleware in different iterations.

Deliverable 5.0.1 “Configuration Management System” defined the initial version plan. This version plan was modified in the last release of this report to reflect the current situation of the project.

Version 0.0. was delayed from month 18 to month 22.

Version 0.1 was delayed from month 24 to month 28.

Version 0.2 was delayed from month 30 to month 32.

4.1 Milestones

The main milestones in the different sub-packages are:

- (WP5.2) M18: First version of the basic infrastructure implementation. Delayed to month 22.
- (WP5.2) M24: Component Infrastructure & Tools Implementation
- (WP5.2) M24: First version with extra functional support
- (WP5.1) M24: Cryptographic algorithms and protocols implemented and security support HW module design
- (WP5.2) M30: Upgrading and Extension Support implemented
- (WP5.3) M30: Network and device specific protocols implementation and integration

4.1.1 Versions

With these milestones in mind, three main versions are defined:

- Version 0.0 (M22). Includes:
 - Basic Component Infrastructure: Instantiation and binding, Communication, Discovery, Self-configuration and run-time adaptation

This version has been produced and more features than expected have been incorporated, such as

- Component Framework Monitorization Tool
- Smepp Light extension

- Secure routing
- Extension support
- Version 0.1 (M28). Includes:
 - Component Infrastructure & Tools
 - Extra functional properties support: Integration of security services & network QoS.
 - Cryptographic algorithms and protocols
- Version 0.2 (M32). Includes:
 - Upgrading and extension support
 - Network and device specific protocols

After version 0.2 has been released, other new versions will appear with the feedback and issues from the application.