Stephan Rupp, Matthias Duspiva and Wolfgang Klenner

Configuration Management as Condition for Service Innovation

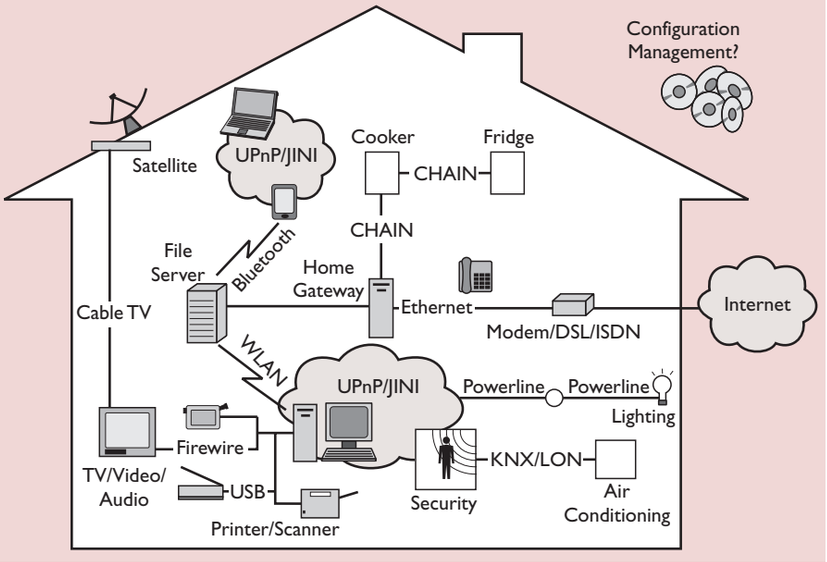
As microprocessors keep entering into more and more devices around us, there is a growing potential for service innovation, comfort and individuality. In particular, context-based applications promise to intelligently follow the specific needs of the individual user. However, complexity around us is growing. Who will handle the many ways of configuration? Who will keep intruders, spam and malicious software away? Who will care for software updates in this environment? If there is a trend from personal computers to personal networks, it certainly demands new ways of configuration management in order to live up to its promise. Handling a mess of CD-ROMs, as with today's PCs, including individual downloads from the Internet and paper clips to follow up a variety of serial numbers, keys and passwords hardly seems to be a viable way into the future. Also, unlike a professional intranet, the costs of maintaining personal networks and home networks will only allow for a modest amount of manual administration. Such networks will need to be self organising and will need to provide innovative means for maintenance and configuration management. This paper describes potential technologies to provide self organisation of networks, as well as potential solutions for configuration management. As a potential business model for the provisioning of configuration management, identity management may be provided as a service (for example, by a mobile network operator), as well as configuration management for specific classes of devices as a service of an ASP.

Introduction

Most of the systems and devices in today's environment contain a microprocessor and so are driven by software, and this will continue into the future. In reality, the development and care of software is a continuing process. Sooner or later, any device will need a software update. Currently, this problem is difficult or impossible to address by the isolated industries (in particular by manufacturers of consumer electronics and domestic appliances), because the required technologies originate in communication technologies and information technology (such as the organisation and operation of networks, data models, semantic models). In other cases, the configuration of a system from subsystems needs to be read out automatically (for example, by using radio frequency identification (RFID) devices). Also in this case, the information needs to be analysed, processed and stored.

Over the past 10 years, numerous different approaches have been utilised for the communications and the organisation of home networks (see Figure 1). Among the

Figure 1 State of the art in home networks



Authors
Stephan Rupp, Matthias Duspiva and Wolfgang Klenner
Alcatel SEL AG
Contact: Stephan Rupp
Alcatel SEL AG, Central Services, Lorenzstr. 10, 70435 Stuttgart-Zuffenhausen, Germany
Tel: +49 711 821 46448
Mobile: +49 171 30 20 867
Email: S.Rupp@alcatel.de

established technologies and standards today are:

- *Communication technologies*: LAN, Wi-Fi (IEEE 802.16.x), Bluetooth, infrared, Firewire (IEEE 1394 or IEEE 802.15.3), powerline.
- *Home bus systems*: LON (LonWorks Local Operating Network, Echelon), EIB (European Installation Bus, EIBA), EHS (European Home System of EHSA), BatiBUS (BCI), KNX (Konnex, Konnex Association), CEBus (CEBus Industry Counsel, CIC), LCN (Local Control Network, Isendorf), CHAIN Platform (CECED Home Appliances Interoperating Network), Server@Home (Siemens).
- *Software technologies for service discovery, respectively 'zero-configuration' networking*: Universal Plug and Play, Bluetooth Discovery, JINI, JXTA, SLP.
- *Application frameworks for residential gateways*: OSGi.

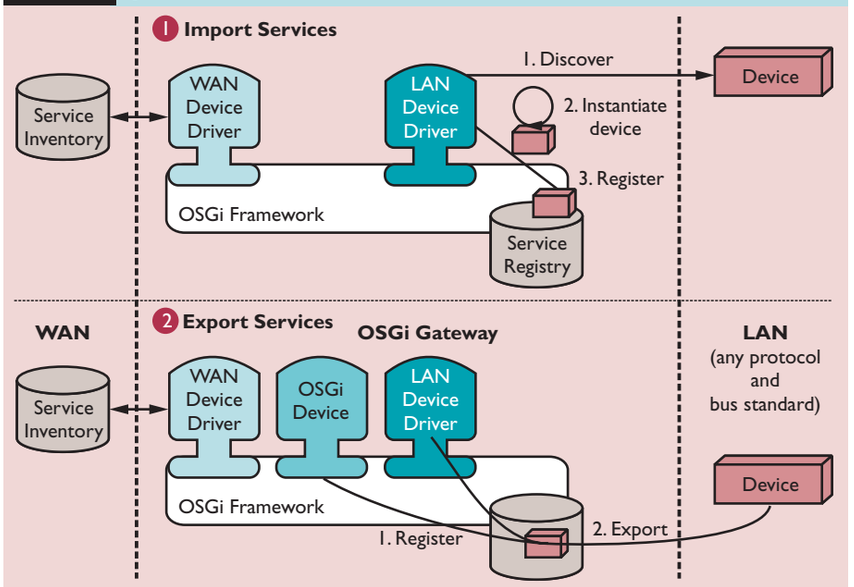
While the existing approaches for communications and configuration management in home networks each have their strengths, they appear to represent isolated solutions in lack of:

- a comprehensive definition of *roles and responsibilities* in a web-based scenario beyond the device and its manufacturers;
- a comprehensive *system for classification* of devices, resources, users, roles, relations and interactions between them;
- the use of *semantic models and meta-models* to handle information; and
- the use of *application frameworks* within network elements and between network elements to cope with heterogeneous communication systems.

This may explain the current lack of success of home communication systems on the market. Over the same period of time, considerable advances have been made in information technologies and communications, mainly in the area of enterprise networks and wide area networks. New technologies have been applied in order to provide services over the Web and to integrate services and applications in enterprise networks. The venue of broadband connections at affordable rates (for example, flat rates) for consumers have put many of the approaches, which apply today in enterprises and wide area networks, within reach of consumers and web-based service offerings for consumers.

This paper is organised in the following way: The next section describes how interaction between a multitude of communication technologies in home networks and personal networks may be achieved. The following section explains the essential concepts to organise networks and to match supply and demand of resources and services. Then, a system for classification of resources, services and roles is introduced. The combination of concepts introduced so far allows to create a service architecture for configuration management. The next section describes identity management and configuration management in a rather simple scenario of providing configuration services for mobile phones as target device. Finally, the paper concludes on the state of achievements, the maturity of available technologies, viable business cases and further steps.

Figure 2 Interworking between a multitude of protocols and bus systems



From Personal Computers to Personal Networks and Home Networks

Home networks and personal networks do not enjoy the same level of administrative support as an intranet in business. They need to organise themselves in the most automatic way. Typical buzzwords in this context are 'zero configuration' or 'plug and play'. The idea is, that a new component (such as a new printer) will make itself known to other components as soon as it is plugged in, so it can immediately be used. Today, this is far from reality.

To organise home networks, the following problems need to be addressed:

- distributed communications over heterogeneous interfaces;
- to handle supply and demand of services in a dynamic way by one of the existing concepts for 'zero configuration'; for example, by Universal Plug and Play;
- a system for classification of devices and services (what is this?, what can it do?, how does it relate to others?);
- interworking between local networks and services offered by wide area networks – this needs to include the handling of information (what is offered?) and meta information (where to find information?, how to access this information?); and
- residential gateways to mediate between different systems in home networks and to provide interconnection to wide area networks.

A residential gateway can be used to organise home networks and to provide connectivity and access to wide area networks. Figure 2 shows the principle. One fundamental condition is that the gateway architecture supports the remote installation of modules and services. Such modules are used to communicate with devices over their respective communication system. In Figure 2, these modules are indicated as 'LAN device drivers'. If a local device supports one of the communication systems indicated in the previous section (such as UPNP over Wi-Fi, or one of the home bus systems such as CHAIN), there will be a corresponding LAN device driver on the residential gateway. As new devices may be installed at any time, the installation of such modules will need to be on demand and by remote configuration. Platform standards such as OSGi support such a modular concept including remote installation.

In the same way, the residential gateway will need to communicate with systems in the wide area network. In order to do this, corresponding modules are installed on demand on the residential gateway (so called 'WAN device drivers' in Figure 2). WAN device drivers provide the basic communication facilities to connect to configuration databases, as well as inventories and resources in the wide area network.

Service Discovery to Match Supply and Demand

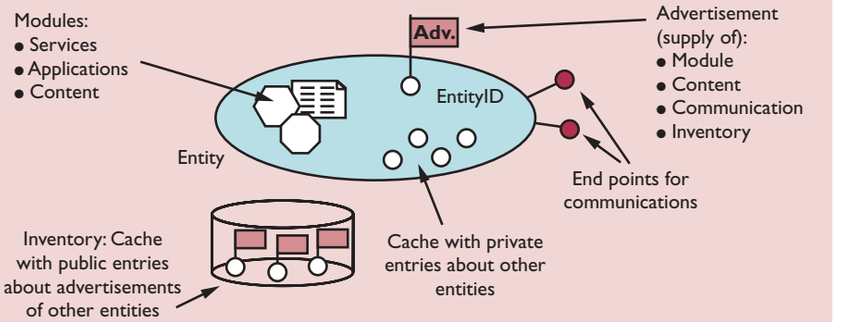
Once communication between devices is possible, the next step is to find out which devices and services are available in the home network, and what is available in the wide area network. Many technologies on the market support such concepts for *service discovery*; however they are not compliant with each other. Bluetooth, for example, allows Bluetooth devices and services in the vicinity to be identified. However, it does not allow the discovery of UPNP devices. Each of the candidate technologies that provide service discovery use their own mechanism of discovery. To make it worse, they also use their own terminology to describe devices and services (such as a printer).

Given the variety of devices in home networks, there is a need to organise corresponding information in wide area networks. It is difficult to imagine that there will be one generally accepted standard for service inventories in wide area networks, or one generally accepted institution in this area. Much more likely, there will be a diversity of offers and demands. While there may be an equal amount of diversity in wide area networks as in home networks, the concepts to provide service discovery are totally different. In a local network, it is always possible to send requests or notifications in a broadcast or multicast way. In a wide area network, the large number of entities makes this impossible. Peer-to-peer networks provide the concepts to organise information in there.

While the diversity in local networks and wide area networks can be matched by corresponding base drivers on the residential gateway (see the previous section), the organisation of information needs some general terminology (or at least the option to translate between different terminologies). Figure 3 shows the general components to handle supply and demand.

An entity corresponds to a device. Each entity may contain services, applications or content (such as files or documents). An entity can make this content accessible to other entities by placing advertisements. In order to communicate with its exterior, the entity is using communication end points (an abstract view of network addresses, protocols and ports). Communication end points are also advertised (the advertisements then contain the specific kind of interface, protocol and port). Each entity has some knowledge about other entities. This information is used to place requests. Entities that serve others as inventories allow others to share this information and to place advertisements there. The capability of running inventory services is also announced as an advertisement.

Figure 3 Service discovery – matching supply and demand



The concept presented in Figure 3 is a very general one. Most technologies which provide service discovery implement it in their own specific way (such as Bluetooth, JINI, UPNP, JXTA and others). Specific base drivers on the gateway provide connectivity and communication between different implementations. Also, OSGi provides its own inventory (the OSGi service registry) to export and import services. That is, a UPNP service may be imported to the gateway and used there like a native application. Or it may be exported to a Bluetooth device, or to a service within the wide area network. However, such a translation still needs a common terminology. For example, a device specified as a printer in UPNP terminology needs to be translated into the meaning of 'printer' in Bluetooth terminology, or the same thing in any other terminology. For wide area networks, we have chosen the JXTA as the best suited technology to organise information in a peer-to-peer way. The development of corresponding base drivers on OSGi is in progress.

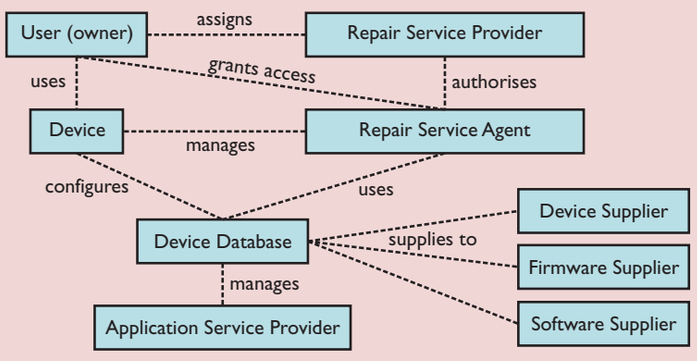
User Profiles and Device Profiles

While the solutions under investigation in the previous section of this paper can make a home network or personal network self organising, there is a need for a common terminology, which defines the meaning or everything which can be discovered and used. What is needed is a classification of devices, users, services, roles and relations. In general, such a classification corresponds to a domain model for a specific area of application. In the context of configuration management, Figure 4 shows an example of such a classification.

The roles and responsibilities shown in Figure 4 may be summarised as follows:

- *User:* Uses devices and services in his/her household or business (small enterprise, SOHO), subscribes to configuration management by a service provider, subscribes to identity management by an identity provider. The user also is the legal owner of the equipment and liable for any misuse done with it.
- *Device supplier and software suppliers*: Holds databases for device classification, software releases and corresponding authorised devices, or provides access to such information by operating a corresponding network infrastructure (databases, inventories). Software suppliers may also specialise on specific operating systems or provide specific operating systems.
- *Service providers*: Service providers provide for example software for devices, but also repair services, or configuration services. Other service providers are focused on

Figure 4 Roles and relations



infrastructure, such as the hosting of databases and applications, which are used for configuration management in the proposed solution.

- *Service organisation*: An organisation which provides services including repair services and workshops for devices. For mobile phones, this may be the phone shop and customer support organisation of a mobile network operator. For domestic appliances (or other devices such as consumer electronics or cars and vehicles) the corresponding service organisations of manufacturers and services apply.

There are many actions, which need authorisation by the user and support or intervention from service providers in the wide area network. Among such actions are software updates, removal of malicious software, back-ups of data or images, taking snapshots from the local network for audits, or installation of new software. Also, the user will prefer a choice of options for services to be installed onto his/her devices and offered to its devices.

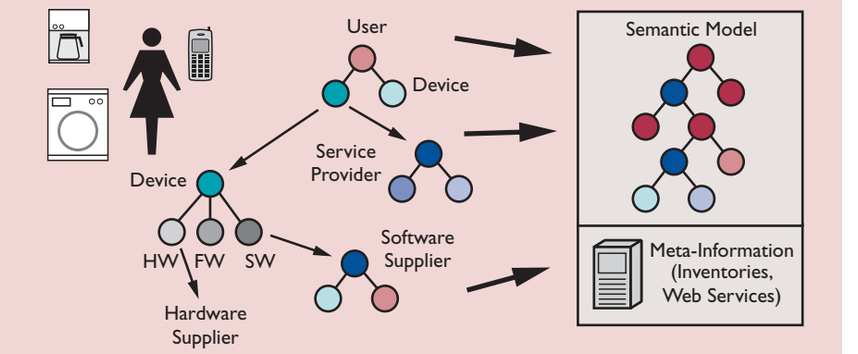
The role of providing authentication may be assigned to a so-called *identity provider*, who identifies users and devices as a service. Users of the identity management (users, device suppliers, software suppliers, service providers) have a trust relationship with the identity provider, but not necessarily with each other. There are different ways to provide identity management, which all appear to be viable in the context of configuration management. An alternative to a centralised approach to identity management may be the use of certificates and a public key infrastructure, such as PGP.

One of the scenarios for remote configuration is the *remote configuration of mobile phones*. Other scenarios are the *remote configuration of residential gateways* and the *remote configuration of domestic devices*. In the first scenario (remote configuration of mobile phone), the mobile network operator most probably also represents the configuration service provider. In other cases, an identity provider may support authentication of devices and users.

Among the concepts and technologies chosen to support configuration management are:

- The *separation of roles and responsibilities* (users and their devices, identity management, device profiles, service organisation, supplier of devices and software, service providers).
- The definition and *usage of semantic models* to classify devices, to represent knowledge, and to provide schema transformations according to the above mentioned roles and responsibilities.

Figure 5 Use of semantic models for configuration management



- The definition and *usage of meta data* to locate information and to provide access to information, such as inventories to be operated by service providers.
- The development of *methods and tools for service providers*, suppliers and other parties involved in configuration management. Methods and tools may be reused and adapted to their specific needs.
- The integration of existing technologies into a *Web-Services framework* (as application framework between network entities).

Figure 5 shows an overview about the use of a semantic classification and the use of meta-information to support configuration management. User profiles are extended by device profiles. Device profiles contain information about the type of device, its supplier and state of software. Equally, service providers and suppliers of devices and software are described. This classification may be populated (instantiated) with the corresponding resources. Meta-information is used to locate and access such resources. This concept is able to support a diversity of systems, roles and terminologies. Rather than trying to establish one common standard on roles, procedures and terminologies, it makes information explicit and accessible. Implementation may use current technologies such as semantic models (for classification and interpretation) and Web Services (to provide access to meta information and resources).

Identity Management and Configuration Management

A simple case for configuration management as presented in this paper is the case of a mobile network operator that provides configuration management to the mobile phones of its customers. Such a service would be useful to provide back-ups and images of their mobile data and applications, as well as to regularly decontaminate their devices from malicious intruders. Among the benefits of such a service is the capability to change to a new device of a different supplier, while still keeping the old environment (such as address book, calendar entries, photos, ringing tones, applications installed on the device).

In this case, the mobile network operator also acts as identity provider for configuration management. Mobile network operators are doing this already: they keep profiles of their own customers and are aware of the services that they use (GSM, UMTS, MMS, etc) and their corresponding tariffs. Such information is stored in *customer profiles* (see Figure 6, upper storage on the right). In order to provide

Figure 6 Identity management and configuration management for mobile phones

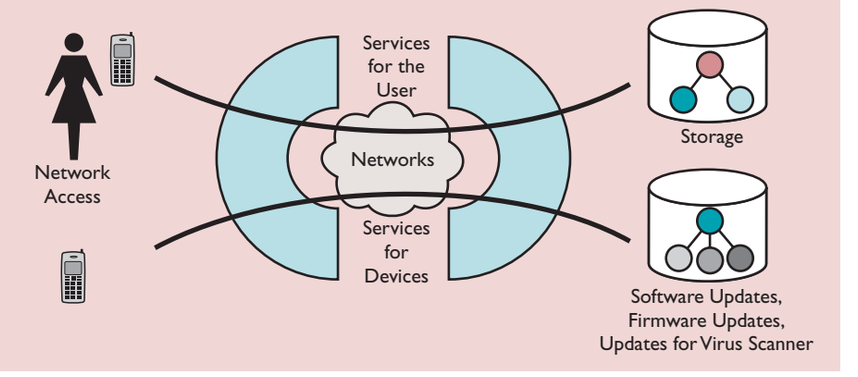
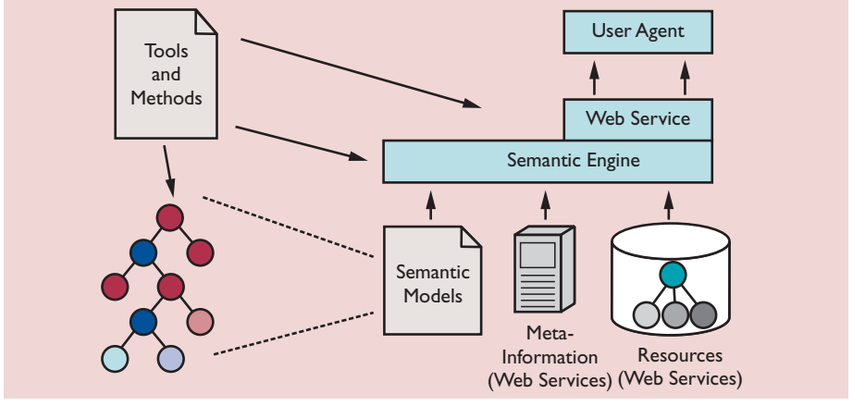


Figure 7 **A Web-Service framework for configuration management**



configuration services for mobile phones, the mobile network operator would need to extend the customer profiles with information about the devices they use, as well as with information about configuration services and pointers to other resources (such as hardware releases, firmware updates, snapshots of applications installed, software updates, updates for virus scanners, etc). This information is obtained from semantic models and meta-models.

The provision of identity management and configuration management could be extended to other devices than mobile phones (such as the residential gateway and further devices in the home network or personal network). This affects the business of a mobile operator in the following ways: (1) Technically, user profiles are extended by profiles of devices, which the users wants to have included into the configuration management service. Of course, the drawback of such a solution is that the mobile network operator gains knowledge about the registered devices; that is, loss of privacy for the user. (2) Operationally, the mobile network operator now is acting as identity provider and identifies devices. Each time a user requires access to a mobile network, the 'fingerprint' of the user is checked in order to provide access to the network and the services. This fingerprinting takes place through the SIM-card by a cryptographic method (respectively the USIM-card in UMTS both for mutual authentication between network and user). If this type of identity management is extended to configuration management, the network operator also fingerprints the devices that a user has registered. This may be achieved in different ways (cryptographic methods), but basically the approach is the same as is done with users already.

Remote configuration of mobile phones by the mobile network operator represents the most simple case. In general, third-party service providers may be a more likely scenario to provide configuration management. A third-party is not limited to the customers of one specific mobile operator, but may focus on one specific device supplier or services for one specific operating system. Also, in general, there are more devices involved, and more intermediate steps (for example, configuration management for residential gateways or devices in home networks which are accessible through residential gateways). For such scenarios, roles, responsibilities and relations are more complex.

Figure 7 indicates the infrastructure which is needed to provide configuration management as a service. Models, methods and tools may be integrated into a Web-Services framework. Models and methods may be published as standards to be imported into the framework by the parties involved. In summary, the following components are required:

- A *Web-Services framework* for configuration management, which allows user demands, device profiles and available resources and services to be matched on the Web. The Web-Services framework consists of a system for classification of roles and relations, the use of *meta-information* to locate and to query information, as well as *resources* for the players and devices involved.
- The use of *semantic models* in order to classify devices, network elements, services, roles, relations and interactions. Ontologies for devices, network elements, services, roles, relations and interactions are kept in the Web in order to allow the import of the ontologies to players involved. Semantic models are also used to drive the semantic engine within the Web-Services framework.
- A modular architecture for *residential gateways*, which allows the different and heterogeneous protocols, systems and concepts for communication and interaction between devices in the home network to be accomodated. The interworking between different technologies and standards is achieved by (1) the capability to remotely install matching *device drivers* (by remote configuration) for the local area network and wide area network, and (2) the use of service *inventories and mediation* between different terminologies (by schema translation and import and export of services).
- *Methods and tools or the provisioning of configuration management* for specific classes of devices. Such methods and tools may be provided by application service providers. They apply for the following areas of application:
  (1) configuration of mobile phones,
  (2) configuration of residential gateways,
  (3) configuration of domestic appliances.

Conclusions

The key concepts presented in this paper have been analysed by conceptual studies and trial implementations. OSGi proves to be a capable platform to import and export services from different technologies and thus to translate between different concepts for service discovery. The number of bundles we have been implementing is still limited, but the concept is feasible for the chosen candidate technologies (UPNP over any kind of LAN, Bluetooth). Concerning wide area networks, OSGi JXTA bundles are in preparation. Although OSGi still is a young technology, there is a surprising amount of free software available. We plan to contribute to the open source community by publishing our OSGi bundles later this year. Remote configuration is contained within OSGi by definition. There is still a limited number of low-budget embedded systems on the market to carry OSGi, but we expect this situation to improve, for example together with the progress of Linux-embedded systems for WLAN routers and modems for broadband access.

On Web-Service frameworks, data models and service architectures, we have positive feedback both from commercial projects as well as from research projects. The framework presented in this paper is in line with the concept which is being developed in the FLEXINET research project (FP6 IST1-507646). Concepts about personal networks have been reflected within the MAGNET project (FP6 IST1-507102). Although this project follows a more conventional approach to organise networks, it contains an infrastructure to provide identity management and security domains, which is in line with the needs for configuration management.

Semantic models are currently being used in commercial projects as an effective and promising way to provide the integration of information (that is, to integrate isolated sources of data and mediate between them). One of the buzz terms in this area is 'enterprise information integra-

tion'. Commercial design tools are available, as well as open source design tools (for example, Protege), and semantic engines. Also, there are many emerging activities concerning the semantic web. In this paper, we only propose to apply those technologies for a different area of application; that is, classification, schema transformations and schema evolution in the context of configuration management. The use of XML as notation makes any of the available tools seemingly compatible, although not necessarily from a conceptual point of view. The assumption is that any of the emerging concepts that will become most popular will apply for this area of application.

The general conclusion is that a service framework for configuration management as described in this paper can be implemented with the suggested technologies. We have implemented some scenarios on emulated OSGi devices, but have not implemented a complete prototype yet, including all components. We plan to do so in future research projects and in cooperation with partners from the industries and academic institutions.

The critical path for configuration management certainly is the availability of a credible business case for any of the parties involved. Our experience from delivering broadband access equipment shows that a high degree of automation during installation and set-up provides simplicity for the end-user and reduces cost for network operators and service providers. Remote configuration follows the same logic, with one significant difference: following installation and set-up, residential users do not expect further support concerning the management of their equipment. This may change.

Bibliography

1 Rupp, S., Siegmund, G., and Lopez-Aladros, R. Flexinet—A Network Service Architecture. *The Journal of The Communications Networks*, Oct.–Dec. 2003, **2**(4).

2 Klenner, W., Jenisch, M., and Rupp, S. The Intelligent Inhouse Ambient. FITCE Congress 2004, Ghent.

3 Rupp, S., and Duspiva, M. Mobile Authentication beyond SIM. Workshop on Security in Heterogeneous Wireless and Mobile Networks, Brussels, 23 Sept. 2004.

4 Rupp, S., and Krauss, J. ASP Services for Residentials—A Challenge for Network Operators. FITCE Congress 2002, Genoa.

5 Fensel, D. Ontologies – a silver bullet for knowledge management and electronic commerce. Springer, Berlin, 2003, ISBN 3540003029.

6 Fensel, S. et al. Information Integration with Ontologies – Experiences from an Industrial Showcase. John Wiley & Sons, 2005, ISBN 0470010487.

Biographies

Stephan Rupp
Alcatel

Stephan Rupp has a master of electrical engineering and Ph.D. in communications technology. From 1986–1991 he worked on the development of digital radiography systems for medical applications at Philips Research. Since 1991 he has been with Alcatel in Stuttgart, Germany. He worked in marketing and product management and was responsible for intelligent networks up until 1999, and then for network solutions. Currently, he is engaged in the design and planning of networks, systems integration, implementation of prototypes, technical consulting and business consulting. He is privately active in education (University of Stuttgart, Germany, Berufsakademie Stuttgart) and as a publisher and author for dPunkt Verlag in Heidelberg, Germany.

Matthias Duspiva
Alcatel

Matthias Duspiva completed his studies in electronics (theory of communication systems) at the University of Karlsruhe in 1976 and then joined the SEL AG. Since then he was involved in various functions in the development of digital telephone exchanges, data communication and telemetry systems, and from 1988 onwards in the development of the GSM mobile network. In 2001, he moved to the Network Services Division. Since then he has been working in Alcatel SEL Stuttgart as a consultant for network security solutions.

Wolfgang Klenner
Alcatel

Wolfgang Klenner gained a degree in Electronic Engineering at the Fachhochschule Aalen, Germany. In 1975, he started his career as Development Engineer at Alcatel SEL AG, Stuttgart, Germany, for hardware design of telemetry systems. Between 1981 and 1991, he was responsible as group and department leader for different hard- and firmware developments of small data multiplexer and supervision systems. From 1991, he was responsible for hard- and software development for access nodes and element management systems. After 1995, he was also responsible for the systems department of cable network technology. In 2002, he joined Central Business development of Alcatel SEL AG as a consultant to cable operators and new residential services. Since 2004, he has been working in the Network Solution Group as a senior manager in the field of lawful interception. He is a member of VDE/ITG, SCTE, DKE K735.