P. Najera, R. Roman and J. Lopez, "User-centric secure integration of personal RFID tags and sensor networks", *Security and Communication Networks*, pp. 1177-1197, 2013.
http://doi.org/10.1002/sec.684
NICS Lab. Publications: https://www.nics.uma.es/publications

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2013; **6**:1177–1197
Published online 19 February 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.684

RESEARCH ARTICLE

User-centric secure integration of personal RFID tags and sensor networks

Pablo Najera[1], Rodrigo Roman[2] and Javier Lopez[1]*

[1] Computer Science Department, University of Malaga, Malaga, Spain
[2] Institute for Infocomm Research

ABSTRACT

A personal network (PN) should enable the collaboration of user's devices and services in a flexible, self-organizing, and friendly manner. For such purpose, the PN must securely accommodate heterogeneous technologies with uneven computational and communication resources. In particular, personal radio frequency identification (RFID) tags can enable seamless recognition of user's context, provide user authentication, and enable novel services enhancing the quality and quantity of data handled by the PN. However, the highly constrained features of common RFID tags and their passive role in the network highlights the need of an adequate secure communication model with personal tags, which enables their participation as a member of the PN. In this paper, we present our concept of PN, with special emphasis on the role of RFID and sensor networks, and define a secure architecture for PNs including methods for the secure access to context-aware technologies from both local PN members and the Internet of Things. The PN architecture is designed to support differentiated security mechanisms to maximize the level of security for each type of personal device. Furthermore, we analyze which security solutions available in the literature can be adapted for our architecture, as well as the challenges and security mechanisms still necessary in the secure integration of personal tags. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

personal networks; RFID security; body sensor network; secure architecture

***Correspondence**

Javier Lopez, Computer Science Department, University of Malaga, Campus de Teatinos s/n,29071, Malaga, Spain.
E-mail: jlm@lcc.uma.es

1. INTRODUCTION

As described in the pervasive computing vision, the advances in technology miniaturization, computation, and communication capabilities in resource-constrained devices, in addition to the decreasing costs, are enabling the development of a wide range of miniaturized and specialized technologies (such as multi-purpose smartphones, advanced sensor nodes, and radio frequency identification (RFID) tags) and their integration in everyday objects and user activities. As a result, the user owns and interacts with an increasing number of proprietary and accessible devices, either carried by himself, in close proximity, or even in remote personal locations (e.g., at home, car, or office). This expected path in technology evolution is leading to the development of emerging personal network (PN) paradigms that enable the coordination and cooperation of these devices.

Conceptually, a PN enables the communication of all the user's devices and services in a flexible, secure, self-organizing, and 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 in order to access centralized resources, collaborate with other PNs, and interact with smart objects regardless of their physical location.

The core of the PN is formed by the personal area network (PAN), the restricted set of devices that the user owns or has the right to access in his or her immediate context. As one of its components, a decisive technology in the realization of the PN are wireless body sensor networks (BSNs), formed by tiny wearable sensor nodes that, depending on the desire applications, consistently monitor user's physiological parameters (e.g., blood pressure, electrocardiogram, or glucose level); recognize 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 including military, elderly care, and patient monitoring applications.

Despite being commonly overlooked as a member of the emerging PNs, 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 technology. In a nutshell, RFID technology enables wireless data transmission by means of a miniaturized integrated circuit equipped with an antenna that can be attached to or embedded in the object to be controlled. When it is queried by a reader, the tag or transponder is able to uniquely identify the object, as well as provide additional data about the item (e.g., characteristics or history log), information typically updated by the reader during the lifetime of the tag. Active RFID tags even include their own battery and on-board sensors in order to provide continuous monitoring and data processing capabilities. ITU describes RFID technology as one of the pivots that will enable the upcoming Internet of Things (IoT), 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. Because of this, the research community has devoted notable efforts in minimizing potential security risks by proposing a huge range of mutual authentication protocols [2,3], privacy protection schemes [4,5], and lightweight cryptographic algorithms [6,7], in order to avoid unauthorized access to personal RFID tags, user's profiling, and tracking.

As discussed in this paper, the secure integration of RFID technology into the PN 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 PN paradigms with the proposal of some network architectures [8–10] and the benefits of the integration of wireless sensor networks and RFID technology have already driven the proposal of several architectures in different scenarios [11–13], to the best of our knowledge, no architecture had introduced the secure integration of RFID and wireless sensor networks technologies in PNs until our initial proposal [14]. This paper expands on our previous work and 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 that 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 fulfillment of security and privacy policies in these communications. Moreover, the role of current communication technologies and first standardization initiatives for PNs in relation to our proposal, as well as the integration of related security solutions in our architecture, are discussed.

The paper is organized as follows. Section 2 presents related works in the area. Section 3 reviews the advantages and limitations of the integration of RFID and BSNs in PNs. Section 4 presents our concept of the PN, types of nodes and alternatives in the integration of RFID and sensors. Section 5 introduces the modules of our secure PN architecture proposal. Section 6 analyzes the secure management and communication with context-aware technologies in the architecture. Section 7 analyzes the role of PN standards and communication standards in our architecture, as well as several security solutions which could be incorporated. Finally, Section 8 concludes the paper.

2. RELATED WORKS

Extensive research has been conducted on the concept and range of issues in PNs including self-organization, addressing, context discovery, or resource awareness. Already in 2001, EURESCOM realized the benefits that a network of personal devices could enable and explored what they called personal nets, a generic concept for providing a user-centric solution to the integration of all communication and information services. The goal was to evaluate if they were technically feasible and commercially achievable in the future. Their results showed what future users could require from a personalized place in a ubiquitous communication and computing environment and suggested further steps in the topic. Between 2002 and 2005, the personal distributed environment (PDE) initiative worked on the perspective of a user interacting with multiple local and remote devices accessed through multiple networks. In this context, they aimed at the inter-working of wireless and broadcast technologies, the service quality, and the accountability of services and user-friendly access. Their solution was based on a central PDE server, which enabled the discovery of services and devices, although assumed that subnetworks would have their own networking and security solutions, lacking a seamless handover in their mobility between subnetworks, as well as burdening the user with the management (e.g., configuration possibilities, user interfaces, and technologies).

In the same years, the Power Aware Communications for Wireless Optimized Personal Area Network Information Society Technologies (IST) project aimed at developing a toolbox for PANs consisting of physical and medium access control (MAC) layers, and consider this network paradigm as a part of the 4G picture. The project also specified security mechanisms for each of the different devices that can

participate in a PAN, providing low-level protocols and encryption algorithms for low-data-rate devices, which included sensor nodes, but no solutions were provided for RFID technology. The Wireless World Research Forum WWRF Book of Visions, in 2006, also devised future communication models on the basis of a "MultiSphere model," which ranged from the first sphere embracing wearable and handheld devices to their fifth sphere, the CyberWorld. They provided their vision although did not provide insights on security and privacy issues.

Among the main contributors to the research and development of the required underlying mechanisms to the realization of PNs are the FP EU6 MAGNET (2004–2005) and its sequel MAGNET Beyond (2006–2008), which have addressed several issues in the area including cluster formation, secure tunneling, service discovery, or federations of PNs. These projects have also addressed security challenges related to this network paradigm; in particular, they proposed security mechanisms and protocols for authentication, key exchange, and key management for generic personal devices, as well as one lightweight physical layer encryption mechanism, which could be adequate for sensor devices, although their perspective is mainly oriented to the most computational-capable entities (e.g., smartphones, laptops, digital cameras, personal video recorders, in-car entertainment devices, and navigation systems), but these mechanisms do not directly address the needs of the most resource-constrained devices in the PN (i.e., sensor and RFID technologies).

The also seminal PNP FreeBand project defined a personal network provider entity that would manage user, service, content, and network-related issues of PN, and would be provided by a commercial party or an expert user with a local server. The project has shown the value of PNs through four demonstrators in the health sector, home services, tourism, and transportation sector. However, each demonstrator is based on a different architecture defined ad hoc for the final living-lab experiment lacking a robust unified architecture for PNs. Personal devices in each PN demonstrator range from the cell phones and PDAs for multimedia streaming and push-to-talk used in "Medicam," to a wider heterogeneity in "Always at home," which includes RFID technology, although their integration is based on a naive solution oriented only to recognize the presence of the user. The issues and challenges in the area realized through the work in these demonstrators have motivated the proposal of the development of standards for PNs.

In the last advances in the area, Ecma International [15] has defined in a technical report an overview of the requirements and standardization needs of PNs. The requirements presented are based on the results of the EU FP6-IST Magnet and Magnet Beyond projects, as well as Freeband PNP. Their perspective takes into account the necessity for a PN with the capacity to communicate with multiple users, offer, and use external services, in line with our current proposal. Ecma defines requirements in several areas including connectivity and mobility support, network formation, and routing. They also name the existence of security, privacy and firewalling requirements, but the TR do not provide any depth in the area.

The knowledge acquired in the Dutch Freeband project is also the base for an initial standardization proposal in the Open Mobile Alliance (OMA). OMA considers a service-oriented vision of PNs that sets the limits on the functionalities that could be finally standardized. While OMA takes into account service discovery and content management, other aspects such as device discovery, imprinting, or intra-PN routing, discussed in this paper, are out of the scope of OMA. Because of their high-level service-oriented approach, the singularities of sensors or RFID technologies are not discussed.

On the other hand, the RFID technology has already proven its benefits (e.g., increase efficiency, productivity, or safety) in sectors such as the supply chain, public transport, healthcare environments, or e-passports. This fact-checked base added to the expected widespread in all kinds of objects in the upcoming IoT has motivated a notable amount of research efforts on this technology and, in particular, related to RFID security. However, until now, the general approach in research on security has focused on the proposal of lightweight protocols, schemes or even cryptanalysis and attacks on RFID as an isolated technology, without a holistic approach taking into consideration the type of networks where tags and readers can participate and the capabilities of surrounding devices and requirements of related applications.

We have revised the database on RFID security research maintained at RFID Security and Privacy Lounge [16], an almost comprehensive collection that includes over 600 publications since 2002. We have categorized the 227 articles, contributions in proceedings, book chapters, and PhD theses published since the beginning of 2010 until February 2012. Figure 1 shows the results of such analysis. The study denotes the fact that most of the security research on RFID focuses on the challenges of the technology separately, where a reduced group of topics concentrates most of the research in the area, while there is yet a scarce set of works that analyzes novel challenges because of their integration in other network paradigms and the coexistence and interaction of these heterogeneous technologies.

The main focus in RFID security is dedicated to the proposal of novel (mutual) authentication protocols between RFID readers/backend servers and RFID tags, although a fraction of the proposals include a wider vision introducing multi-domain systems, trusted computing technologies or OpenID solutions. The second major area of research is related to the cryptanalysis of the body of proposals and the definition of attacks on RFID systems, including commercial solutions such as keyless cars or near field communication (NFC) mobile phones. The intersection of the two major topics, cryptanalysis and attacks on (mutual) authentication protocols, forms a relevant area of research *per se*. The combinations of these three topics represent almost half of the current research on RFID security. An additional aspect that gathers a notable proportion of the work is the definition and

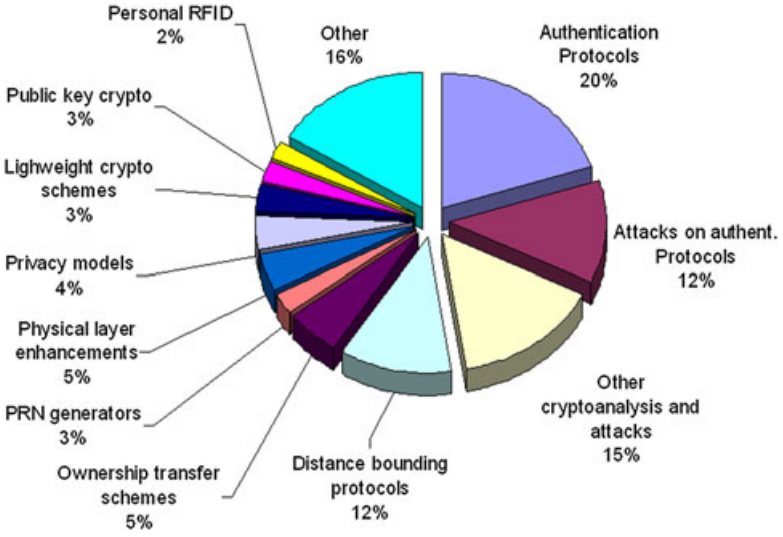

Figure 1. Focus of research in radio frequency identification (RFID) security.

analysis of distance-bounding protocols. Apart from them, significant topics in RFID security research are the design of ownership transfer schemes, physical layer enhancements (mainly, physically unclonable functions), formal privacy models, lightweight cryptographic functions, public key cryptography, or pseudorandom number generators, whereas the remaining part of analyzed works addresses a wide range of topics on their own such as RFID-based electronic voting, tag cooperation, or secret sharing.

As deduced from the analysis, these results provide a wide range of solutions to enhance the security level in RFID communications although leave their integration in other network paradigms barely explored. However, some recent works have already pioneered the security implications of personal RFID tags, such as adequate security mechanisms in e-Passports and other personal documents [17], as well as noting the distinguishing feature of the involvement of a human user in personal tags to provide solutions for reader revocation in systems based on public key infrastructures. However, this concept of "personal tag" has not been yet integrated in the PN paradigm. Selected works have also addressed another aspect of this integration, the participation of RFID tags as members of the IoT, taking into account their security [18], and their accessibility envisioned as IPv6 Nodes [19]. Moreover, research on RFID security as an isolated technology can be incorporated in real networks and scenarios, such as PNs, where solutions on (mutual) authentication protocols or ownership transfer schemes, among others, are necessary and should be adopted as exposed later in Section 7.

3. INTEGRATION OF RFID AND BSN IN THE PN

Even if BSNs provide context awareness to the PN by enabling a seamless connection to the current state of the physical reality, providing information on the physiological parameters of the owner and his or her activities and environment, the snapshot of the surrounding reality achieved by BSNs is far from complete, and the knowledge handled by the information system to monitor and support the user is open to further contributions. The resource-constrained RFID technology can act as a double-edge sword. The technology features relevant characteristics to complement BSNs in order to provide a more comprehensive vision of the user's current state and context to the PN, while requiring a well-designed integration to prevent potential security and privacy threats. In particular, RFID could enhance the features of the network in the following aspects:

- *Reach further*: Because the significant size and cost of wireless sensor nodes, as well as their limited battery lifetime and consequent maintenance requirements, the range of objects where this technology can be embedded is limited. RFID allows spreading computation and communication capabilities to a much wider range of items (e.g., consumer products, furniture, building components and personal belongings) thanks to the extreme miniaturization of RFID tags, its ability to harvest the energy required for operation during the reading process, and low cost. These characteristics substantially increase the number of nodes, quality, and quantity of data that can be handled by the PN. However, part of these novel RFID-enabled personal items will embed low-cost tags that feature highly resource-constrained capabilities. These tags implement lightweight cryptography and rise potential security and privacy risks into the PN.
- *Detect presence*: As an intrinsic characteristic of RFID, the technology allows the network to recognize the presence or absence of individual objects, which are carried by the user or in his or her context in a

specific period. The fact that a particular item is present can denote information about the tools the user has available, his or her current activity, and range of potential actions. With this data, the PN may provide specific information to support and help the user, enable services of the network triggered by the current personal or professional activity, or achieve special privileges in the surrounding environment thanks to the possession of keys, professional equipment, ID cards, or other distinguished items. Such presence information should be accessible to the PN and authorized local or remote entities in the provision of their services but must be blocked from potential attackers and rogue users.

- *Characteristics of personal items*: RFID tags do not only allow to recognize the presence of specific personal belongings in the context of the user but can also provide further information on the characteristics of each one of these objects. The description and metadata about the items must be provided in a standardized format in such a way that the PN can seamlessly obtain this information, increase its knowledge on the situation where the user is immerse and features of accessible items, and use it to improve its services.
- *On-item history log*: The on-tag memory can be exploited to maintain a log of previous interactions of the personal item. Advanced tags with programmable behavior (e.g., NXP SmartMX family) can be proactive in the generation of such log, but the policy to update the memory should reside on the reader side in the case of basic tags based on state machines. Such log could maintain previous interactions of the personal item with other objects and PNs, places where the object has been, previous ownerships, or relevant facts related to the tagged item. The specific historical data maintained in each tag should be defined and adapted for the specific characteristics and purposes of each type of personal object. Such data 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 is currently handled in paper-based documentation (e.g., certificate of personal life events, academic qualifications, medical and monetary documents, personal writings, and reports). Although the traditional paper-based format is not likely to disappear in the near future as it is easy to use and deeply adopted in daily life, its physical handling turns the processing of documents into a slow and error prone task. Moreover, traditional documents are prone to cloning, alteration, and counterfeiting attacks. The integration of RFID technology into personal documentation enables 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 pioneer hybrid personal documents (e.g., the comprehensive ePassport security mechanisms), without sacrificing the reliability and convenience provided by the physical support [17].
- *User authentication*: as an additional benefit of the integration of RFID technology in personal documents, the integration of this technology in identification cards and documents enables the secure identification and authentication of the user (e.g., in his or her PN, surrounding context, or even to access remote networks and services) with minimal user interaction. The use of advanced tags with appropriate security properties can allow smoothing over the handicaps for a more convenient immersion of the user in the pervasive computing context without giving up his or her privacy.

Therefore, a secure integration of RFID technology into the PN could greatly enhance the context-aware services of the network. In fact, RFID technology can be interpreted 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 (e.g., their characteristics and history). 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). While the RFID reader typically integrates enough hardware resources to implement advanced security schemes for their communication with the network (in this case, the PN), passive tags typically implement only limited computational capabilities to support data processing and security functions.

Active RFID technology could also be evaluated in order to provide autonomous monitoring of personal items. These types of tags can also offer traditional sensing information, although active tags also share part of the limitations of common sensor nodes (e.g., size, battery lifetime, and cost) and do not provide collaboration between multiple active tags. Whether RFID technology represents a better alternative in order to provide a seamless link to the information system for personal items depends on the information required from the smart item. Passive RFID technology is likely the best option to turn the personal object into part of the network when the requirements are limited to recognizing the presence of the object and recovering static data about the item and its history, generated during the discrete events of interaction with specific readers. However, if higher processing capabilities are required and the object should be able to generate data autonomously, either at specific events or at a constant monitoring rate, without the support of external entities, then active RFID technology and wireless sensor networks are more adequate. If multi-hop communication and collaboration between nodes is required, then wireless sensor networks turns out as a more suitable option to RFID technology. In this case, the sensor node could be provided with unique identification codes and provide basic RFID capabilities through software implementation.

The active technology has been standardized in ISO 18000-7 and the DASH7 Alliance has been established to

support its development. Although initially designed for military applications with oversized dimensions and costs, since 2010, the Alliance have developed the OpenTag initiative, able to compile in 16 Kb, and are promoting their adoption in smart phones as the 433.92 MHz operating frequency can be implemented in the 13.56 MHz antennas already used in NFC. Because of this, active RFID technology could become an effective solution for PNs in the near future. However, the higher computational and cryptographic resources of Dash7 tags (i.e., 128-bit Advanced Encryption Standard (AES) and public key cryptography) and their active capabilities places them closer to wireless sensor nodes for the purpose of our analysis. Therefore, our current work focuses on the integration of the passive RFID technology in personal items and the PN.

Although the integration of RFID and sensor technologies brings multiple benefits to the PN, 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.

4. THE NETWORK ARCHITECTURE

Our vision of the PN 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. Moreover, we focus in the communication of this enhanced core network with remote nodes (e.g., clusters of personal devices at remote locations, other PNs, or central monitoring servers). The EU FP6-IST Magnet and Magnet Beyond [10] projects, the main projects dedicated to PNs and the basis for the Ecma standardization initiative in PNs [15], consider a centralized network architecture where the master device supports PN communications and network management. We also adopt the centralized architecture approach where we provide special emphasis 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 (Figure 2):

- *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/Universal Mobile Telecommunications System (UMTS), Long-Term Evolution (LTE), or Worldwide Interoperability for Microwave Access (Wimax)) and is usually carried by the user. Although specific devices could emerge in the upcoming future to fulfill this role, the widespread smartphones already satisfy this profile.

  The hardware features and evolving operating systems of these devices enables them to implement most security solutions from symmetric cryptography to asymmetric cryptography, the full-fledge TCP/IP stack including IPSec, virtual private network solutions, and advanced authentication protocols providing a robust gateway to wireless area networks Wide Area Network (WANs).
- *Wireless sensor nodes*: located either in the context of the user, but mostly in, on, or around the owner conforming a BSN, sensor nodes provide a significant amount of information about physiological parameters of the user and his or her 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 PN. The PN could include a base station, which manages the sensor nodes and aggregates their data, or this function could be integrated in other node of the network such as the master device.

  Sensors are usually limited in computational resources (up to 32 MHz) and memory (up to 256 KB). Cryptographic primitives (e.g., standard AES-128) can be implemented in software and even can execute asymmetric elliptic curve cryptography (ECC) in less than 2 s. Standards such as ZigBee and WirelessHARTTM use a symmetric master key for node authentication and session key agreement. More advanced mechanisms based on mathematics and statistics are under research. Recent research has provided many additional mechanisms not yet standardized such as secure clock synchronization, secure distribution of code and updates, intrusion detection systems, and anomaly detection techniques.
- *RFID tags*: identify and keep data related to the personal tagged items. Different types of RFID technology would coexist for a variety of purposes in the PN. For example, passive Ultra High Frequency (UHF) tags such as Electronic Product Code (EPC) Gen2 tags are more adequate to be embedded in personal objects (e.g., clothes, glasses, or professional tools) as they fulfill the identification and reduced data management requirements of these items while featuring low cost per tag and long reading distance; however, they present highly constrained resources. On the other side, the RFID technology embedded in personal documentation embed computational resources similar to smartcards.

  Beyond the extensive recent research in RFID security discussed previously, the standards for the heterogeneous RFID devices (e.g., ISO/IEC 11784–11785, ISO 10536–15693, ISO 18000) provide some data confidentiality and integrity through the definition of basic security mechanisms: password-based read protection, tag addressing based on random numbers, XORed masked communications, silent modes, or protection on writing commands. The ISO 1443 standard, oriented to personal documentation and electronic payment, presents a noteworthy case. The tags based on this standard provide higher cryptographic resources including

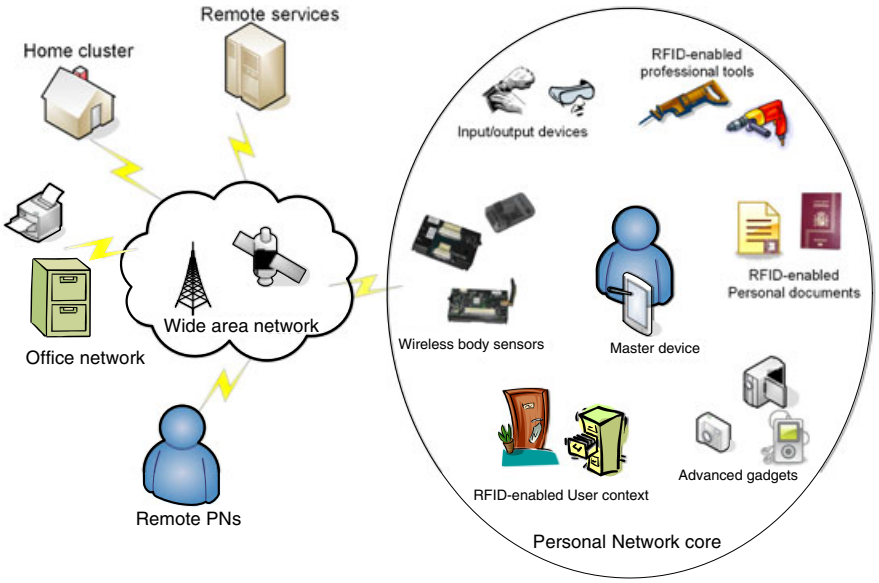

Figure 2. Outline of communications in the personal network (PN). RFID, radio frequency identification.

triple-Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Secure Hash Algorithm (SHA)-1 algorithms. The most advanced current commercial tags (e.g., Mifare SmartMX family) even integrate a co processor for public key cryptography based on RSA and ECC.

- *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 (approx. radius of 2 m) while HF passive readers (such as the ones integrated in some smartphone models [20,21]) do require close proximity to hybrid personal documentation during the communication process. In case the personal tag requires a short reading distance, the user can explicitly interact during the authentication (through input/output devices). The reader typically implements two differentiated sets of security protocols: lightweight mechanisms for secure communication with tags and higher security solutions to establish a secure channel with backend nodes (e.g., the master device).
- *Input/output devices*: in addition to all-in-one smartphones, additional technologies are expected to emerge in PNs in order to provide convenient and unobtrusive methods for explicit interaction of the user with the network including data input (e.g., tactile panels in clothes, sensor equipped bracelets) and output (e.g., head-mounted displays and augmented reality glasses).

  Several cryptographic options might be implemented in these devices depending on their hardware resources. The ISO/IEC 29192 standard provides lightweight cryptography solutions for constrained devices including stream ciphers and block ciphers. Other solutions include the recent Sony's CLEFIA block cipher, which supports 128-bit keys or stream ciphers such as Salsa10/12 and Trivium analyzed in the eSTREAM project. The SHA-3 competition will also lay the foundation for lightweight dedicated hash functions. Moreover, optimizations in operational modes can make data processing more efficient in those devices without enough resources for the conventional version of the algorithms. For example, both AES-Counter with CBC-MAC (CCM) and AES-Galois/Counter Mode (GCM) offer data integrity and confidentiality.
- *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). Depending on the resources available, security solutions can vary from the lightweight cryptography of input/output devices to full-fledge algorithms and protocols similar to the master device.

In a PN architecture that contemplates the secure integration with wide area networks (e.g., the IoT), secure access to RFID-enabled personal items may be requested from both local PN nodes and remote entities. The PN could require authenticating and accessing personal tags in order to enhance context awareness by aggregating this data with the one provided from other data sources such as the BSN, using this information to make better decisions and improve network services. However, remote users and services could also interact with the context-aware devices of the PN for medical, governmental, recreational,

or professional activities, so the network architecture should provide adequate mechanisms to enable the secure access to personal tags from remote actors.

5. SOFTWARE COMPONENTS IN THE PN ARCHITECTURE

As previously presented, RFID-enabled personal objects and documents are a key component of the PN; however, external and 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, because of 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. Because of this, the PN should manage the secure addressing and access to personal tags, ensuring the fulfillment of security requirements in these communications.

Our proposal is not the first contribution of a software architecture for PNs. Existing literature [8–10] 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, an aspect yet to be discussed in the previous literature.

In the realization of our vision, the PN should provide support to the secure collaboration of the heterogeneous nodes that coexist in the network (i.e., wireless sensor nodes, RFID readers and tags, advanced gadgets, and input/output devices), 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 fulfillment 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 behavior (Figure 3):

- *PN members database*: in charge of maintaining a database of the nodes that are recognized as nodes of the PN. The database should maintain metadata related to each unique node during their membership in the network such as addressing data (e.g., IP, MAC, and 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 be 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 that are willing to communicate with a PN network node identified by a recognizable naming convention. The module handles 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

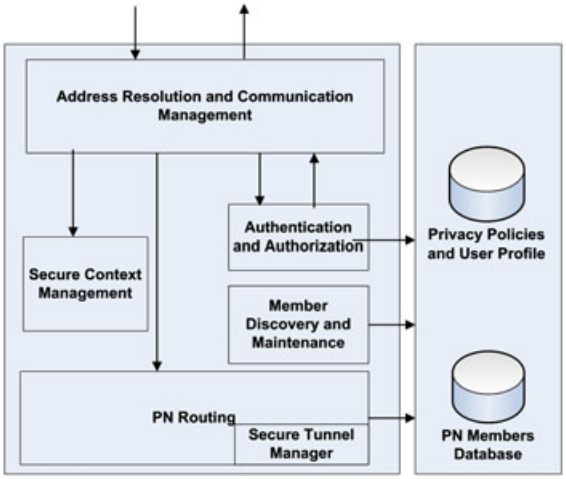

Figure 3. Software components of the personal network (PN) architecture.

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 connections to PN devices, both PN members and remote nodes are required to authenticate in the PN. This module handles the secure process and, on the basis of 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, because of 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 Database (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 predefined privacy levels associated to a set of privacy policies, which can be later updated and fine-tuned on the basis of 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. With 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. This distributed network architecture may be statically defined although novel proposals could provide secure mechanisms for dynamic delegation of PN functions in the network. Figure 4 shows a two-layer vision of the PN architecture including the network abstraction layer and the corresponding service abstraction layer. In the example, the core of the PN architecture is deployed in the master device, whereas a wireless base station is in charge of the secure context management and an advanced permanent gadget stores the PN member database, and the privacy policies and user profile repositories. An RFID reader adopts the role of RFID gateway discussed later in the paper. The figure also presents two active connections with remote entities (i.e., a request of direct access communication with a personal tag and a secure context query from an authenticated entity), as well as a snapshot of the secure communications triggered in the architecture. Further details on direct access modes and secure context management are provided in Sections 6.2 and 6.3.

6. SECURE MANAGEMENT OF RFID NODES AND SENSORS IN THE ARCHITECTURE

The integration of RFID technology in the PN requires specific considerations on the functions carried out by the modules. In the following, we will discuss how this integration can be achieved, and the functions and behavior 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.

6.1. Discovery and management of RFID-enabled items

Despite their passive nature, we propose that personal RFID tags should be included in the PN Members Database as members of the PN. This approach enables to recognize which tags from the user context belong to the network as well as handle the required credentials to authenticate and access the RFID devices. In order to properly manage the tags, new metadata must be included in the database. First, the database should store adequate identification data, such as the unique identification code of each tag. PNs could make use of novel naming conventions in order to provide uniform and more convenient naming of PN nodes (e.g., using a prefix to recognize the PN, a code to define the type of node, and a suffix unique code in the

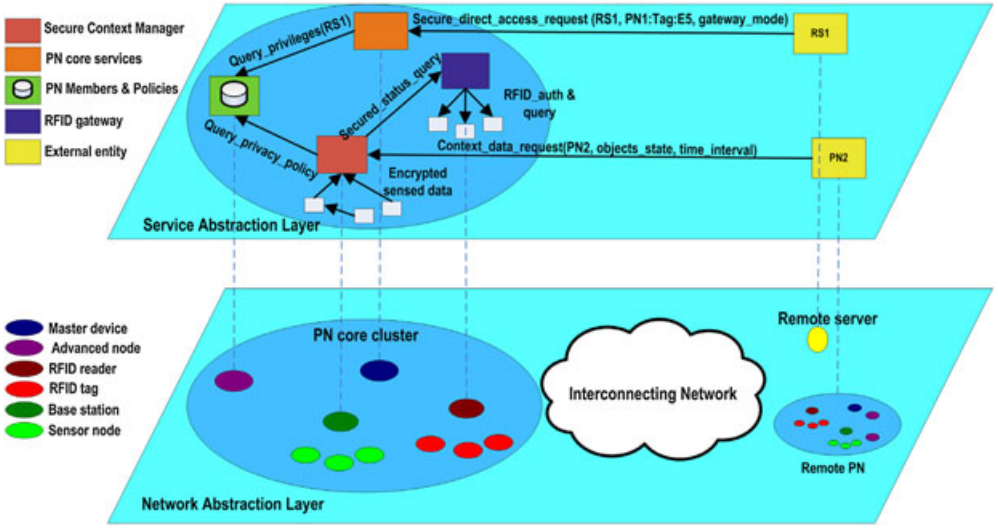

Figure 4. Two level view of the secure personal network (PN) architecture. The diagram also presents two active connections from external entities. RFID, radio frequency identification; RS, remote server.

category). Other options include providing a mobile IPv6 address to each RFID device as proposed in [22] or pseudonyms for privacy protecting purposes. The database should store the required data for the set of naming and addressing schemes accepted for personal tags. Moreover, the database should maintain the adequate cryptographic material and keys that will enable authorized remote or PN nodes to successfully accomplish mutual authentication protocols, access and update specific memory sectors, or even kill the tags.

The PN will have to deal with RFID tags attached to personal items from different sources, which generate a variety of challenges. From an ideal perspective, the user could have deployed the PN from scratch with the direct deploy of tags for personal applications. The deployment from scratch 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 that 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 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 tag. This approach would allow to unify the management of the personal tags including: secure communication protocols, cryptographic materials, or 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 Authorization modules) have to be prepared to manage the cryptographic data and authentication protocols required by adopted RFID tags in the PN. By way of illustration, Figure 5 presents an extract of the database scheme required to manage the heterogeneity of personal devices and related security protocols.

During the lifecycle of the PN, the user can own new RFID-enabled objects, either by ownership transfer of tagged items (e.g., through purchase or gifts) or explicitly embedding tags in personal belongings. All 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 (according to our previous analysis, around 32% of the literature on RFID security is dedicated to this topic). 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

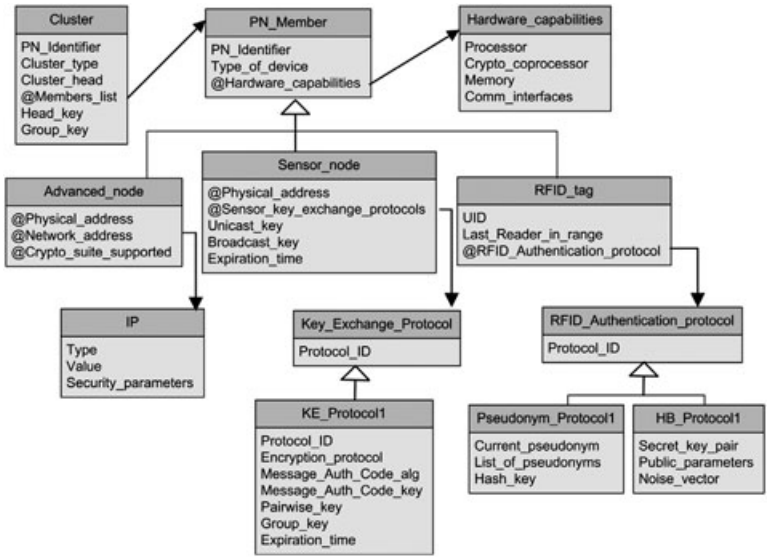

Figure 5. Extract of tables structure in personal network (PN) members database. UID, user identification; RFID, radio frequency identification; KE, Key exchange; HB, Hopper and Blum.

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 [23,24] and could be adopted (and adapted) to the PN context. However, novel protocol proposals could also consider in the ownership transfer mechanisms the distinctive aspects of PNs (e.g., services and resources available in the PN, the integration of the PN into wide area networks and the 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 changes from ownership transfer to secure tag ownership sharing [25] between the PN and an external entity. As an alternative solution, the original owner could maintain its role but enable the PN to securely access the tag. This can be achieved by the execution of a key management protocol or granting the required privileges to query a key management server.

6.2. 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.

A PN member or a remote device could be interested in the information provided by an RFID tag in two possible ways (Figure 6):

- *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 is designed to handle both kinds of interaction requirements. In case of a direct access request, the applicant is first required 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. If

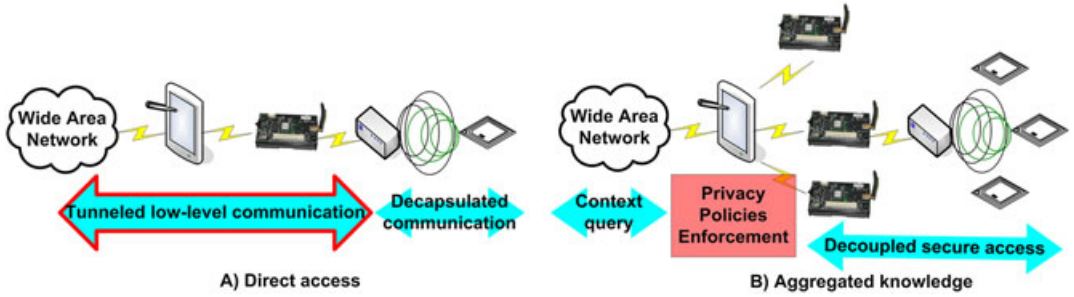

Figure 6. Secure access methods to context technologies in the personal network.

the confidentiality and integrity of data 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 closer to the requested tag. The capabilities of the intermediate nodes may not allow the creation of such tunnel. In this case, hop-by-hop secure links can be used 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. The behind-the-scenes communications between secure context management and the pervasive computing resources available in the PN can be initiated based on two options: triggered directly by a request to the module or as a period process to update context awareness. As a result, this module allows to decouple 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 to read or update specific information in the tag. This approach is very convenient in applications such as the remote interaction with personal documentation, as the secure communication with the advanced RFID-enabled documents would be used to authenticate the owner of the PN and even obtain non-repudiable proofs of interaction with the PN, which is facilitated by a direct communication with the smart document.

However, because of the low-level communication with the final tag, controlling the fulfillment of security requirements and privacy policies in the direct access mechanism becomes a binary 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, the granularity of disclosed personal information cannot be properly adjusted. Once the direct access is performed, the low-level data transferred could potentially contain sensitive private data. Because of this, the authorization mechanisms could be reinforced increasing the requirements to grant direct access privileges to remote devices. Section 6.3 provides further discussion of direct access alternatives.

On the other side, the aggregated knowledge approach allows to filter 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. With these mechanisms the network can further ensure the fulfillment of the security requirements and protect the privacy of the user. As this module would be responsible of ensuring the privacy of the final personal data accessed, the requirements that the applicant node must fulfill (e.g., trust/reputation levels or explicitly granted privileges) to access the secure context management module can be relaxed in comparison with the direct access requirements. However, the aggregated knowledge access method reduces the flexibility of the applicant node in its interaction with the final tag and burdens the PN with additional processing tasks. Additional discussion on the use of privacy policies in the PN architecture is provided in Section 6.4.

6.3. Alternatives in secure direct access to RFID nodes

In the direct access approach, a remote or local entity requests to establish a communication with a specific node of the PN (base station, sensor node, RFID node, or advanced gadget). While the routing module could provide a direct path to PN nodes, which feature IP connectivity (including sensor nodes [26]), 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 that 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 forward queries and commands from the applicant to the final tag. These gateway nodes should also have a key role in enforcing the fulfillment of the security and privacy policies during the communication with the RFID tag.

In the secure routing of direct access communications to personal RFID tags, the following alternatives could be adopted (Figure 7):

- *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 access to a node of PN (in this study case, an RFID tag) through any addressing scheme recognized by the naming module. A secure tunnel is established from the remote node to an RFID reader or smart node in reading range of the requested RFID tag.

One or more proxy nodes could participate in the path in order to reach the final tag; however, the secure communication links between these nodes 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 that the tag is based on and send commands that 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 commands against the tag, 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) before accessing the PN. Otherwise, the PN could directly provide them to the applicant once he or she 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 that do not fulfill 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 based on the applicant query is identical to the previous scenario. However, once the applicant has been authenticated and authorized to access the RFID tag, 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 require to "talk" the language of the particular tag queried. That is, the applicant does not need to know the RFID standard that the tag is based on, its memory characteristics, compatible commands, or required cryptographic materials to complete the (mutual) authentication with the personal tag. The applicant could send his or her 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, as the gateway is required to translate any communication between the final entities, a deeper control is reached during the "direct" low-level communication with the tag, enabling a more convenient supervision of

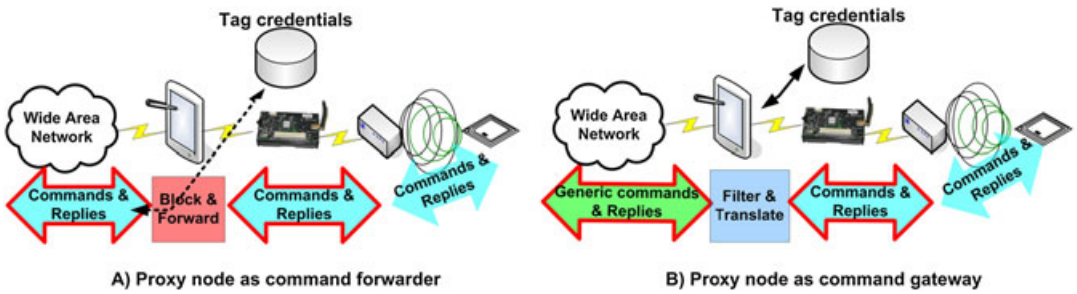

Figure 7. Alternatives in secure direct access to radio frequency identification nodes.

the operations and data transferred (e.g., commands issued and memory zones accessed) in order to check sensitivity of data and applicant privileges and enforce the fulfillment of the security policies.

Although the security and privacy in the PN is enhanced in this solution, this approach could not fulfill 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).

The role of the gateway could be assumed by either, the external interface in the PN (e.g., the master device), or by the RFID reader or smart node which issues the final commands. The former would allow analyzing and filtering inappropriate request at the entry point of the network, therefore controlling the propagation of the unwanted messages, preventing potential attacks (e.g., malformed requests) and saving network resources (e.g., battery and network bandwidth), whereas the latter would concentrate on the RFID functions (e.g., RFID commands and protocol messages) into the most related network entities.

6.4. Enforcing 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 disassociated 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., Access Control List (ACL) or Role-Based Access Control (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. Although it is a good starting point, this device is not integrated in a PN and only considers RFID as an isolated technology, without taking into account the information generated by other technologies such as sensor networks to evaluate the context of the user. Moreover, it focuses on the local access to RFID tags from readers which are physically near to the user, and do not consider the integration of the personal devices in wide area networks and their communication with remote service providers and PNs. Our more advanced vision of the RFID technology integrated in the PN do take into account both aspects and provide the appropriate architecture to securely access the context-aware technologies also from wide area networks, while leaving the door open to specific privacy policies for this context.

6.5. In-cluster and inter-cluster mobility of personal nodes

Regarding the initial association of a personal device, and subsequent events of node authentication and establishment of secure communications, the particular characteristics of our network environment must be taken into account in the definition of secure protocols for the PN architecture.

Because of the user-centric character of our network, the set of devices present in the core PN cluster (i.e., carried or in the immediate context of the user) can change as a result of a wide range of causes (e.g., items required in current user's activity, clothes worn, and user location). As a consequence, we have to assume a dynamic and mobile network where the nodes that are active in the network and the location of a particular node can vary during a given period.

Regarding *the PN core cluster*, its physical area covers approximately 2–5 m around the user location. A particular node could change its location in the PN core cluster because of passive motions of sensor nodes caused by human ambulatory and posture change directed by human extremities. However, because of the reduced size of the cluster, the movement of a node can be expected to have a reduced impact on network topology. Taking into account the particular characteristics of each type of personal device, typical advanced devices employ communication technologies (e.g., IEEE 802.11 and Bluetooth) of which coverage range exceeds the diameter of the core cluster. As a consequence, their mobility inside the core cluster does not raise additional security concerns. Wireless body sensor nodes are typically based on low-power technologies (e.g., 802.15.4/ZigBee or Bluetooth Low Energy) with a communication range that also meets the previous requirement. As a consequence, sensor nodes will not lose connectivity with their base station, and therefore, some security mechanisms (i.e., secure handover schemes, link-level authentication, and key agreement protocols for visiting nodes in foreign base stations) are not mandatory in the core PN cluster. Part of the personal RFID tags are based on proximity technologies (e.g., IEEE 15693, IEEE 14443, and ISO 18000 Part 3) where the mobility of a tag in the cluster may cause that the tag loses connectivity with the previous RFID reader or all the reader in the

network. This challenge can be mitigated by means of two mechanisms previously discussed in the paper: the management of HF tags based on explicit user interaction and the architecture capabilities to recognize the adequate RFID reader for the current personal tag location.

However, there are two different cases where the mobility of personal nodes must be addressed: (a) *micro-mobility*: the mobility of nodes within large remote clusters (e.g., the home or office cluster) and (b) *macro-mobility*: the mobility of nodes between different clusters of personal devices.

- *Inside the same cluster (micro-mobility)*: nodes move between different access points (APs) or base stations located within the same secondary personal cluster. Although the current work focuses on the secure integration of personal RFID tags and sensors in the core PAN, other external clusters (e.g., home network or office network) should provide adequate security mechanisms to manage node mobility. Large external clusters should implement handover mechanisms for wireless sensor mobility. Inside the cluster, a node can lose or weaken connectivity with its current AP or base station. Several techniques in the literature recognize node transition within the same network domain based on the evaluation of the received signal strength indicator; if the link quality decreases below a threshold, the handover mechanism is initiated. In this case, roaming between APs or base stations can be solved at the link layer.

  Mobile nodes, particularly in remote unattended clusters, could be compromised by an attacker. Overall, constrained nodes such as commodity sensors have a lack of inexpensive tamper-resistant hardware to detect such event or regain security after compromise (intrusion resilience). The solution for these mobile nodes could be based on an online trusted third party (TTP) (e.g., the master device in the PN core), which can adopt a key-insulated scheme to prevent past and future secrets to be learned by an adversary, as long as the TTP is not compromised simultaneously. A different scheme without the need of a TTP is proposed by Di Pietro, Soriente, and Tsudik [27] where the rest of the nodes in the same cluster act as a source of secure randomness for their peers and collaborate to regain control of a previously compromised sensor node. The security mechanisms designed to address node mobility should also take into account energy consumption and communication overhead aspects.
- *Inter-cluster (macro-mobility)*: nodes move between different personal clusters (e.g., between core cluster, office cluster, and car cluster). The Mobile IP protocol defined in IPv6 (MIPv6) should provide support for the mobility of personal devices; however, the most constrained devices do not offer enough resources to handle the mobility and security as defined in IPv6. Moreover, 6LoWPA does not support the mobility protocol MIPv6.

  The core PAN, where this paper is focused, has the corresponding cryptomaterials to establish a secure communication with those nodes that have been previously authenticated and imprinted. To solve the mobility of nodes, the core PAN can be established as the base network, while nodes can move into other networks (visited networks).

  The user can assist the initial device imprinting in the core PAN, while later authentication of personal devices in remote clusters can be enabled through specific mechanisms. Jara, Zamora, and Skarmeta [28] defined a mobility protocol to enable the authentication of a mobile resource-constrained node in a visited network. The protocol is based on the forwarding of challenge request and replies between agents in the home and visited networks.

  However, this mechanism requires that the visited network has continuous connectivity to the core PAN in order to authenticate and authorize the guest node in the remote personal cluster. The protocol used during the first authentication in the visited network could be extended to include key exchange that enables subsequent secure communications with the guest node without interaction with the core PAN. If the core PAN should also control the privileges granted to the nodes in the remote clusters, a Certificate Revocation List or analogous mechanism could be enabled in the core PAN to prevent revoked nodes from establishing communications in remote clusters.

Section 7.2 discusses the secure interconnection of clusters and secure inter-cluster routing needs as later extensions of the secure PN architecture.

6.6. Real expectations of lightweight cryptography in personal RFID tags

The secure authentication and encryption mechanisms adopted in personal RFID tags have to be tailored to the capabilities provided by these highly resource-constrained devices. Software implementations provide high flexibility, low cost, and short time to market to integrate suites of security algorithms in embedded devices, but their low performance and the constrained hardware capabilities of RFID tags require the adoption of hardware alternatives. As discussed by Sklavos [29], application-specific integrated circuits (ASICs) are used to implement cryptoprocessor architectures providing high performance at low power consumption, but require a large circuit to implement a set of ciphers. Each encryption algorithm covers an area of 40–60 mm^2, whereas a complete WAP cipher set integration (composed of eight algorithms) requires 400–480 mm^2, which increases significantly the cost of the chip. Field-programmable gate arrays provide a middle ground between software applications and ASICs devices as its programmable logic is more flexible than ASICs, but power consumption increases and performance decreases compared with ASICs.

As a result, the current hardware capabilities of RFID tags and state of the art in lightweight cryptography determines and limits the mechanisms and protocols that can be adopted in these personal devices and limits the possibility to

share common security protocols between heterogeneous personal devices.

The hardware requirements in passive RFID tags involve power constraints, chip area, and timing requirements. Tags must allow cryptographic operations in the whole range of normal operation (e.g., up to 7 m in UHF range), and power is reduced linearly with the operating distance for UHF tags. As a result, the power consumption of cryptographic operations should not exceed the available power budget. The threshold is defined between 20 μW [30] and 30 μW [31]. Additionally, the chip area establishes also a hardware requirement as the cost of an RFID tag linearly increases with the die size, and a cryptographic hardware module may require significant resources. Oren and Feldhofer [30], as wellas Plos *et al.* [31], estimate that nowadays, the total chip area of an RFID tag has a size of 20 000 gate equivalents (GEs) of which 7500 GEs are already consumed by the controlling unit that handles the communication protocol. The more restrictive Maimut and Ouafi [32] establishes the total tag resources to 10 000 GEs of which only 2000 GEs are available for security. Moreover, low-cost passive tags are stated to typically feature an operating frequency of 100 kHz [33] and a process tag of 0.35 μm [34]. Regarding timing requirement, the widespread EPC Class 1 GEN 2 protocol specifies a T1 timing boundary. T1 establishes the maximum delay from the interrogator transmission to tag response. In a query command, using typical parameters (i.e., DR = 8, M = 1, and, therefore, a link rate of 128 kbps), the T1 boundary becomes 78.125 μs. Some implementations use a 2-MHz chip clock rate, which leaves a maximum of 157 clocks cycles for protocol execution [35].

Taking into account these hardware restrictions, a typical low-cost passive tag is remarkably restricted to implement the same cryptographic functions used in wireless sensors or other more capable devices. However, specific solutions can be integrated in low-cost personal tags. Optimized versions of symmetric cryptography solutions approximately meet the specified requirements of passive tags. A serialized version of DES requires 2310 GEs [32] and the encryption-only architecture of AES 3100 GEs. The PRESENT block cipher has been implemented with as few as 1000 GEs [36], wheres Kitsos *et al.* have implemented many other solutions (i.e., PUFFIN, DESL, DEXL, XTEA, and HIGHT) within the 2000–4000 GEs, using 90-nm Complementary metal-oxide-semiconductor (CMOS) technology using 10–30 cycles per block and power consumption of 20–60 μW [33]. Beyond the hardware implementation of individual solutions, a cryptographic VHDL microcontroller can be implemented in 5594 GEs [31]. Such microcontroller has a power consumption of 10.3 μA at 100 kHz and 3 V, and requires 3000–5000 clock cycles for AES-128 encryption and a code size of less than 1000 bytes to implement Scalable Encryption Algorithm (SEA) and Trivium.

A reduced range of specific solutions in asymmetric cryptography can also be considered an option for low-cost passive tags. A variant of Rabin encryption scheme has been defined, which requires 4682 GEs for a complete ASIC implementation, and is enabled for 1024-bit encryption [34]. The requirements for such hardware almost meets RFID capabilities; the public key working prototype requires an additional 7.5% code size to the standard firmware in a UHF Demotag and a cipher execution time of 180 ms (325 ms for the execution of the complete protocol). Recent optimizations of public key cryptography are promising for RFID technology although are still in the borderline to fit all the requirements of common passive RFID at once. Wenger *et al.* have designed a 16-bit microcontroller in 8958 GEs, which supports ECC. The microcontroller has a power consumption of 3.2 μW at 100 kHz for a point multiplication (which meets RFID requirements) although the design uses 0.13 μm CMOS technology (instead of the 0.35 μm typically used in RFID). When the Elliptic Curve Digital Signature Algorithm is used, the specifications overpass RFID requirements: signature generation requires 15 387 GEs, 41.11 μW at 1 MHz and 378 kCycles, and signature verification requires a chip area of 16 005 GEs, 605 kCycles, and 40.76 μW at 1 MHz [37].

As a result, specifically tailored implementations of public key cryptography are becoming a reality for mainstream passive RFID technology, although the strict constraints previously described define a goal hard to achieve. Even lightweight solutions based on symmetric cryptography commonly exceed part of the requirements (i.e., chip area, power consumption, full execution time, code size, or memory required). As a consequence, specific security protocols needs to be defined for low-end personal RFID tags, although more advanced RFID tags, wireless sensors, and other personal devices may provide enough hardware capabilities to implement a more comprehensive suite of standardized security mechanisms.

Even if the PN enables the unified management of personal devices, it does not mean that heterogeneous nodes (e.g., wireless sensors and RFID tags) should implement the same lightweight cryptography, but the PN architecture through its metadata in databases and offered interfaces should accommodate the optimal mechanisms for each type of device.

7. PN STANDARDS AND INTEGRATION OF RELATED SECURITY SOLUTIONS

7.1. Wireless communication technologies and initiatives for PN standards

Regarding the position of our proposal in relation to standardized communication technologies and initiatives in the PN arena, personal RFID tags and our alternatives for secure access could make use of actual RFID solutions (e.g., ISO 15693/14443, EPC Gen2, and NFC). Because of the resource-constrained characteristics of RFID tags, the role of these leaf nodes in the architecture should be restricted to securely store their required cryptomaterials and perform the mutual authentication protocol with the requesting reader. The tag is not aware if the entity that will

finally process the (private) data is the authenticated reader; therefore, its role is limited to authenticate the reader, whereas subsequent forwarding of such data is out of its scope. As a consequence, the security protocols that have been widely proposed in the later years for RFID security are suitable for their integration in the PN architecture, while the grant of privileges to access the personal tags, the enforcement of privacy policies, or the exchange of the cryptographic materials required to be authorized against the tag must be securely managed by the PN architecture. Although existing RFID security proposals could be adopted in this network paradigm, the mechanisms will have to withstand the increased delay in case of forwarding of messages through secure tunneling to remote networks; the PN architecture would be requested to handle heterogeneous protocols (as presented previously), and the protocols could take advantage of user presence (e.g., biometrics and explicit interaction) and related resources available in the PN (i.e., cloud of personal devices and services). These aspects are open to future research in the definition of novel security protocols for personal tags.

On the other side, the RFID reader (or personal device with such functionality) is required to implement the proxy/gateway functionality presented in our proposal. Such secure tunneling mechanisms could be implemented in compliance with current RFID standards, as the proposed functionality can act as a novel secure module that uses the RFID and PN network (e.g., Bluetooth, 802.11, and 802.15.4) communication interfaces. The secure module would require to be initialized in order to ensure the authentication and authorization of the requesting node, as well as complete the key agreement required to establish a secure link with such entity, prior to establish the secure bridge between the entity and the final tag. Whereas the standards of the underlaying communication technologies can remain untouched, the authentication and key agreement procedure, as well as generic RFID commands (as introduced in Section 6.3), could be defined in the novel standards for PNs.

In the global vision of the secure PN, current PAN/LAN technologies (e.g., Bluetooth, IEEE 802.15.4/ZigBee, and IEEE 802.11) and WAN interfaces (e.g., 3G/UMTS, WiMax, and LTE) could provide the support required in the realization of such architecture, as higher-level secure management procedures could be deployed as middleware. However, the integration of the security mechanisms required to achieve secure cluster formation and communication as those presented in Section 7.2 would involve link and network level protocols. Moreover, current service and discovery protocols highly increase their discovery times when tunneling mechanisms are integrated to extend their reach to remote clusters [38]. These challenges should lead to novel mechanisms in communication technologies in order to fulfill the requirements of PNs.

In relation to the current initiatives of standards for PNs, our current work focuses on specific aspects not examined in their overview. Our architecture provide the foundation in order to enable the secure integration of personal RFID tags and sensors in future PNs, as well as their interaction with remote devices, discussing related challenges and security mechanisms that should be composed with the solution (e.g., authentication protocols, ownership transfer schemes, secure context management, or tunneling), partially adoptable from those available in the existing literature related to PNs, BSNs, and RFID security. Once this secure integration, management and communication of personal tags is achieved, the resources and features of this kind of nodes, as shown in Section 3, can be exploited from anywhere in the PN and combined with the provision of services and federation of PNs envisioned by the standard initiatives.

On the basis of the results of the Freeband project, the current OMA standardization efforts adopt a service-oriented PN definition. According to OMA [39], the reach of their standardization efforts could embrace service discovery and content management, but aspects related with the particular underlaying technologies such as device discovery or routing could be out of scope. However, the realization of a PN would require such underlying functionalities, the level where RFID and sensors integration would be situated. Therefore, our current analysis cover specific aspects that would complement those in OMA's future service-level definitions. OMA's vision of a PN contemplates a WPAN that could communicate with external entities through a gateway device, such as a mobile phone, being compatible with our current vision and proposal. However, their PN require a Converged Personal Network Service (CPNS) server [40], an entity external to the WPAN, which surrounds the user and which could be managed by a commercial party or a home server. The specific functions of such OMA's server are still to be defined. In our approach, the PN management is controlled from a master device in the PAN; therefore, the user is always able to control his or her network, even if no interface to the IoT or other WAN is available at a specific point in time. OMA's PN definition should take into account this "offline" scenario and grant enough capabilities to the WPAN to guarantee its secure functional state, even deprived of access to the central CPNS server. Moreover, if such third-party server were finally standardized to support the management of PNs, part of the functions in our architecture could be deployed in such server, whereas all the security implications, which have been discussed regarding the integration of RFID and sensors in the PN, should still be considered.

Regarding the recent technical report from Ecma International [15], which provides their general outline of what a PN is and points out a wide range of requirement areas and standardization needs that should be addressed in the future, our current work deepen in some requirements stated in their report, mainly in the management of the network, security, and privacy needs, and we provide the foundations of a secure architecture where the communication and security mechanisms could be integrated to fulfill the previous needs and requirements. Moreover, in the general PN overview presented by Ecma, we contribute analyzing the secure integration of personal RFID tags and sensor technologies in the network paradigm as their report do not refer to specific technologies.

7.2. Integration of related security proposals

In the realization of the proposed secure architecture from a higher-level vision, that is, including any type of personal device in addition to the previously analyzed personal tags and sensors, several results from the existing literature can be integrated to fulfill their requirements and extend the range of functionalities that may be demanded to offer external services and federate multiple PNs. For this purpose, *node initialization* and *pairing mechanisms* are required to imprint any new personal device that has become a PN member. Such mechanism could be based on a parallel offline channel to securely exchange additional data in order to establish initial pairwise keys. In a PN, the user can assist the process providing such channel (e.g., input to both personal devices) or make use of additional proximity communication interfaces (e.g., infrared communication, RFID tags) to provide the required data. The mechanisms defined in [41] can be considered for this purpose as these solutions exploit the possibilities of personal devices with different input/output capabilities and communication interfaces in addition to Diffie–Hellman exchanges to imprint a new personal device. As the role of a master device in the core of the PN can be typically fulfilled by a smartphone, a user-driven approach supported by this particular device can be implemented to *authenticate and register a new device* in the architecture. From this perspective, the security mechanism defined in [42] can be considered although it requires a centralized server and the implementation of IP Multimedia Subsystem/Multi Media Domain (IMS/MMD) functions from cellular systems, as well as the mobile phone-based solutions by Fujino *et al*. [43], which require the previous registration of devices in IMS, which reduces its flexibility. The *authentication of the user in the PN* can be achieved on-demand, whenever explicit user input is required. The solution can range from typing a password to the use of novel mechanisms based on the available input devices. For example, Guerra-Casanova *et al*. [44] authenticate a person by gesture recognition: the user performs a gesture moving his or her hand while holding a mobile device equipped with an accelerometer (similar to a 3-D signature). However, for non-critical decisions, continuous and non-intrusive user authentication could be achieved during the normal use of the personal devices (e.g., voice verification, facial recognition, or even keystroke analysis during keypad interactions [45]).

Beyond the registration of personal devices, *secure cluster formation of personal devices* in the same physical area should be enabled including the establishment of group keys for secure intra-cluster communication. For this need, the solution proposed by Jehangir *et al*. [46] could be integrated, which includes the role of a security agent in charge of distributing and refreshing cluster keys. Once intra-cluster communications are secured, methods to *interconnect clusters* are required. Moreover, *secure inter-cluster routing* requires the creation of dynamic tunnels, as well as the configuration of gateway nodes in each cluster and (centralized) track of all active clusters in the PN. Such tunnels could be based on standardized Internet Protocol Security (IPSec), Transport Layer Security (TLS), or Secure Socket Layer (SSL) mechanisms between unconstrained and severely constrained personal devices. As a user-centric network, the context-related data provided by our secure integration of RFID and sensors could be exploited by the global PN network to adapt the security mechanisms applied such as encryption algorithm, access, or privacy policies. A *context-aware security manager* could be defined on the basis of this information such as the solution provided in [8], which switches between three security levels according to four context parameters (i.e., localization, service confidentiality, battery, and throughput), where sensory and identification data could be combined to define a more dynamic and precise adaptation of security mechanisms.

Related security features, in addition to the security foundations presented in our architecture, include the eviction of members of the PN in case a personal device is lost or stolen; otherwise, the leakage of stored cryptographic materials could compromised the intended security level. In this matter, keys exchange should be forward-secure and leakage-resilient, and mechanisms should allow the revocation of privileges such as the RFID reader revocation for personal documents in [47]. Compared with the privacy threats generated by the leakage of linkable data from RFID tags, the PN multiplies such concerns as information disclosed include IP addresses, security parameters, offered services, or status of available devices, which increases the complexity of controlling the type and amount of personal data disclosed. As the PN could establish relationships for different purposes, a different identity (i.e., set of data linkable to the owner) should be presented to each communication profile in order to link user roles to *virtual identities* to protect user privacy. To achieve this goal, a solution such as the modularized virtual identities defined in Daidalos II [48] can be adapted to define which parts of the user profile are presented in each identity as well as set multiple user pseudonyms.

Once the PN has been securely formed, devices could *offer services* to their peers or external networks based on a framework such as that in [49] to publish the kind of events that a device is able to generate or subscribe to adequate data from others, taking into account user's preferences, privacy policies, or user and cluster context. Although the previous solution and existing standards such as Digital Living Network Alliance (DNLA) are designed for multimedia content, solutions should be adapted to the heterogeneous range of data that can be shared by personal devices. Moreover, security proposals such as the authentication, authorization, and accounting module defined in [50] could be integrated to enable access control to these services. In a step forward from single secure PNs, resources and services from multiple PNs could be composed for a common goal, establishing a *federation of PNs*. Such approach would require authentication mechanisms between different users, which could be based on x.509 certificates issued for the user or for his or her personal devices. The solution could be based on a

personal public key infrastructure such as that in [51] although the lack of permanent access to a TTP and the use of ECC cryptography for resource-constrained devices should be evaluated in the present paradigm. Last, but not the least, rogue PNs could be mitigated through *reputation-based frameworks* such as that in [52] to take into account previous behavior or quality of service of a PN, whereas additional security mechanisms could offer bootstrapping of trust and reputation levels in federation of PNs without revealing previous user's identities.

8. CONCLUSIONS AND FUTURE WORK

As presented, the emerging PN paradigm could benefit from the integration of RFID-enabled personal items, in conjunction with BSNs, as the seamless link between the network and physical reality that surround the user. However, the special characteristics of tagged items (e.g., passiveness, non-IP-enabled, restricted non-IP-enabled communication resources, 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, which should maintain related cryptomaterials, naming information and metadata on sensitive data to enable secure access and interaction with other members and external entities. The deployment and integration 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, in a more practical view, 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 the 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.

Because of the interaction of the heterogeneous personal devices both in local context and through the IoT, our secure architecture requires the support of communication standards in several areas. We have discussed the requirements of our proposal over communication standards in PAN/LAN (e.g., Bluetooth, IEEE 802.15.4/Zigbee, and IEEE 802.11), WAN (e.g., 3 G/UMTS, LTE, and WiMax) and RFID technologies (e.g., IEEE 15693, IEEE 14443, NFC, EPC Gen 2). The deployment as middleware of part of the secure management procedures could be based on current standards; however, the integration of part of the security mechanisms at link and network levels and the limitation of existing PAN technologies in secure tunneling to remote clusters could lead to novel mechanisms. Moreover, our analysis on the secure integration of personal RFID nodes could complement the perspective of the first initiatives to standardize a global vision of PNs.

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, and integrated in wide area networks, instead of analyzed as isolated technologies, leave the door open to novel proposals specifically designed for the requirements and resources of this emerging paradigm.

From a higher-level perspective, that is, including any type of personal device, several results from the existing literature can be integrated to fulfill their requirements and extend the range of functionalities of the core architecture. As discussed, different security solutions could be adopted in areas such as node initialization, pairing mechanisms, authentication and registration of a new device, secure cluster formation, and intra-cluster communication or inter-cluster routing. Additionally, the context-aware security architecture proposed could be extended to include aspects such as virtual identities to protect user privacy, securely offer services, federate PNs, or incorporate reputation-based frameworks.

ACKNOWLEDGEMENTS

This work has been partially supported by the Spanish Ministry of Science and Innovation through the IOT-SEC (ACI2009-0949), ARES (CSD2007-00004) and SPRINT (TIN2009-09237) projects. The latter is cofinanced by FEDER (European Regional Development Fund).

REFERENCES

1. International Telecommunication Union. ITU Internet Reports 2005. The Internet of Things, November 2005, http://www.itu.int/osg/spu/publications/internetofthings
2. Yum DH, Kim JS, Hong SJ, Lee PJ. Distance bounding protocol for mutual authentication. IEEE Transactions on Wireless Communications 2011; **10**(2): 592–601.

3. Piramuthu S. RFID mutual authentication protocols. Decision Support Systems, Elsevier (in press), 2010.
4. Armknecht F, Sadeghi A-R, Scafuro A, Visconti I, Wachsmann C. Impossibility results for RFID privacy notions. Transaction on Computational Science XI (6480) 2010; 39–63.
5. Alomair B, Poovendran R. Privacy versus scalability in radio frequency identification systems. *Computer Communications*, 2010; **33**(18): 2155–2163.
6. Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM, Palomar E, van der Lubbe JCA. Cryptographic puzzles and distance-bounding protocols: practical tools for RFID security. IEEE International Conference on RFID—IEEE RFID 2010, IEEE, IEEE Computer Society, Orlando, Florida, USA, 2010; 45–52.
7. Kavun EB, Yalcin T. A lightweight implementation of Keccak hash function for radio-frequency identification applications. In *Workshop on RFID Security—RFIDSec'10'*, Yalcin SO (ed). Springer: Istanbul, Turkey, 2010; 258–269.
8. Anggraeni PN, Prasad NR, Prasad R. Secure personal network, IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008; 1–5.
9. Malohat Ibrohimovna, Sonia Heemstra de Groot, Jinglong Zhou. Secure and Dynamic Cooperation of Personal Networks in a Fednet, 6th IEEE Consumer Communications and Networking Conference, 2009. CCNC 2009. 2009; 8–14.
10. Project IST-FP6-IP-027396, Magnet Beyond. http://cordis.europa.eu/projects/80699_en.html, last accessed: March 2012.
11. Anggorjati B, Çetin K, Mihovska A, Prasad N. RFID added value sensing capabilities: European advances in integrated RFID-WSN middleware. 2010 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010; 1–3.
12. Xiaoguang Z, Wei L. The research of network architecture in warehouse management system based on RFID and WSN integration. IEEE International Conference on Automation and Logistics, ICAL 2008; 2556–2560.
13. Tolentino RS, Lee K, Kim Y-T, Park G-C. Next generation RFID-based medical service management system architecture in wireless sensor network. In *Communication and Networking*, Kim T-h, Chang AC-C, Li M, Rong C, Patrikakis CZ, Slezak D (eds). Springer Berlin: Heidelberg, 2010; 147–154. 10.1007/978-3-642-17587-9_17
14. Najera P, Roman R, Lopez J. Secure architecture for the integration of RFID and sensors in personal networks. 7th International Workshop on Security and Trust Management (STM11), Springer, Copenhagen, Denmark, In Press.
15. Ecma International. Technical Report TR/102, Personal Networks—Overview and Standardization Needs. 1st Edition, December 2010.
16. RFID Security and Privacy Lounge. http://www.avoine.net/rfid/index.php, last accessed: March 2012.
17. 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* 2009; **15**(5): 970–991.
18. Aigner M. *Security in the Internet of Things*. Workshop on RFID Security—RFIDSec Asia'10. IOS Press: Singapore, Republic of Singapore, 2010.
19. Dominikus S, Gross H, Aigner M, Kraxberger S. *Low-cost RFID Tags as IPv6 Nodes in the Internet of Things*. Workshop on RFID Security—RFIDSec Asia'11. IOS Press: Wuxi, China, 2011; 114–128.
20. Google Nexus. http://www.google.com/nexus/techspecs.html, last accessed: March 2012.
21. Blackberry Bold 9900. http://worldwide.blackberry.com/blackberrybold/blackberry-bold-9900-9930, last accessed: March 2012.
22. Dominikus S, Schmidt J-M. Connecting passive RFID tags to the Internet of Things. Interconnecting Smart Objects with the Internet Workshop, Prague, Czech Republic, 2011.
23. Yu Ng C, Susilo W, Mu Y, Safavi-Naini R. Practical RFID ownership transfer scheme. *Journal of Computer Security—Special Issue on RFID System Security* 2011; **19**(2): 319–341.
24. Song B, Mitchell CJ. Scalable RFID security protocols supporting tag ownership transfer. *Computer Communications*, 2011; **34**(4): 556–566.
25. Kapoor G, Piramuthu S. Single RFID tag ownership transfer protocols. IEEE Transactions on Systems, Man, and Cybernetics 2011; **42**(2): 1–10.
26. Mulligan G. The 6LoWPAN architecture. Proceedings of the 4th Workshop on Embedded Networked Sensors, ACM, New York, NY, USA, 2007; 78–82.
27. Di Pietro R, Oligeri G, Soriente C, Tsudik G. Securing Mobile Unattended WSNs against a Mobile Adversary. 2010 29th IEEE Symposium on Reliable Distributed Systems, IEEE Computer Society, Washington, DC, USA, 2010; 11–20.
28. Jara A, Zamora M, Skarmeta A. An architecture based on Internet of Things to support mobility and security in medical environments. Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, 2010; 1–5.
29. Sklavos N. On the hardware implementation cost of crypto-processors architectures, information systems security. *The official journal of (ISC)2*, A Taylor & Francis Group Publication 2010; **19**(2): 53–60.

30. Oren Y, Feldhofer M. A low-resource public-key identification scheme for RFID tags and sensor nodes. Proceedings of the second ACM conference on Wireless network security, ACM, New York, NY, USA, 2009; 59–68.
31. Plos T, Groß H, Feldhofer M. Implementation of symmetric algorithms on a synthesizable 8-bit microcontroller targeting passive RFID tags. In *Selected Areas in Cryptography*, Biryukov A, Gong G, Stinson D (eds). Springer Berlin: Heidelberg, 2011; 114–129. 10.1007/978-3-642-19574-7_8,
32. Maimut D, Ouafi K. Lightweight cryptography for RFID tags. *Security Privacy IEEE* 2012; (10:2):76–79.
33. Kitsos P, Sklavos N, Parousi M, Skodras AN. A comparative study of hardware architectures for lightweight block ciphers. *Computers and Electrical Engineering* 2012; **10**(2):148–160.
34. Arbit A, Oren Y, Wool A. Toward practical public key anti-counterfeiting for low-cost EPC tags. 2011 IEEE International Conference on RFID, 2011; **38**(1)184–191.
35. Seshabhattar S, Jagannatha S, Engels D. Security implementation within GEN2 protocol. 2011 IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 2011; 402–407. DOI: 10.1109/RFID.2011.5764620. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5764620&tag=1
36. Rolfes C, Poschmann A, Leander G, Paar C. Ultralightweight implementations for smart devices—security for 1000 gate equivalents. Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications, Springer-Verlag, Berlin, Heidelberg, 2008; 89–103.
37. Wenger E, Hutter M. A hardware processor supporting elliptic curve cryptography for less than 9 kGEs. In *Smart Card Research and Advanced Applications*, Prouff E (ed). Springer Berlin: Heidelberg, 2011; 182–198. 10.1007/978-3-642-27257-8_12
38. den Hartog FTH, Blom MA, Peeters ME, *et al*. First experiences with personal networks as an enabling platform for service providers. Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp. 1–8, Philadelphia, August 2007.
39. Open Mobile Alliance, On the definition and architectural needs of Personal Networks. 2008.
40. Open Mobile Alliance, OMA-TP-CPNS-2008-0027-INP-CPNS: CPNS Scope. 2008.
41. Mirzadeh S, Armknecht F, Pallares JJ, *et al*. CPFP: an efficient key management scheme for large scale personal networks. International Symposium on Wireless Pervasive Computing 2008 (ISWPC 2008).
42. Matsunaka T, Warabino T, Kishi Y, Nakauchi K, Umezawa T, Inoue M. Device authentication and registration method assisted by a cellular system for user-driven service creation architecture. 2009 6th IEEE Consumer Communications and Networking Conference. CCNC 2009; 1–5.
43. Fujino S, Motoyoshi G. Authentication procedure and terminal switching scheme for PAN services. In Asia-Pacific Conference on Communications (APCC'06), 2006; 1–5.
44. Guerra-Casanova J, Sánchez-Ávila C, Bailador G, de Santos Sierra A. Authentication in mobile devices through hand gesture recognition. *International Journal of Information Security* 2012:1–19.
45. Clarke N, Furnell S. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security* 2007; (6):1–14.
46. Jehangir A, de Groot SH. Evaluating secure cluster formation in personal networks. Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE, 2007; 3134–3140.
47. Nithyanand R, Tsudik G, Uzun E. Readers behaving badly. In *Computer Security ESORICS 2010*, Lecture Notes in Computer Science, Gritzalis D, Preneel B, Theoharidou M (eds). Springer Berlin: Heidelberg, 2010; 19–36. http://dx.doi.org/10.1007/978-3-642-15497-3_2
48. Sarma A, Matos A, Girão J, Aguiar RL. Virtual identity framework for telecom infrastructures. *Wireless Personal Communications* 2008; **45**(4):521–543.
49. Chaabane A, Louati W, Jmaiel M. A framework for managing composed multimedia delivery in personal networks. Multimedia Computing and Systems (ICMCS), 2011 International Conference on, 2011; 1–6.
50. Jacobsson M, Niemegeers I, Groot SH. *Personal Networks: Wireless Networking for Personal Devices*. Wiley Publishing: 2010. ISBN: 9780470681732
51. Prasad R. *My Personal Adaptive Global NET (MAGNET)*. Springer, 2010. ISBN: 9048134366
52. Ibrohimovna M, Groot SH. Reputation-based service management and reward mechanisms in fednets to improve the quality of cooperation between personal networks. 2010 Fifth International Conference on Digital Telecommunications (ICDT) 2010; 98–103.