*ICT-MobileSummit 2008 Conference Proceedings*
*Paul Cunningham and Miriam Cunningham (Eds)*
*IIMC International Information Management Corporation, 2008*
*ISBN: 978-1-905824-08-3*

*Poster Paper*

# Assessing Personal Networks on a Pan-European Testbed

Luis SANCHEZ[1], Jorge LANZA[1], Ingrid MOERMAN[2], Jeroen HOEBEKE[2], Kimmo AHOLA[3], Mikko ALUTOIN[3], Jordi JAEN PALLARES[4], Martin BAUER[5], Marc GIROD-GENET[6], Joachim ZEISS[7]

[1] *University of Cantabria, Spain, {lsanchez, jlanza}@tlmat.unican.es*
[2]*Gent University/IBBT/IMEC-IBCN, Belgium,*
*Email: {ingrid.moerman, jeroen.hoebeke}@intec.ugent.be*
[3]*VTT, Finland, Email: {Kimmo.Ahola, Mikko.Alutoin}@vtt.fi*
[4]*FOKUS, Germany, Email: jordi.jaen.pallares@fokus.fraunhofer.de*
[5]*NEC, Germany, Email: Martin.Bauer@nw.neclab.eu*
[6]*GET-INT, France, Email: marc.girod_genet@int-edu.eu*
[7]*FTW, Austria, Email: Zeiss@FTW.at*

**Abstract:** The development of new research paradigms is usually not supported by a proof-of-concept that helps to showcase the potential impact of the research concept behind. Personal Networking is an emerging concept which combines pervasive computing and strong user focus. The idea is that the user's personal devices organize themselves in a secure and private personal network transparently of their geographical location or the access technologies used. The user expects the network to be always ready for supporting his necessities without requiring too much involvement on her/his side. Additionally, the PN must be ready to share the services it provides to the user with other users that have been authorised in order to allow the collaboration between the PNs' users. The PN Federation concept is presented as a secure cooperation between a subset of devices belonging to different PNs for the purpose of achieving a common goal or service by establishing an alliance. This paper presents the highlights of the implementation of a full-blown Personal Networking system carried out and the set up of a pan-European testbed where the system can be subject of functionality and performance tests as well as be used to demonstrate the potentiality of Personal Networking concept.

**Keywords:** Implementation, Testbed, Personal Networks, Pilot Services

## 1. Introduction

Take the concept of pervasive computing and combine it with strong user focus and you get Personal Networks (PN) [1]. PN is a collection of one's most private devices referred to as personal nodes. The PN consist of devices sharing a common trust relationship. Security and privacy are the fundamental properties of the PN, as well as its ability to self-organize and adapt to mobility and changing network environments.

The IST project MAGNET vision is that PNs will support the users' professional and private activities, without being obtrusive and while safeguarding privacy and security [2]. A PN can operate on top of any number of networks that exist for subscriber services or are composed in an ad hoc manner for this particular purpose. These networks are dynamic and diverse in composition, configuration and connectivity depending on time, place, preference and context, as well as resources available and required, and they function in cooperation with all the needed and preferred partners.

The PN consists of clusters of personal nodes. One cluster is special, so-called Private Personal Area Network (P-PAN), because it is located around the user. The clusters are

connected with each other via an interconnecting structure, which is likely to be infrastructure based.

In order to protect the privacy of the user and the integrity of the PN, security measures are used to encrypt the user's data when it is sent outside of the device, i.e. using a wireless medium or the infrastructure. The user can reach all of his or her devices using a variety of underlying networking technologies, which are invisible to the user. The user only sees the services that are available in the PN and on foreign nodes that have been made available.

Nonetheless, personal communications cannot be restricted to the services provided by the devices the user owns, but the possibility to interact with other user's PN has to be enabled in order to support the user in his/hers private and professional activities. The concept of PN Federations (PN-F) is even a more challenging one since the relations between users have to be managed and the security has to be reinforced in order to not open security holes while allowing authorized users to cooperate with you. PN-F is a secure cooperation between a subset of devices belonging to different PNs for the purpose of achieving a common goal or service by establishing an alliance. It can be established through interconnecting infrastructures (namely infrastructure case) or by direct communication between PN nodes (namely ad hoc case).

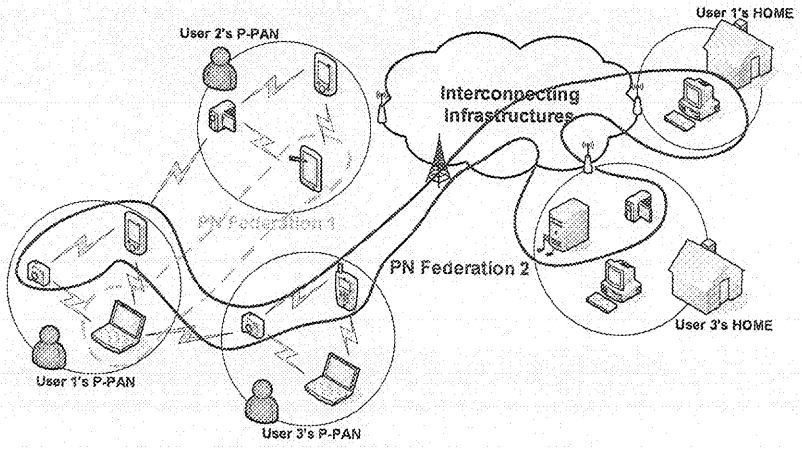



*Figure 2: Personal Network Federation*

The evaluation of this concept cannot be fully tackled just by means of simulations or theoretical analyses. Instead, there is a clear need for a real system that based on the requirements imposed implements the required functionalities so that both functional, performance and usability evaluations can be carried out. Additionally, the implementation has to be done taking into account the scenarios in which the system is going to be used. Thus, it is necessary to assure that the system can be run over real portable devices like PDAs and laptops. Finally, the Personal Networking concept has a global footprint that imposes remote operation. In this sense, it is not enough to test the system on reduced laboratory setups but there is the need for extending the range of the tests and embracing multiple sites located at remote places and connected using the current interconnecting infrastructures.

This paper will present the highlights of the Personal Networking system implementation and the different components that compose it. Additionally, it will describe the main aspects of the pan-European testbed that have been settled between a group of research laboratories in order to assess the system functionality and performance as well as to help on the system integration and in the future to perform usability tests with real users.

The rest of the paper is organized as follows. In Section 2 the system implementation will be presented. Starting from the single PN system implementation and analyzing how the different components have extended in order to cope with the PN Federations scenario.

Section 3 will describe the testbed settled. It will present not only the physical details of the testbed such as locations and involved hardware but also the way the system has been partitioned and made available for implementation so that further locations can be added to the testbed. The main tests to be performed over the testbed and the scenarios that are prone to be analyzed will be presented in Section 4. Finally, Section 5 will conclude the paper describing which is the actual and expected impact of both the system implementation and the testbed deployment, which has been the lessons learned and how the testbed has helped on the integration of the system and which are the future steps to be taken.

## 2. Implementation of the PN and PN-F Concept

For the PN and PN-F concept, conceptual solutions have been proposed and evaluated ([3] [4]), and the most promising solutions have been selected and implemented on x86 and ARM architectures for a Linux-based platform. In the following subsections we will first briefly summarize the implementation of the PN concept, as reported earlier in [5], followed by a more elaborated discussion on how the different components have been extended to support the PN-F concept. Figure 3 presents the Birds Eye View of the different components that have been implemented and integrated into the PN and PN-F platform.

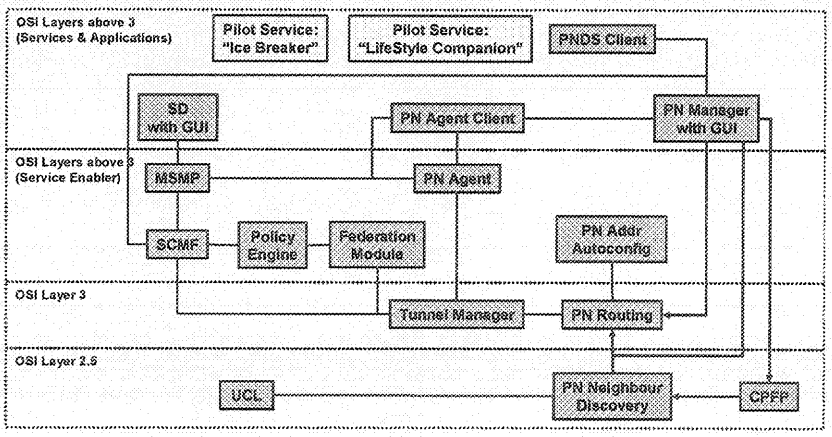



*Figure 3: PN and PN-F system Birds Eye View*

### 2.1. Implementation of the Personal Network Concept

The basic approach taken to realize the PN concept was to implement the PN as a secure and self-organising overlay network consisting of all nodes that belong to the PN. This overlay network has its own private IP addressing space, creating a confined and private network in which personal nodes (PN nodes) can freely communicate with each other and on top of which a service discovery platform and PN applications can be deployed.

A basic requirement to realize this overlay network, is the ability to discriminate between personal nodes and non-personal nodes (i.e. foreign nodes). This discrimination is stored as a property of the corresponding trust relationship. This bilateral secure association between the PN nodes is negotiated using the Certified PN Formation Protocol (CPFP).The CPFP protocol is based in asymmetric cryptography and uses the novel Elliptic Curve Cryptography algorithms to generate the secret keys. The concept behind is that each new node must be introduced to the PN by the user during a procedure called *imprinting*. After a successful imprinting, the new personal device receives a valid PN certificate and is ready to establish secure associations with any other personal node based on each other PN certificates. While the first step (i.e. the introduction to the PN through the imprinting) has to be monitored by the user, the subsequent secure associations that the node establishes with each of the other personal nodes are done automatically and transparently to the user.

Next, physically neighbouring PN nodes can authenticate each other and establish short-term link-level security associations based on the long-term pair-wise keys exchanged during the imprinting. Direct secure communication is then possible at the link level. In order to be able to have IP communication, an address configuration protocol with duplicate address detection allows PN nodes to automatically generate a unique PN IP address from the private IP addressing space assigned to the PN. After the establishment of a secure link, ad hoc routing information is exchanged. The result of the above procedures is a secure and self-organising cluster in which PN nodes can communicate over one or multiple hops.

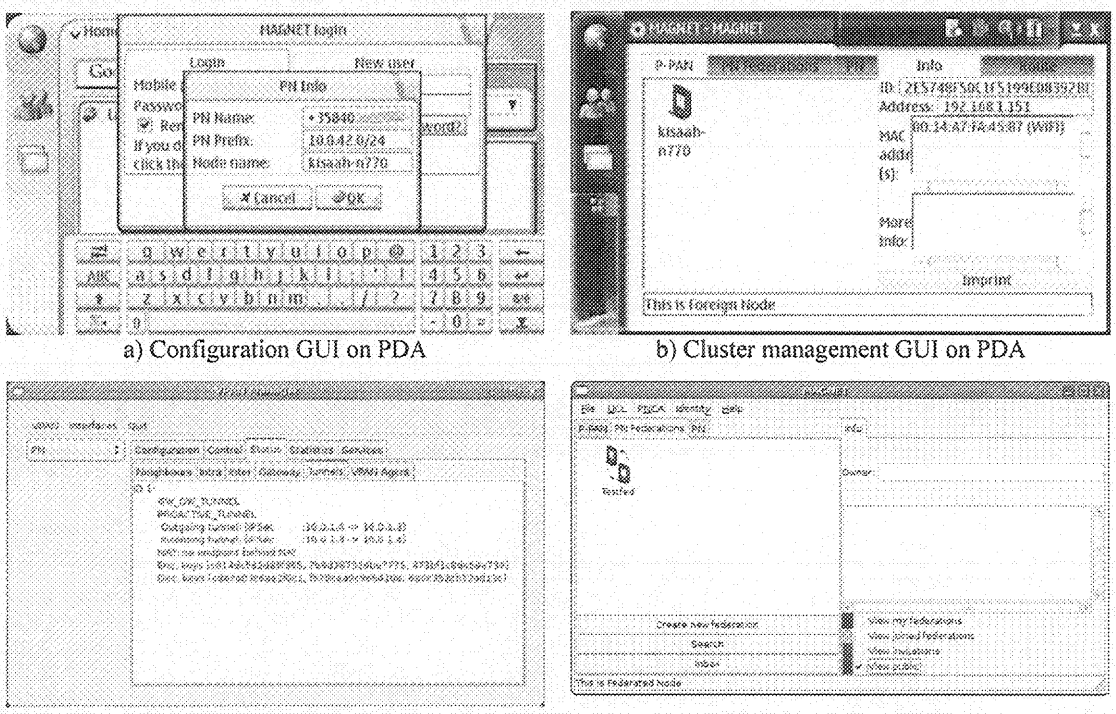
In order to realize full PN connectivity, clusters at different geographical locations need to be interconnected through PN Gateway Nodes that have access to the Internet. To secure inter-cluster connectivity GW nodes will use CPFP over the insecure channel to derive a secure key which will be used to set up an IPsec tunnel between the clusters. A new PN entity called the PN Agent was designed and implemented for maintaining up to date the information of all the PN cluster attachment points. This PN Agent provides name registration/deregistration/discovery, publish subscribe and name resolution functions at PN and PN Federation level. During the PN formation process, the PN Gateway Nodes register themselves to the PN Agent (mainly in terms of attachment point to the Internet - public/private IP addresses and ports) and get, as registration response, the location information of the Cluster Gateway Nodes of all the remote PN Clusters. This remote PN Gateway information will be maintained up to date by the PN Agent through binding updates. The PN Gateway information in the PN Agent is used to dynamically establish and maintain tunnels between the PN Gateway Nodes. Finally, after the exchange of routing information over these tunnels, full inter-cluster connectivity within the PN IP addressing space is possible, allowing secure communication between every pair of PN nodes.

Additional mechanisms have been implemented to improve communication. A universal convergence layer manages all network interfaces and hides the heterogeneity of the underlying interfaces to the routing layer and PN IP addressing space. Extensions have been implemented to be able to take into account NAT boxes. Next to unicast functionality, cluster-wide and PN-wide broadcasting functionality is also supported. Also, the combination of mechanisms to deal with dynamics (such as cluster splits and merges) and private PN addressing allows applications to maintain connectivity despite mobility. Finally, a PN Manager GUI presents the user an interface to use, manage and monitor the implemented software. Figure 4 shows some screenshots taken from the PN Manager. This tool gathers the management and control of the system through its GUI. User interacts with the system, triggers service discovery, etc through this GUI.

On top of this network overlay, a service discovery and management platform (called MAGNET Service Management Platform, MSMP) and a Secure Context Management Framework (SCMF) are implemented. The MSMP offers the user viewing, managing and secure access to all PN resources and services. Its structure follows a twofold approach centralized at the PN cluster level and distributed P2P structure at the PN level (i.e. between the PN clusters). A Service Management Node (SMN) is elected for each PN cluster. The SMN discovers and manages services within its cluster and interacts with other clusters' SMNs in a peer-to-peer fashion via a service overlay. This SMN is also responsible for discovering and advertising remote services within the cluster. The user can achieve this in a very flexible manner, through a GUI, by performing SD queries based on any combination of service/name attributes (e.g. a device name, a service name, a service type and wildcards to get all available matching services); selecting nodes presented on the GUI as icons attached to friendly names; and finally triggering the service invocation and control.

The Secure Context Management Framework [6] provides access to all context and user profile information within a PN. The SCMF consists of context agents running on all PN

nodes. Applications can access all information through the context agent running on their local node. The internal structure of the SCMF follows the structure of the PN. For each cluster a Context Management Node (CMN) is elected. The CMN keeps index information regarding what information can be accessed from each node in the cluster. On the PN level, the CMNs in the different clusters interact with each other on a peer-to-peer basis. For accessing context information, the Context Access Language (CALA) is used. CALA provides a synchronous query/response as well as an asynchronous subscribe/notify interaction style. The modelling of information is entity-based with an underlying entity type hierarchy. The entity type defines what kind of attributes an entity can have. Access to information can be based on entity id/attribute or entity type/attribute combinations. A scoping concept makes access to information more efficient by limiting the nodes that need to be queried, e.g., only the local node or the cluster. Context agents access local context information through retrievers that provide a uniform interface to context sources. Examples for context sources are sensors, the networking stack, and the operating system. User profile information is stored in a storage component within a context agent.




a) Configuration GUI on PDA

b) Cluster management GUI on PDA

c) PN Tunnel management GUI

d) PN-F management GUI

*Figure 4: System Management GUI (aka PN Manager) Screenshots*

## 2.2. *Implementation Personal Network Federation Concept*

In order to realize the PN-F concept, a mechanism to define new PN-Fs and to add PNs to this PN-F is needed, resulting in a PN-F creation and participation protocol. The PN-F Creator generates a PN-F Profile containing the main details of the PN-F (i.e. identification, means to proceed with the participation protocol and policies that rule the federation) and store it in the SCMF. The PN-F Profile is made public and candidates (i.e. other PNs) go on a dialogue with the creator to see whether they are allowed to enter on the PN-F or not.

In order to proceed with the next step in the PN-F participation phase, the PN-F Creator and potential PN-F members (i.e. other PNs) need to be able to authenticate each other and to establish a security association that can be used to secure all ensuing communication. A new PN component, called Personal Network Directory Service [7], is also introduced as

the identity provider (i.e. trusted third party entity). The PNDS, operated by a service provider, acts as a Certificate Authority (CA) providing X509 certificates which associate public key with a particular user. The PNDS authenticates users via GSM's Short Message Service (SMS). The PNDS certificates are leveraged by CPFP to establish bilateral trust relationships between the PNs that are afterwards enforced each time the two PNs communicate under the auspices of any federation.

After this authentication and security association step, the PN-F member can actually join the PN-F. A PN-F participation profile that lists the services that the new PN-F member will make available within the PN-F is created and stored in the SCMF. At this stage, each member knows in which PN-Fs she/he participates, which other PNs are currently member of the PN-F and, optionally, what services are made available by these members. This information can in any case be retrieved through a PN-F wide service discovery mechanism since the MSMP implementation has been extended to support also this feature.

The concept of a network overlay selected to realize secure PN-F communication enables all PN nodes of the PN-F members to become part of the PN-F overlay. In order to separate the internal PN communication from any PN-F communication, every PN-F will also have its own PN-F addressing space (defined in the PN-F profile) and every involved node will obtain a unique PN-F IP address within this addressing space. In a similar way to the PN, the PN-F overlay will be established. Neighbouring clusters of different PNs are discovered through the use of beacons. When establishing secure associations with a PN, a pair-wise (1 key for each pair of PNs) primary master key is exchanged (using the PNDS certificates through CPFP). This key is then used for deriving link level session keys used to secure the link between nodes of different PNs. Using this secure link, PN-F routing information can be exchanged, forming a PN-F cluster. For the interconnecting of clusters of PNs at different locations, the PN Agents of the respective PNs are used. All clusters location information can be retrieved by contacting the PN Agents of the other PN-F members. Tunnels are then established using the primary master key as basis and routing information is exchanged, creating full end-to-end secure PN-F connectivity.

The service discovery framework is extended to allow PN-F service discovery and use. Higher-level SMNs, called PN-F Agents, are introduced. The PN-F Agent implements all the PN SMN functionality but is exclusively dedicated for storing and discovering PN-F resources and services at PN level. One PN-F Agent per federation is activated within a PN. The PN-F Agents of each participant interact in a peer-to-peer manner via a PN-F service overlay to provide PN-F wide service discovery according to PN-F participation profiles. The service related functions provided by the GUI are extended to the PN-F case.

In the PN-F case, the SCMF also provides access to context information from the members of the PN-F [8]. The SCMF of each PN has a dedicated Context Management Gateway (CMG). The CMGs interact with each other, exchanging context information, while enforcing the privacy policies of the user.

## 3. Testbed Description

Testing the functionality of even a single PN needs several clusters with a reasonable number of devices in each one of them. Therefore, a minimum set of hardware devices was defined as requisite to set up and test a PN and PN-F platform. Indeed, a fully operational system has now been built through a process of conformance verification, integration, and interoperability testing of the different baseline components described before.

Different partners are hosting different parts of the PN/PN-F platform in their premises, as shown in Figure 5, with all individual parts interconnected via the Internet to form a distributed testbed, as prerequisite to validate how the developed PN/PN-F solutions and pilot applications function over real-life network conditions.

In order to promote and ease the usage of the system among the partners and developers of pilot services in particular, a set of system installation and usage guidelines have been developed. The distributed testbed is set up on four different laboratories across Europe and has been the cornerstone for the integration process. The testbed is composed of both laptops and PDAs in order to showcase the feasibility of the system to be run on real user equipment. All the integrated components are implemented to run over the Linux Operating System. For the high capable devices like laptops, the Ubuntu distribution was selected while for the PDA-like devices, the project decided to use Nokia Internet Tablets. Accordingly, easy to install SW packages have been created for the two selected kinds of MAGNET nodes, while the respective installation guides are planned to set all software from scratch. Thereby, the PN/PN-F Platform towards pilot services is now a reality, and the necessary means have been set to promote its use among application developers and potential end users.

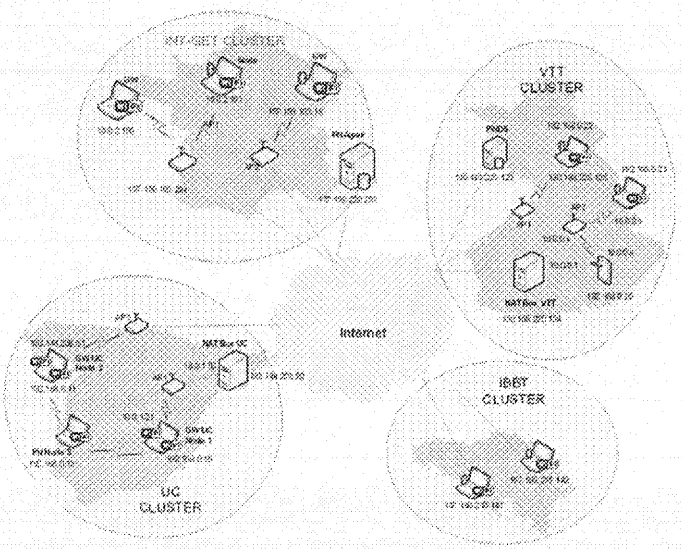



*Figure 5: Physical Location of the Remote Testbed*

## 4. Testbed Scenarios and Objectives

The PN/PN-F platform is currently being used for testing the developed PN and PN-F functionality, as described in the previous sections.

The availability of this dedicated "always on" testbed was the only viable way to guarantee that all participating partners can assess the real usability of the pilot applications and the performance of the underlying platform. Since the objective of the platform is not only to prove the feasibility of a PN system but to support the pilot services atop of it, it is possible to assess the usability of the PN concept from a user-centric viewpoint. Indeed, the same platform will evolve via further performance testing to serve also as the platform to support the pilot services.

## 5. Pilot Services

The transparent and seamless federation of networks and services comprises a highly novel feature in the MAGNET project. By federating networks, the amount of services potentially available to users increases dramatically as does the radius of action for individual users. Services can now be based on collaborative behaviour among individual users and/or nodes in a networked infrastructure. The impact of physical distances diminishes thus as nodes become interconnected using MAGNET technology. MAGNET selected Pilot Services goes around two main topics: 'The Lifestyle Companion' and 'The Ice-breaker'.

These two MAGNET pilot services intended to demonstrate the MAGNET project in its entirety are initially analyzed and described. This analysis focuses on their general importance for MAGNET as seen from a user's perspective. Through this analysis, three key issues are identified as being of special importance for the two pilot services; federation, trust and initiative.

The Lifestyle Companion service targets primarily diabetic users who have a desire for being in good shape by using a fitness centre as well as monitoring and adjusting their blood glucose level. This service allows these users to automatically monitor and register their blood glucose concentrations and receive recommendations for insulin injections based on this input. The service furthermore offers a "personal trainer" functionality by which the service acts as a fitness trainer guiding the user through fitness programs in a fitness centre keeping track of repetitions, load settings, etc. This service comprises the following core MAGNET functionalities;

- Proximity-based PN formation (enabling the user to easily interconnect an amount of MAGNET-enabled nodes into a PN).
- Location/context-aware service-discovery (providing the user with service-related information based on the current physical location of the user)
- LDR transmission (wireless transmission of low-rate data between MAGNET-enabled nodes)
- Automated proximity-based PN federation (enabling quick and easy inter-node communication when required)

The Icebreaker scenario is situated at a conference where knowledge workers e.g. journalists meet physically and exchange information. This scenario allows a nomadic worker to cooperate with one or more colleagues using shared digital material and to share computational power of individual devices. The service furthermore provides means for exchanging "digital business cards" easing the establishment of new business contacts and acting as a social 'icebreaker'. Whenever it would be convenient for the user to view data on a larger screen than currently available (e.g. a small handheld device), the service offers in addition the possibility of 'beaming' information from one device to another. Large quantities of data on a PDA can in this way be projected to a larger (MAGNET enabled) public screen for closer inspection. The scenario addresses:

- context awareness applied as physical access control: mobile device as ticket to the conference, and as settings change of the mobile devices according to the activities of the users
- Location/context-aware service-discovery in the shape of the 'Icebreaker' services, offered to the guests at the fair, and notification of the users of 'Icebreaker' according to the context.
- PN discovery based on filtered search in local area allowing for the user to explore the presence of available PNs applied as social software embedded in a physical setting
- seamless high data rate transfer from device to device (a mobile unit to a screen) to demonstrate the 'Public Screen' concept and device discovery / device management and in general demonstrating the concepts: 'digital handshaking' and 'digital hospitality'
- exchange of a digital business card as demonstration of a temporary PN-F formation
- forming of a long term ad hoc PN-F for the purpose of collaborative work

## 6. Conclusions

This paper has described the main aspects of the implementation of a full-blown system fulfilling the key requirements imposed by the Personal Networking concept. It has presented the different components that compose the system and portrayed how they

support the system functionalities. Additionally, the deployment of a pan-European Personal Networking testbed has been depicted. The implementation of a PN and PN Federations system has driven part of the MAGNET project research agenda that has its target on making Personal Networks happen. Indeed, some aspects of the initial specification have been revisited since particular issues have only shown up during the implementation and deployment phase. The deployment of the distributed testbed has been helpful not only because it has eased the system integration but also because it has set the basis for a larger scope platform that can be used to perform usability tests with real users.

The following steps for the implemented system and the testbed are to go into a thorough system performance evaluation both from a network and user centric point of view. Specific tests will be carried out in order to measure the response of the system under specific scenarios. Pilot services will be implemented atop of the system and usability tests based on these applications will be carried out. Besides the performance evaluation, usability of PN services is central for the success of a developed and implemented PN architecture. Focus will be to fundamentally develop a usability concept which is applicable for understanding the performance and user acceptance of PN services, and to apply this usability concept to selected pilot services.

## Acknowledgements

This paper describes work undertaken in the context of the IST-FP6-IP-027396 'My personal Adaptive Global Net and Beyond' MAGNET Beyond is a worldwide R&D project within Mobile & Wireless Communication beyond 3G. MAGNET Beyond will introduce new technologies, systems, and applications that are on the same time user-centric and secure. Please visit: www.ist-magnet.org

## References

[1] I.G. Niemegeers and S. Heemstra de Groot, "From Personal Area Networks to Personal Networks: A user oriented approach", Journal on Wireless and Personal Communications 22 (2002), pp. 175-186.

[2] E. Gustafsson, A. Jonsson, "Always best connected" IEEE Wireless Communications, vol. 10, nº: 1, 2003.

[3] L. Munoz, L. Sanchez, J. Lanza, M. Alutoin. S. Lehtonen. D. Zeghlache, M. Girod Genet, W. Louati, J. Hoebeke, I. Moerman, G. Holderbeke, M. Ghader and M. Jacobsson, "A Proposal for Self-Organizing Networks", Wireless World Research Forum Meeting 15 (SIG 3), White Paper, Dec. 8-9 2006, Paris, France

[4] J. Hoebeke, G. Holderbeke, I. Moerman, M. Jacobsson, V. Prasad, N. Wangi, I. Niemegeers, S. Heemstra De Groot, "Personal network federations", 15th IST Mobile & Wireless Communications Summit, Myconos, June 2006

[5] J. Hoebeke, G. Holderbeke, I. Moerman, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, L. Sanchez, J. Lanza, M. Alutoin, K. Ahola, S. Lehtonen, J. J. Pallares, "Personal networks: from concept to a demonstrator", 15th IST Mobile & Wireless Communications Summit, Myconos, June 2006.

[6] L.Sanchez, J.Lanza, R.L.Olsen, M.Bauer, M.Girod-Genet, A Generic Context Management Framework for Personal Networking Environments, Pernets Workshop 2006, Mobiquitous, July 2006.

[7] M. Alutoin, K. Ahola, S. Lehtonen, J. Paananen, "Personal Network Directory Service", Telektronikk Journal, Volume 1.2007, March 2007.

[8] R. L. Olsen, M. Bauer, L. Sanchez, J. Lanza, "Self Organisation of Context Agents in Personal Networks and Federations", 10th International Symposium on Wireless Personal Multimedia Communications, India, December 2007

# ICT-MobileSummit 2008

**10 - 12 June, Stockholm, Sweden**



## Preface

In the context of convergence, the 17th ICT Mobile and Wireless Communications Summit addresses the challenges of Future Ubiquitous Networks based on mobile and wireless communications, complemented by fixed infrastructures.

Supported by the European Commission and eMobility and Technically Co-sponsored by IEEE, the ICT-MobileSummit's reputation is based on high quality paper and poster sessions that showcase original results in all areas of wireless communications systems and networks, including Mobile and Fixed, Terrestrial and Satellite. All papers are double blind peer reviewed by at least two Members of the Technical Programme Committee.

The ICT-MobileSummit 2008 Conference Proceedings gathers together a comprehensive collection of over 200 paper and poster contributions from Europe, North America and Asia sharing insight, cutting edge research and good practice.

Reflecting the breadth and depth of the Mobile related research undertaken by the contributors, the contents are broken down into 11 broad thematic areas. These are: 4G & Beyond; Future Internet; Sensor Networks; Wireless and Fixed Broadband; Short Range Wireless Systems, Piconets; Ubiquitous Content; Application and Service Enablers; Components for Wireless Systems; Pervasive and Trusted Networks; Research Strategies and Challenges and Fixed, Mobile, Content Convergence. Papers within each thematic area are grouped as Issues, Applications and Case

Studies, reflecting their primary focus.

We would like to acknowledge the valuable contribution of the Technical Programme Committee who provided authors with actionable feedback in finalising their papers for publication, and the encouragement and support of the European Commission and eMobility.

Paul Cunningham

Miriam Cunningham


ICT-MobileSummit 2008
Conference Proceedings
ISBN: 978-1-905824-08-3
To view Conference Proceedings
open 'toc.html'
10 - 12 June 2008
Stockholm, Sweden
ICT
MobileSummit
www.ICT-MobileSummit.eu