

Architecture of a Personal Network service layer

Rieks Joosten¹, Frank den Hartog¹, and Franklin Selgert²

¹TNO, Information- and Communication Technology
Brassersplein 2, P.O. Box 5050, 2600 GB Delft, The Netherlands
{Rieks.Joosten, Frank.denHartog}@tno.nl.

²Koninklijke KPN N.V
Maanplein 55, P.O. Box 30000, 2500 GA Den Haag, The Netherlands
Franklin.Selgert@kpn.com

Abstract. We describe a basic service architecture that extends the currently dominant device-oriented approach of Personal Networks (PNs). It specifies functionality for runtime selection and execution of appropriate service components available in the PN, resulting in a highly dynamic, personalized, and context-aware provisioning of PN services to the user. The architectural model clearly connects the responsibilities of the various business roles with the individual properties (resources) of the PN Entities involved.

1 Introduction

Recently, a significant research effort has been made in the new concept of Personal Networks (PNs), most notably by the European FP6 projects MAGNET (BEYOND) and Ambient Networks [2]. Confusingly, both projects meant something slightly different with PNs. MAGNET defines a PN as “consisting of a core Personal Area Network (PAN) extended with clusters of remote devices which could be private, shared, or public and able to adapt to the quality of the network accessed” [3]. In a nutshell, this is about a user having remote access to his other devices. Ambient Networks, however, considered PNs more like defined by 3GPP, as “a PN consists of more than one Personal Network Element (PNE, i.e. either a single device or a group of devices) under the control of one user, providing access to the serving mobile network. The PNEs are managed in a way that the user perceives a continuous secure connection regardless of their relative locations [4]”. This is more about redirecting sessions to the device that is most convenient to the user at a given time.

Both definitions have in common that they are oriented towards device access and device connectivity. One of the major results of the Dutch Freeband project PNP2008 is the understanding that, from a user perspective, the added value of PNs is more in accessing personal services and content, provided by either personal devices or other devices. Device access is then a *sine qua non*, but does not guarantee access to services offered by the device, nor does access to a personal service guarantee any control over the device which offers it.

This paper describes a basic architecture of a service layer extension for PNs as envisaged by MAGNET. As such we redefine PNs to include this service layer as

follows: “a user-centric environment of potentially globally distributed resources, such as devices, services, content, network-nodes, etc.” Devices, both within and outside PNs, host services and content that are dynamically configured to collaborate as individual applications whose functionality is enhanced by personal preferences and context information. The main challenge is to construct applications at runtime, from services that are technically available and the user is allowed to access from a business point of view.

2 Architecture

The architecture consists of PN Entities. PN Entities are instances of PN Entity Types, which are devices, network nodes, content, applications and other services. PN Entities are associated with the following PN business roles:

- Owners, who are responsible for issuing permissions and/or conditions under which the specific PN Entities they own may be used.
- Providers, who are responsible for the correct functioning of PN Entities at runtime including their operational management.
- Customers, who are responsible for the use of PN Entities within the context of a PN User Session, which may result in having to pay for that use.
- Users, who are individuals that within the context of a PN User Session actually use PN Entities.

The relations between these roles and PN Entities are graphically shown in the left part of Fig. 1. Notice that Customers, Providers and Owners may be organizations rather than individual persons, but Users may not. And only individuals can use or manage PN Entities, while organizations cannot. Even though organizations bear responsibilities, they always need a human individual that represents the organization to get something done.

Fig. 1 shows, on the right, the most relevant part of a functional architecture of a PN service layer. The central entity is the PN Administration Integrity Service (PNAIS). Its role is to preserve and provide guarantees with respect to the integrity of the administration data that resides in a potentially distributed database, the PN Provisioning Administration (PNPA). The integrity of the PNPA is defined as compliance to a set of constraints that have been specified explicitly for the PNPA, in terms of what defines the concepts (Device, PN Entity, User, etc.), and the relations between them. The PNAIS must enforce, in a runtime fashion, this set of constraints.

The User Agent & Authentication (UA) component manages the communication between individuals and their PNs, and ensures that PN Users only use services in their own PN. To achieve this, the UA must (a) interact with the user, (b) provide and maintain the context (which includes a user-id) within which applications can run, (c) provide messaging authentication services, (d) spawn applications upon request of the user and (e) be able to create sessions for different users and switch between them. The Service & Content Discovery (SCD) component selects service and/or data components that satisfy the constraints of a specific request for functionality and/or content. It matches the specifications of the available components with the constraints from the request, and passes the set of selected components to Access Control (AC).

The AC component prevents the illegitimate use of services and/or content. Its task is to filter out service and/or content components from the set provided by the SCD, for use in the context of a specific application session. This is done by deciding for each component whether its execution/access is authorized, which means it must satisfy all constraints (rules) imposed by its Owner, Provider, Customer and User. The Service Context Service component enables services to enhance their efficiency and/or effectiveness by determining and using information from the context of the service relevant for the various PN Entities involved.

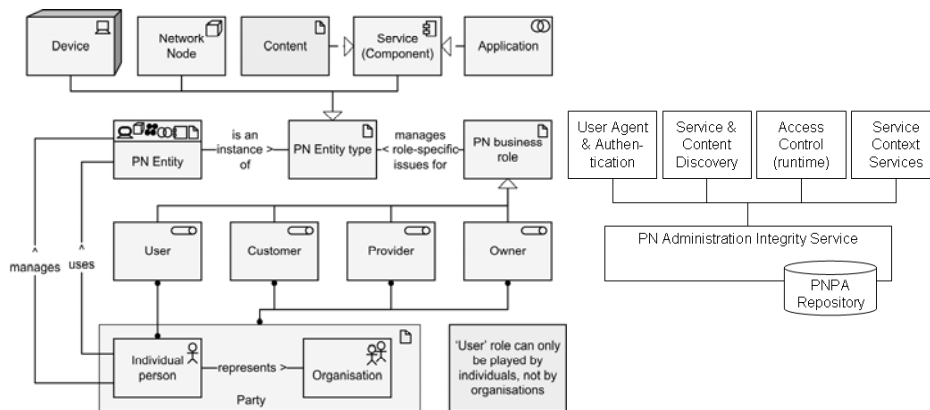


Fig. 1 PN architectural model (left), and functional blocks (right)

We implemented this architecture in a demonstrator as described in [5,6]. On the whole we conclude that the demonstrator works well. However, for commercial deployment a number of research issues still need to be tackled. For instance, what are the consequences of such architectures on the business processes of organizations such as IT departments of the work place? How should the PNPA and the rule engines be implemented? Centralized or distributed? How should the rule engines be constructed? How are security, privacy and ease of use in a PN managed in a balanced way? What algorithms and protocols are needed for supporting automated decision-making and follow-up? For example, PN content management requires intelligent, dynamic rules and protocols for replication, streaming, and deleting of content on the various PN Entities [7].

3 Conclusions and future work

The PN service layer architecture and the PN network layer architecture complement each other in the sense that the PN service layer assumes PN networking functionality, and the PN network layer is only useful if something is actually done with the messages it sends around. The service layer architecture specifies functionality for runtime selection and execution of appropriate service components

available in the PN, resulting in a highly dynamic, personalized, and context-aware provisioning of PN services to the user.

The service layer also imposes new requirements, for example with respect to the development of service components. Developers of reusable service components for PNs may no longer rely on assumptions with respect to the applications interacting with their service component. As a result, high quality PN service components are much more sophisticated than the classical, silo-oriented application programs we often find in mobile phones.

We experienced that a pure device-oriented approach to PNs inevitably leads to a lot of discussion about the role of commercial operators and service providers in realizing and providing PN services to users. The PN service layer architecture provides a firm base to solve these issues. The architectural model clearly connects the responsibilities of the various business roles with the individual properties (resources) of the PN Entities involved. Any desired PN service component and/or its management that is too taxing for the device or too complex for the user to manage, may be provided by a centralized server instead.

It is obvious that achieving universal Personal Networking is highly dependent on standardization of mechanisms, protocols, data models, etc. of the various PN Entity Types involved. Unfortunately this may concern more or less every standards development body in the world, given the degree of heterogeneity that is inherent to PNs. For the standardization of the service layer components we are currently targeting the Open Mobile Alliance, which recently started a Converged Personal Networks Services work item. There we are advertising the service-oriented approach [8], which is well adopted by many partners.

References

1. Prasad, R.: Personal Networks and 4G. In: 49th International Symposium ELMAR-2007 focused on Mobile Multimedia, pp. 1--6. IEEE Press, New York (2007)
2. Niebert, N., et al.: Ambient Networks: an Architecture for Communication Networks beyond 3G, IEEE Wireless Communications 11 (2), 14--22 (2004)
3. Niemegeers, I.G., Heemstra de Groot, S.M.: From Personal Area Networks to Personal Networks: A User Oriented Approach. Wireless Personal Communications 22 (2), 175--186 (2002)
4. Service Requirements for Personal Network Management (PNM) Stage 1. Technical specification TS 22.259 V9.0.0, 3GPP (2008).
5. Hillen, B., Jager, E., Joosten, R.: Detailed PN Management Functionality. Technical report Freeband/PNP2008/DA.2.3, Freeband PNP2008 (2008)
6. Joosten, R.: Light-weight Security Services for an Integrated Personal Network Demonstrator. Technical report Freeband/PNP2008/D2.13v1.0, Freeband PNP2008 (2007)
7. Hartog, F.T.H. den, et al.: First Experiences with Personal Networks as an Enabling Platform for Service Providers. 2nd International Workshop on Personalized Networks , pp. 1--8. IEEE Press, New York (2007)
8. Selgert, F., Hartog, F.T.H. den.: On the Definition and Architectural Needs of Personal Networks. Contribution OMA-TP-CPNS-2008-0032-INP_CPNS, Open Mobile Alliance (2008)