P. Najera, R. Roman, and J. Lopez, "Secure architecure for the integration of RFID and sensors in personal networks", *7th International Workshop on Security and Trust Management (STM11)*, LNCS vol. 7170, pp. 207-222, 2012.
http://doi.org/10.1007/978-3-642-29963-6_15
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure Architecure for the Integration of RFID and Sensors in Personal Networks*

Pablo Najera, Rodrigo Roman, and Javier Lopez

University of Malaga, Campus de Teatinos s/n 29071, Spain,
{najera | roman | jlm}@lcc.uma.es,
WWW home page: http://nics.uma.es

Abstract. The secure integration of RFID technology into the personal network paradigm, as a context-aware technology which complements body sensor networks, would provide notable benefits to applications and potential services of the personal network (PN). RFID security as an independent technology is reaching an adequate maturity level thanks to research in recent years; however, its integration into the PN model, interaction with other network resources, remote users and service providers requires a specific security analysis and an architecture prepared to support these resource-constrained pervasive technologies. This paper provides such PN architecture and analysis. Aspects such as the management of personal tags as members of the PN, the authentication and secure communication of PN nodes and remote users with the context-aware technologies, and the enforcement of security and privacy policies are discussed in the architecture.

Keywords: RFID security, BSN, personal network, secure architecture

1 Introduction

The emerging personal network paradigm enables the communication of all the user's devices and services in a flexible, secure, self-organizing and user friendly manner. This network paradigm should provide a base for personal and context-aware service provision as well as enable the communication with wide area networks (e.g. Internet of Things) in order to connect to remote devices or networks and offer complex and comprehensive services.

A key technology in the realization of this network paradigm are wireless body sensor networks (BSNs), formed by tiny wearable sensor nodes which, depending on the desire applications, consistently monitor user's physiological parameters (e.g. blood pressure, electrocardiogram or glucose level), recognize

* This work has been partially supported by the European Community through the NESSoS (FP7-256890) project and the Spanish Ministry of Science and Innovation through the ARES (CSD2007-00004) and SPRINT (TIN2009-09237)projects. The latter is cofinanced by FEDER (European Regional Development Fund). The first author has been funded by the Spanish Ministry of Education through the National F.P.U. Program.

the user's current activity in, either, personal (e.g. walking, reading, sleeping) or professional (e.g. repairing an airplane or controlling a fire) arenas, or monitor parameters such as temperature, humidity or radiation levels of the surrounding environment. These features are driving the adoption of BSNs in several areas ranging from elderly care and patient monitoring to novel applications in military and consumer electronics.

Although commonly overlooked as a member of the emerging personal network paradigm, another key and crucial technology in the realization of the pervasive computing vision, and the technology that is really enabling the integration of computation and communication capabilities to common and low-cost everyday objects is RFID (Radio Frequency IDentification). RFID enables the unique identification of an object as well as provide additional data about the item (e.g. characteristics or history log) by attaching or embedding an RFID tag. ITU describes RFID technology as one of the pivots that will enable the upcoming Internet of Things, turning regular objects into smart ones[1], while the European Commission expects that the use of this technology will multiple by five during the next decade. The widespread adoption of this technology combined with the novel applications enabled collides with the potential privacy and security threats that its penetration on the user's personal belongings and documentation may arise. Due to this, the research community has devoted notable efforts in minimizing potential security risks by proposing a huge range of mutual authentication protocols[2], privacy protection schemes[3] and lightweight cryptographic algorithms[4] for this promising technology, in order to avoid unauthorized access to personal RFID tags, user's tracking and profiling.

As presented later in this paper, the secure integration of RFID technology into the PN paradigm as a context-aware technology which complements BSNs provides notable benefits to the knowledge and potential services of the PN. Security of RFID as an independent technology is reaching an adequate maturity level thanks to research advances in recent years; however, its integration into the PN model, interaction with other network resources, remote users and service providers requires a specific security analysis and a secure PN architecture prepared to support these heterogeneous pervasive technologies. Although an increasing amount of research is focusing on the personal network paradigms with the proposal of some network architectures[5–7], and the benefits of the integration of wireless sensor networks and RFID technology have already driven the proposal of several architectures for the collaboration of these technologies in different scenarios[8–10], to the best of our knowledge, no architecture has introduced the secure integration of RFID and wireless sensor networks technologies in personal networks. This paper exposes the benefits of the collaboration of RFID and sensor technologies in PN networks, analyzes how this integration could be achieved and defines a secure PN architecture which provides the foundations in order to securely register and maintain the personal tags as members of the PN, authenticate and authorize PN nodes and remote devices in their requests to access these context-aware technologies, provide a secure tunnel to

communicate with this non IP-enabled entities and enforce the fulfilment of security and privacy policies in these communications.

The paper is organized as follows. Section 2 reviews the advantages and limitations of the integration of RFID and BSNs in personal networks. Section 3 presents our concept of the personal network, types of nodes and alternatives in the integration of RFID and sensors. Section 4 introduces the modules of our secure PN architecture proposal. Section 5 analyzes the secure management of PN nodes and communication with context-aware technologies in the architecture. Finally, section 6 concludes the paper.

2 Convenience of the Integration of RFID and PNs

Even if BSNs provide context awareness to the PN gathering information on the physiological parameters of the owner, his activities and environment, the snapshot of the surrounding reality is far from complete and the knowledge handled by the information system to monitorize and support the user is open to further contributions. RFID technology greatly complements BSNs in order to provide a more comprehensive vision of the user's current state and context. In particular, RFID enhances the features of the network in the following aspects:

- *Reach further*: thanks to the extreme miniaturization of RFID tags, ability to harvest the energy required for operation during the reading process and low cost, RFID allows spreading computation and communication capabilities to a much wider range of consumer products, furniture, building components and personal belongings than wireless sensor nodes, substantially enhancing the number of nodes, quality and quantity of data handled by the personal network. However, at the same time, these novel RFID-enabled personal items only feature highly resource-constrained capabilities and lightweight cryptography rising potential security and privacy risks into the PN.
- *Detect presence*: RFID technology allows the network to recognize the presence and absence of individual objects which are carried by the user or in his context in a specific period of time. The fact that a particular item is present denotes information about the tools the user has available and range of potential actions, in order to support and help the user, enable services of the network triggered by the current activity or achieve special privileges in the surrounding environment thanks to the possession of distinguished items. Therefore, such presence information should be accessible to authorized local or remote entities in the provision of their services, but blocked from potential attackers and rogue users.
- *Characteristics of personal items*: tags can provide further information on the characteristics of each objects. The description and metadata about the items must be provided in a standardized format in such a way that the personal network can seamlessly obtain this information, increase its knowledge on the situation where the user is immerse and features of available items, and use it to improve its services.

- *On-item history log*: tags can maintain a log about previous interactions of the personal item, places, ownerships or relevant facts. This type of historical item data defined for each type of personal object would further enhance the quality of the information handled by the PN, as well as the forensic data gathered to detect rogue actors, intrusions and attacks.
- *Secure and transparent management of personal data*: a significant portion of personal data (including certificate of personal life events, academic qualifications, medical and monetary documents, personal writings and reports) are currently handled in paper-based documentation. The integration of RFID technology into personal documentation will provide a seamless link with the digital world for agile and automated processing of its contents, as well as enable the use of advanced security mechanisms extensively addressed in electronic documents and piooner hybrid personal documents (e.g. the comprehensive ePassport security mechanisms) without sacrificing the reliability and convenience provided by the physical support.
- *User authentication*: the integration of this technology in identification cards and documentation enables the secure identification and authentication of the user in his PN, surrounding context or even access remote networks and services with minimal user interaction, but advanced security properties.

Therefore, a secure integration of RFID technology into the PN can greatly enhance the context aware services of the network. In fact, RFID technology can be considered as an additional sensing source, where, instead of sensing parameters such as temperature or humidity, the network senses which items are present and relevant metadata. From this perspective, the RFID reader acts as an additional sensor node, which senses this particular type of data about the context based on the support of passive nodes (i.e. the RFID tags). Although the integration of RFID and sensor technologies brings multiple benefits to the personal network, most RFID tags only implement lightweight cryptography and feature highly constrained memory and computation capabilities rising potential security risks in the PN. Moreover, the heterogeneous resources between RFID, sensors and other personal devices highlight the need of an adequate secure communication model with personal tags in the PN architecture.

3 Network Architecture of the PN

Our vision of the personal network paradigm focuses on the definition of a secure network architecture for the integration of RFID technology in the core PAN, the immediate sphere of nodes surrounding the user, and the communication of this enhanced core network with remote nodes (e.g. clusters of personal devices at remote locations, other personal networks or central monitoring servers). As related literature [6, 7], we consider a centralized network architecture where the master device supports PN communications and network management, while special emphasis is focused on the integration of the two foundation technologies for context awareness: wireless sensor networks and RFID technology. In particular, we assume the following types of nodes (see Figure 1):

- *Master device*: a device with no serious computational and memory constraints. This node incorporates reasonable battery life; the user interacts with it frequently and guarantees its functional state or incorporates energy harvesting features so that its continuous operation can be assumed. The node integrates communication interfaces to interact with external and wide area networks (e.g. 3G/UMTS, LTE or Wimax) and is usually carried by the user. Although specific devices could emerge in the upcoming future to fulfil this role, the widespread smartphones already satisfy this profile.
- *Wireless sensor nodes*: provide a significant amount of information about physiological parameters of the user and his activity. A wide range of sensor features, sensing variables and locations on the user are possible, and they should be adapted to the purpose and potential applications of the personal network. The PN could include a base station which manages the sensor nodes and aggregates their data or this function could be integrated in other nodes such as the master device.
- *RFID tags*: identify and keep data related to the personal tagged items. Different types of RFID technology would coexist for different purposes. For example, passive UHF tags such as EPC Gen2 tags are more adequate for personal objects (e.g. clothes, glasses or professional tools) as they fulfil the identification and reduced data management requirements of these items while featuring low cost per tag and long reading distance, however they present more constrained resources. On the other side, personal documentation would benefit from advanced cryptographic security mechanisms such as the ones available in passive HF RFID tags based on ISO/IEC 14443. Along the same lines as wireless sensor nodes, active RFID technology provide sensing and less constrained computational capabilities in case a more advance item monitorization is necessary.
- *RFID reader(s)*: in charge of identifying and recovering the data stored in the personal tagged items. Multi-standard or more than one reader is required to communicate with the different types of RFID technology. Portable and handheld UHF passive readers are able to seamlessly access tagged personal items in the sphere surrounding the user while HF passive readers (such as those integrated in some smartphone models[12]) do require close proximity to hybrid personal documentation during the communication process. In case the personal tag requires a short reading distance, notification (through input/output devices) and explicit user interaction could be required to complete de communication.
- *Input/output devices*: in addition to all-in-one smartphones, additional technologies are expected to emerge in order to provide convenient and unobtrusive methods for explicit interaction of the user including data input (e.g. tactile panels in clothes, sensor equipped bracelets) and output (e.g. head-mounted displays, augmented reality glasses).
- *Advanced gadgets*: appliances and devices owned by the user and useful for particular jobs (e.g. GPS device, music players, digital cameras and gaming devices). These devices participate in a non-continuous basis in the network enabling additional features and services, and present less resource

constrained characteristics than the core context-aware technologies of the PN (i.e. sensor and RFID nodes).

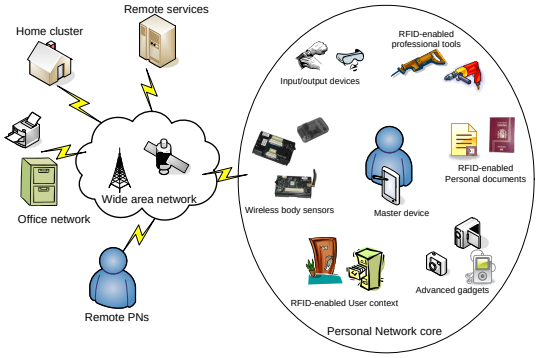

Fig. 1. Outline of communications in the personal network

4 Software Components in the PN Architecture

Our proposal is not the first contribution of a software architecture for personal networks. Existing literature[5–7] has already worked in this arena providing a general architecture for this novel network paradigm which already addresses a wide spectrum of network management issues for generic personal devices. While these previous works provide a good foundation for the development of PNs, a generic approach do not take into account how to achieve the secure integration of RFID technology in the PN.

Remote entities which require communicating with the tags are not able to address them directly (e.g. RFID tags do not have their own IP address and remote entities should not burden with their current location inside the PN or RFID readers in range). Furthermore, due to the potential leakage of personal data and potential threats to owner's privacy, user's privacy policies should be enforced in any communication with personal items. Due to this, the PN should manage the secure addressing and access to personal tags, ensuring the fulfilment of security requirements in these communications.

In the realization of our vision, the PN should provide support to the secure collaboration of the heterogeneous nodes which coexist in the network, as well as their interaction with external entities. To achieve this purpose, personal devices need to be recognized as members of the PN, providing secure mechanisms to initialize new nodes or transfer ownership from other parties. The members of the PN and authorized external entities require maintaining updated keys and credentials in the network, as well as being able to establish secure communications with other network nodes (including nodes based on incompatible network

technologies). During the communications, entities must be authenticated and the fulfilment of security and privacy policies must be enforced. In order to meet these requirements, we propose a PN architecture based on the following modules and behaviour (see Figure 2):

- *PN Members Database*: in charge of maintaining a database of the nodes that are recognized as nodes of the personal network. The database should maintain metadata related to each unique node during their membership in the network such as addressing data (e.g. IP, MAC, PN address), cryptographic materials (e.g. digital certificates, keys), roles, reputation levels and privileges in the network.
- *Member Discovery and Maintenance Module*: PN is a dynamic network paradigm where new personal devices are required to be incorporated on-demand, while previous PN members can change ownership, be compromised or disposed. This module handles the secure lifecycle of the devices associated with the PN, whether with a permanent or temporal relationship, including secure device incorporation to PN (i.e. imprinting process, key and cryptographic material exchange), refresh of shared keys and cryptographic resources during devices lifetime, as well as node disassociation protocols.
- *Naming Resolution and Communication Management*: receives requests from PN members or remote devices which are willing to communicate with a PN network node identified by a recognizable naming convention. The module handle the request by checking the applicant node and its privileges in the network (supported by the Authentication and Authorization module), and later forwarding the connection to the appropriate network module (i.e. PN Routing or Secure Context Management).
- *Authentication and Authorization Module*: in order to (re-)connect to the PN and establish queries or secure connection to PN devices, both PN members and remote nodes require to authenticate in the personal network. This module handles the secure process and, based on the node privileges, provides authorization to the node for further interactions with the PN members during its communication.
- *PN Routing*: determines the most adequate route to interconnect the applicant (local or remote) node with the requested PN network entity. The route takes into account the mobility of PN nodes in the network, as well as the heterogeneity in communication technologies and computational capabilities in order to locate the current position of the final node and include the required gateway nodes in the path.
- *Secure tunnel Manager*: secure communications are required between PN members and to/from remote devices and servers. However, due to the limited communication capabilities and strongly resource-constrained characteristics presented by some personal devices, secure connections cannot be directly established between any pair of devices. This submodule is in charge of enabling the secure communication between end-to-end nodes, including the use of intermediate proxy and gateway nodes in the PN which may act as a bridge between different networking technologies, adapting the security

mechanisms used at each hop-to-hop connection in order to maximize the security level according to the capabilities of each pair of nodes.
- *Privacy policies and profile DB*: manages the information regarding the user profile and personal information, as well as the privacy policies which define how its personal information, as well as the data stored or generated by the PN should be managed. The process to define the most adequate privacy policies could be based on different alternatives and it is open to innovative proposals. In a basic approach, the user could initially select between a range of predefined privacy levels associate to a set of privacy policies which can be later updated and fine-tuned based on the user input during the PN lifetime.
- *Secure Context Management*: in charge of managing the information generated by context-aware technologies (i.e. RFID and sensor networks). This data must be properly processed according to the security and privacy restrictions desired by the user. Based on this input, context-aware data is properly filtered, anonymized and aggregated depending on the requesting entity and related privileges.

In our centralized PN model, the master device has a distinguished position featuring a global vision of the underlying network of personal devices, providing external interfaces to wide area networks and expected continuous presence in the network. As a result, the complete PN architecture could be deployed in the master device which would be in charge of all the management and communication functions in the network. However, part of the modules of the architecture and related functions could also be outsourced to other PN devices with adequate computation and communication capabilities, as well as reliable power supply and availability in the network. For example, a wireless base station could be in charge of the Secure Context Management module or an advanced gadget could store the PN Members Database or Privacy Policies and User Profile repository. This distributed network architecture may be statically defined, although novel proposals could provide secure mechanisms for dynamic delegation of PN functions in the network.

5 Secure Management of RFID Nodes and Sensors in the Architecture

The integration of RFID technology in the personal network requires specific considerations on the functions carried out by the modules of the architecture. Following, we will discuss how this integration can be achieved, and the aspects to be required in the architecture. In particular we will analyze the discovery and management of personal tagged objects, the secure communication with context-aware technologies and the enforcement of security and privacy policies.

5.1 Discovery and Management of RFID-Enabled Items in the Architecture

As members of the PN, the personal RFID tags should also be included in the PN Members Database in order to know which tags from the user context do

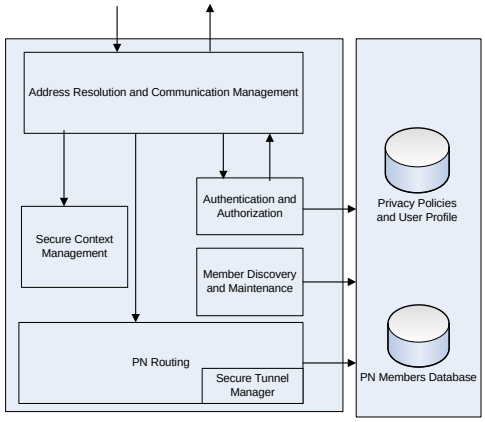

Fig. 2. Software components of the PN architecture

belong to the network and how to authenticate and access the tag. In order to properly manage the tags, the database should store adequate identification data, such as the unique identification code (UID) of each tag, along with other naming conventions which could be used in the PN to provide uniform and more convenient naming of PN nodes (e.g. using a prefix to recognize the PN, a type-of-node code and a sufix unique code in the category), a mobile IPv6 address as proposed in[18] or pseudonyms for privacy protecting purposes. Moreover, the database should maintain the adequate cryptographic material and keys so that authorized remote or PN nodes can successfully accomplish mutual authentication protocols, access and update specific memory sectors or even kill the tags.

From an ideal perspective, the deployment from scratch of a PN would allow the selection of a (set of) common security mechanism(s) and authentication protocol(s) to be used by all the RFID tags embedded in personal items. As characteristics of RFID tags differ widely from basic tags which behave as state machines with extremely limited memory to advanced tags capable of performing high level cryptographic operations (including public key cryptography), the PN network should adopt not only one, but a range of authentication and privacy protection mechanisms, in order to maximize the security level achieved with the resources available for each type of personal tag. This ideal solution would allow standardizing the secure communication protocols and unifying the management of the cryptographic materials involved in the secure storage and key refreshment processes. However, in real-world conditions, the tags adopted in the PN will be embedded in the personal items by different sources, so that a wide range of heterogeneous tags, based on different RFID technology branches and/or different authentication protocols, will coexist in the PN. Therefore, a common set of authentication protocols (depending on the type of tag, purpose and computational resources) could be defined for the RFID tags directly deployed for the applications of the PN, while the PN architecture (including the PN Members Database, Secure tunnel manager or Authentication and Autho-

rization modules) should be prepared to manage the cryptographic data and authentication protocols required by adopted RFID tags in the PN.

As new RFID-enabled objects are owned by the user or tags are explicitly embedded in personal belongings, these tags should be securely recognized and included into the personal sphere. The process of incorporating an RFID tag into the PN is managed by the Member Discovery and Maintenance Module. In the case of virgin RFID tags, deployed specifically for PN applications, an imprinting protocol should be used to initialize the tag, exchange the appropriate cryptographic materials (e.g. keys, pseudonyms and/or certificates) and register the tag in the PN Members Database. The specific mechanism to securely identify the tag and imprint the adequate cryptographic materials to prepare the tag is out of the scope of this paper and will depend on the RFID authentication protocol(s) selected for later accesses from the wide range available in the literature. The incorporation process could require some explicit interaction of the PN owner with the master device (or some other PN device with input/output capabilities) in order to confirm which tagged objects should be accepted as members of the network (e.g. by selection in a display or physically bringing the reader in close proximity of a tag) and participate in the generation or establishment of keys with a high level of entropy (e.g. by shaking a device enabled with an accelerometer or providing input through a keypad).

If the tag has not been initially deployed in this network, a tag ownership transfer protocol is required to obtain the rights to securely access the tag, dissociate it from the previous owner and refresh its cryptographic materials. Several RFID ownership transfer schemes are available in the literature[14, 15] and could be adopted (and adapted) in the PN context. However, novel protocol proposals could take into account the services and resources available in the personal network and the integration of the PN into wide area networks, as well as potential explicit user interaction in order to achieve secure remote tag ownership transfer between distant parties. In scenarios where the tag is still required in the original application where it was deployed (e.g. products under warranty which take advantage of RFID, or private/public identification documents), the goal of the incorporation process could change to securely share tag ownership[16] between the PN and a external entity or the original owner could maintain its role but enable the PN to securely access the tag by the execution of a key management protocol or granting the required privileges to query a key management server.

5.2 Secure Access and Communication with RFID Nodes and Sensors

In order to gather information from the pervasive computing technologies present in the PN, obtain awareness about the user context, sense the physical parameters and conditions or recognize and authenticate the personal items in close proximity, the PN nodes, as well as remote parties from wide area networks, require an appropriate scheme to reach and communicate with RFID nodes and sensors in the PN. The Naming and connection management module has a particular importance in accessing the RFID tags as it provides flexibility to remote

devices which may use a pseudonym scheme or PN naming scheme instead of the physical and technology specific code recognized by the tag. Moreover, the PN routing module releases the requesting node from knowing the path to the smart node or RFID reader where the tag can be found in reading range.

In our vision, a PN member or a remote device could be interested in the information provided by an RFID tag in two possible ways:

- *Direct access*: the device wants to establish a direct communication with the tag in order to identify the item, authenticate it, update its memory or retrieve specific data.
- *Aggregated knowledge*: the device requires context-awareness about the current (or past) state where the user is immersed. For its convenience, this knowledge can be better represented by the aggregated data provided by RFID-enabled personal items and sensors, rather than directly accessing each node and composing the picture on its own.

Our architecture handles both kind of interaction requirements. In case of direct access request, the applicant first requires to authenticate itself in the PN. Once it has been authenticated and authorized, the naming and routing modules are responsible to resolve the identity of the requested tag as well as its current location in the PN and provide an adequate path to reach it. In case secure communication is required, the Secure tunnel Manager submodule supports the establishment of a tunnel from the point-of-access of the PN to the smart node or RFID reader close to the requested tag, or if the intermediate nodes do not allow such a tunnel, hop-by-hop secure links inside the PN in order to maximize the security of the end-to-end channel according to the communication and computational resources of each node in the path.

On the other side, if aggregated knowledge is required, the Secure Context Management module is used after the initial authentication to provide the required context data on sensing parameters and personal items nearby. The context aware data is gathered and processed by the module as background procedures which make use of the secure naming and routing services provided by the PN to access the RFID tags and sensor nodes in the network. These behind-the-scenes communications between Secure Context Management and the pervasive computing resources available in the PN could be triggered directly by a request to the module or take place periodically to update context awareness, decoupling the remote or internal network queries from the actual secure communications with the RFID or sensor nodes.

The direct access mechanism allows the applicant to control the communication with the final tag at low level, in order to read or update specific information in the tag. This approach is very convenient for example in the remote interaction with personal documentation, as the secure communication with the advanced RFID-enabled documents may be used to authenticate the owner of the PN and even obtain non-repudiable proofs of interaction with the PN.

However, due to the low level communication with the final tag, controlling the fulfilment of security requirements and privacy policies becomes a binay decision with low granularity control. That is, queries and commands to the

tag could be blocked or forwarded, but, without filtering and processing the raw data, granularity of disclosed personal information can not be properly adjusted. Therefore, authorization mechanisms could be reinforced increasing the requirements to grant direct access privileges to remote devices as once the direct access is performed the low level data transferred could potentially contain sensitive private data. Section 5.3 provides further discussion of direct access alternatives.

On the other side, the aggregated knowledge approach allows the network to further protect the security requirements and user privacy by filtering the data obtained by the context-aware technologies, anonymize the specific nodes where the data was generated and enforce the privacy policies established by the user before the data is presented to the applicant. Therefore, this mechanism to access personal data would allow to reduce the requirements on the applicant node (e.g. trust/reputation levels or explicit privileges grant by user) in order to authorize the node to interact with the Secure Context Management module, as this module would be responsible of ensuring the privacy of the final personal data accessed, at the cost of reducing the flexibility of the applicant node in its interaction with the final tag, as well as burdening the PN with additional processing tasks. Additional discussion on the use of privacy policies in the PN architecture is provided in Section 5.4.

5.3 Alternatives in Secure Direct Access to RFID Nodes

In the direct access approach, a remote or local entity request to establish a communication with a specific node of the PN. While the routing module could provide a direct path to PN nodes which feature IP connectivity (including sensor nodes[17]), one or more proxy nodes will be required in case of devices based on incompatible communication technologies or extremely constrained cryptographic and computational resources. In particular, in the case of personal RFID tags which lack from a TCP/IP stack and feature highly constrained communication, computation and memory resources, the direct access mode (for non-local RFID readers) requires proxy nodes to establish a bridge between communication technologies and enforce the fulfilment of the security and privacy policies during the communication.

In the secure routing of direct access communications to personal RFID tags, the following alternatives could be adopted (see Figure 3):

- *Proxy node as a command forwarder*: the remote node is first required to contact an external interface of the PN (e.g. the PN master device) and authenticate itself in the network. Once the applicant has been successfully authenticated, it requests accessing a node of PN (in this study case, an RFID tag) through any addressing scheme recognized by the naming module and a secure tunnel is established from the remote node to an RFID reader or smart node in reading range of the requested RFID tag.

Once or more proxy nodes could participate in the path in order to reach the final tag, however, the secure communication links between this entities are only

used to forward the communication between both final entities. In this case, the remote node is required to understand the particular RFID technology which the tag is based on and send commands which are compatible with this final entity. The RFID reader or smart node close to the tag extract the commands received through the secure tunnel and send them to the personal tag. On reply, the response from the RFID tag is encapsulated and sent back to the remote device through the tunnel.

In this scheme, apart from being able to assert compatible RFID commands, the applicant is responsible to successfully complete the (mutual) authentication protocol against the final tag. Therefore, the applicant should know or be able to gather the necessary cryptographic materials (e.g. keys or digital certificates) required in the process. In case tag ownership is shared with an external service or the tag adopted in the PN belongs to an application external to the PN (e.g. RFID tags in private or governmental personal documentation), the applicant could obtain the cryptographic materials from third parties (e.g. a key management server[18]) before accessing the PN. Otherwise, the PN could directly provide them to the applicant once he has been authenticated in the PN. In the latter case, the PN would be responsible of refreshing the involved keys by means of the Member Discovery and Maintenance Module (e.g. once the communication has finished or in a periodic schedule) in order to prevent future unauthorized communications. As direct commands are sent to the final tag, the PN has a low control on the personal and private data recovered or modified by the applicant; however, a proxy node in the path (e.g. the master device or RFID reader) could further analyze the traffic flow and block those messages which do not fulfil the security policies, warning the applicant node.

– *Proxy node as a command gateway*: the initial authentication of the remote node in the PN and resolution of the final tag to be addressed and authorization is identical to the previous scenario. However, a gateway node in the secure route between the applicant and the tag would be required to intermediate and translate any communication between both final entities.

In this case, the applicant does not need to know the RFID standard the tag is based on, compatible commands or required cryptographic materials to complete the (mutual) authentication with the personal tag. The applicant could send his commands based on a set of normalized operations for generic RFID tags, while the gateway node would be responsible of translating the generic requests into specific commands to be executed on the RFID tag, as well as interpreting and translating the tag replies.

In this solution, the applicant only requires to maintain the adequate credentials to authenticate itself in the PN. Once authenticated and authorized, the gateway node gathers the necessary cryptographic materials through the mechanisms provided by the PN and performs the (mutual) authentication with the personal tag, therefore unburdening the applicant from the dual authentication process and the management of credentials with the individual nodes of the PN. The secure management and maintenance of personal tags also benefits from the gateway approach as the required cryptographic materials in internal secure

communications are not disclosed to external entities. Furthermore, a deeper control is reached during the 'direct' low level communication with the tag, enabling a more convenient supervision of the operations and data transferred (e.g. commands issued, memory zones accessed) in order to check sensitivity of data and applicant privileges and enforce the fulfilment of the security policies. Although the security and privacy in the PN is enhanced in this solution, this approach could not fulfil purposes where a fine control of the communication with personal tag is required by the applicant (e.g. during the authentication and validation of RFID-enabled personal documents).

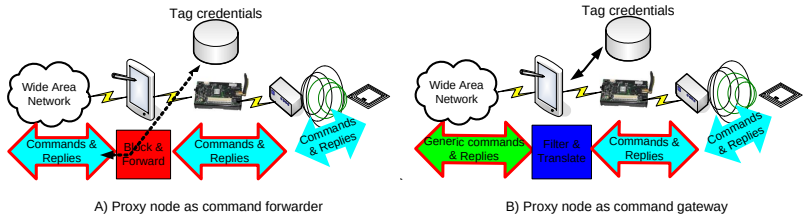

Fig. 3. Alternatives in secure direct access to RFID nodes

5.4 User Privacy in the Access to Context-Aware Technologies

The privacy policies will have an important role in the integration of RFID technology in the PN. These policies should be flexible enough to manage the ecosystem of personal RFID-enabled items, as they will belong to a wide range of categories and type of objects, as well as the potential diversity of personal and professional remote devices and service providers who may request access to the personal tags and their associated data. In this context, the privacy policies should provide a mechanism to represent which categories or individual tags maintain private data, which ones do not represent a privacy threat, when public or restricted access to selected actors can be provided, and even which personal data should be filtered and desassociated from the individual objects where it was generated before being shared with external actors.

In the case of direct access to individual tags from external actors, access control mechanisms (e.g. ACL or RBAC) can be used to define which actors are allowed to execute which commands on which tags. Additional parameters related to the context of the user (e.g. location, current activity or other PNs around) could also be used in the access policies. In the case of aggregated knowledge from multiple sensors and/or tags, the solution could also be based on these techniques, but, in this case, the targets to be accessed would be the types of knowledge that the PN is able to generate after processing and filtering the sensed data, instead of the individual sensors and RFID tags.

In the literature, a relevant solution in this direction is the RFID Guardian device which maintains a centralized security policy defining which RFID readers

are authorized to access which tags in which situations. The device achieves its purpose by eavesdropping the communication process and applying tag emulation tactics to block unauthorized readers. However, this device considers RFID as an isolated technology without taking into account data generated by other technologies to evaluate the context of the user. Moreover, it focuses on the local access to RFID tags, and does not consider the communication of personal devices with remote service providers and PNs. Our vision of RFID technology integrated in the PN takes into account both aspects and provides the appropriate architecture to securely access the context-aware technologies also from WANs, while leaving the door open to specific privacy policies for this context.

6 Conclusions

As presented, the emerging personal network paradigm could benefit from the integration of RFID-enabled personal items and BSNs, however, the special characteristics of tagged items (e.g. passiveness, non-IP enabled, constrained computation capabilities) and potential security and privacy risks require a PN architecture prepared to support these context-aware technologies.

In this paper, we have defined the foundations of an adequate secure PN architecture for this purpose. In our model, personal tags should be recognized as nodes of the PN handling related crypto materials, naming information and metadata on sensitive information to enable secure communications with other members and external entities. The deployment of RFID-tagged items from scratch would allow the selection and definition of a set of common authentication protocols to standardize personal tags management, however, the PN should support the adoption of heterogeneous tags and incorporate mechanisms for secure ownership transfer and sharing.

Authentication and authorization of entities are also controlled by the architecture before granting privileges in the network and enabling communications. In our approach, requests on resource-constrained pervasive technologies would be provided in two alternatives: direct access to final nodes and aggregated context-aware knowledge. As previously discussed, each one presents their own benefits and handicaps and should be managed independently, through secure context management and direct access schemes.

On direct access, the PN would be able to resolve and establish a secure route to reach the final node, in particular non-IP-enabled tags. As discussed, the role of proxy nodes as message forwarders or gateway nodes does also have an impact on the requirements of the applicant and enforcement of security requirements. Last, but not least, the privacy policies have a crucial role in the PN and must be able to represent which members of the PN and external parties should be able to access which context-aware nodes or types of knowledge in which situations.

Previous research in aspects such as the integration of RFID and sensor technologies, RFID security, secure tag ownership, access control schemes and RFID privacy management devices could be adopted and adapted to this purpose providing the foundations to the realization of such architecture. However, the

global vision of RFID and sensor network technologies as components of the heterogeneous and user-centric PN paradigm integrated in wide area networks leaves the door open to novel proposals specifically designed for the requirements and resources of this emerging paradigm.

References

1. International Telecommunication Union, ITU Internet Reports: The Internet of Things, November 2005.
2. Yum, D. H. et al., Distance Bounding Protocol for Mutual Authentication, IEEE Transactions on Wireless Communications, pp. 592-601, 2011
3. Alomair, B. and Poovendran, R. Privacy versus Scalability in Radio Frequency Identification Systems, Computer Communication, 2010.
4. Peris-Lopez, P. et al., Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security, 'IEEE International Conference on RFID 2010', Orlando, USA, 2010, pp. 45-52.
5. Anggraeni, P. N., Prasad, N. R. and Prasad, R. Secure personal network, Personal, Indoor and Mobile Radio Communications, IEEE 19th International Symposium on, 2008, pp. 1-5.
6. Ibrohimovna, M., et al., Secure and Dynamic Cooperation of Personal Networks in a Fednet, 6th IEEE CCNC 2009, pp. 8 -14.
7. Project IST-FP6-IP-027396, Magnet Beyond, http://magnet.aau.dk, last accessed: March 2011
8. Anggorjati, B., et al., RFID Added Value Sensing Capabilities: European Advances in Integrated RFID-WSN Middleware, IEEE SECON 2010, pp. 1-3.
9. Xiaoguang, Z. and Wei, L. The research of network architecture in warehouse management system based on RFID and WSN integration, IEEE International Conference on ICAL 2008, pp. 2556 -2560.
10. Tolentino, R. S., et al., Next Generation RFID-Based Medical Service Management System Architecture in Wireless Sensor Network, in Communication and Networking, Springer Berlin Heidelberg, 2010, pp. 147-154.
11. Memsic WSN product family, http://www.memsic.com/products/wireless-sensor-networks.html, last accessed: March 2011
12. Google Nexus S, http://www.google.es/nexus/tech-specs, accessed on: March 2011
13. Dominikus, S. and Schmidt, J.-M. Connecting Passive RFID Tags to the Internet of Things, Interconnecting Smart Objects with the Internet Workshop, Prague, 2011.
14. Yu Ng, C., et al., Practical RFID Ownership Transfer Scheme, Journal of Computer Security - Special Issue on RFID System Security, 2010.
15. Song, B. and Mitchell, C. J. Scalable RFID Security Protocols supporting Tag Ownership Transfer, Computer Communication, Elsevier, 2010.
16. Kapoor, G. et al. Single RFID Tag Ownership Transfer Protocols, IEEE Transactions on Systems, Man, and Cybernetics, 2011, pp. 1-10.
17. Mulligan, G., The 6LoWPAN architecture, 4th workshop on Embedded networked sensors, ACM, New York, NY, USA, 2007, pp. 78-82.
18. Najera, P., Moyano, F., Lopez, J., Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents, Journal of Universal Computer Science, 15, 2009,970-991.