An Identity Aware WiMax Personalization for Pervasive Computing Services

Rosa Sánchez-Guerrero, Daniel Díaz-Sánchez, Florina Almenárez, Andrés Marían Patricia Arias and Davide Proserpio
Dept. Telematic Engineering, Carlos III University of Madrid
Avda. Universidad 30, 28911 Leganés (Madrid), Spain
Email: {rmsguerr, dds, florina, amarin, ariasp, dproserpio}@it.uc3m.es

***Abstract*— Mobile Internet access is becoming more and more pervasive in the new 4G scenarios, where WiMAX is to play a crucial role. WiMax has advantages when considering both energy consumption and bandwidth, when compared with HSDPA and LTE. However, we have found some limitations in IEEE 802.16 security support, which may limit authentication and authorization mechanisms for ubiquitous service development. In this article we analyze weaknesses and vulnerabilities we have found in WiMAX security. WiMax, with the adequate identity management support, could be invaluable for developing new pervasive computing services. We propose the introduction of identity management in WiMAX, as a pervious step to the definition of identity aware WiMax personalization of pervasive computing services.[1]**

Index Terms—WiMAX; IEEE 802.16; Security; Identity Management; authentication; personalization.

I. INTRODUCTION

Mobile internet access popularity is increasing with new network technologies, more powerful terminals, and the progressive reduction of tariffs. Mobile internet access has deep implications in pervasive system design and personalization. The lessons learned are still valid: design for worst case uneven conditioning environments, zero configuration and autonomous system, or exploit cooperation for scalability among others. We should benefit from improving network quality and availability, and require adequate support from newer and upcoming network technologies. Adequacy in the sense of ease of integration, and more specifically in invisibility, since human attention keeps the most limiting factor in the whole system. Architectures are progressively moving towards Service Oriented Architectures (SOA), and even to Software as a service (SAAS), like in cloud computing. This movement brings more importance to security aspects of service composition, and user privacy, like in Identity management and established trust relations among the entities of a composite services. They help us minimizing the number of times a user has to be distracted in order to authenticate with the different entities involved in the service.

The importance of WiMAX (*Worldwide Interoperability for Microwave Access*) is growing quickly and is expected to play a key role in 4th generation communication. Besides, recent works like [1] show advantages in power consumption for WiMax over LTE (*Long Term Evolution*) and HSDPA. In this context, security support is a fundamental aspect to be addressed in order to protect users' information as well as corporate networks. WiMax has been in constant revision to address those problems. Several amendments to the IEEE 802.16 standard, as 802.16d [2] and 802.16e [3] that define security mechanisms for fixed and mobile networks, have been proposed in the past few years. The most recent one, from March 2011, is IEEE 802.16m [4] that is part of the Wireless MAN-Advanced or WiMAX2-defined profiles. IEEE 802.16m provides performance improvements needed to support advanced services and applications for the next generation broadband focusing on mobile applications.

Concerning security, the IEEE 802.16d standard security architecture was based on the PKMv1 (Privacy Key Management) protocol that had many security problems, such as Man-in-the-Middle and replay attacks. Later versions of PKMv2 and PKMv3 protocols, used in IEEE 802.16e and IEEE 802.16m respectively, try to address these problems. The Privacy Key Management protocol offers solutions that enable device and user authentication between a mobile station (MS) and the base station (BS) or the home connectivity service network (CSN). In IEEE 802.16, security has been considered as one of the main objectives of the protocol. However, some security mechanisms of EEE 802.16 still have certain threats and risks [5], as how to address security and privacy of user information in an inter-domain scenario, or how to manage identity among different operators. These problems should be addressed to bring access to services in a secure fashion.

Personalization is key to enhance user experience and this has been signalled since the first proposals of ubiquitous computing. Personalization also leads to reduced complexity of management tasks for average users. To achieve this sort of personalization it would be necessary to identify users and exchange their profiles in a secure fashion respecting users' privacy. WiMAX allows the use of X.509 digital certificates together with RSA encryption or Extensible Authentication Protocol (EAP) [6] to perform user authentication and access control. However, nowadays this technology is not able to provide an adequate degree of flexibility to bring a better user experience by its own. Therefore, new paradigms need to be defined in order to make WiMAX a suitable technology for accessing multiple domain services in a user centric, dynamic, and secure manner. According to that, Identity Management (IdM) Systems reveal as an indispensable vehicle to provide a seamless, secure, and personalized user experience within 4G services. To overcome those limitations, we propose the use of an IdM System based on infoCards and SAML along with the WiMAX architecture to

[1] This article has been partially funded by the grant CCG10-UC3M/TIC-4992 from the state of Madrid and Carlos III University and by the State of Madrid (CAM), Spain under the contract number S2009/TIC-1650, project E-Madrid

enable a user centric identity framework for secure and personalized services in a wireless scenario.

The rest of this paper is structured as follows: section II provides a brief background on security WiMAX identifying the challenges to be faced. Section III reviews the current identity management frameworks that lay the foundations of our work. Section IV analyzes requirements for identity management and provides a novel architecture to enhance digital identity management in WiMAX. Then, Section V describes some potential use cases. Open issues and related works regarding security in WiMAX are illustrated in section VI. Finally, section VII summarizes the work and presents the conclusions and future lines.

II. WIMAX SECURITY

WiMAX architecture is composed of two main layers: the **Medium Access Control (MAC) layer** and **physical (PHY) layer**. The MAC layer is responsible for managing connections and security, whereas the physical layer is in charge of handling signal connectivity, error connection, etc. Regarding security, the 802.16 standard specifies a security sublayer at the bottom of the MAC layer. This security sublayer provides *Subscriber Station* (SS) (or Mobile Station (MS)) with authentication and privacy services. It also protects *Base Stations* (BS) from unauthorized network access and service hijacking. In addition, there are two component protocols in the security sublayer: an encapsulation protocol for encrypting packet payloads across the fixed broadband wireless access (BWA) systems, and a Privacy Key Management Protocol (PKM) that provides secure distribution of keying material from BS to SS, as well as, enables BS to enforce conditional access to network services. The reminder of the section describes the WiMAX security architecture and the main concepts on which it is based.

The security architecture [7] of WiMAX is divided in three logical entities that perform security management, encryption, and integrity. The security management functions include overall security management and control, security association management, location privacy, EAP encapsulation and de-encapsulation and PKM control. The latter controls security components such as key derivation, update or usage. The encryption and integrity functions are in charge of dealing with confidentiality and authentication. These functions include message authentication and message confidentiality as well as user data encryption and authentication. Fig. 1 shows the functional blocks of the latest IEEE 802.16 (IEEE 802.16m) security architecture.

1) Privacy Key Management (PKM): The WiMAX standard uses an underlying trust model based on Public Key Infrastructure (PKI) to carry out the exchange of cryptographic material between the mobile station (MS) and the base station others, on the context in which the information is used. Several variants of the PKM protocol have been proposed aiming at covering security issues not addressed in the previous versions. This section gives a brief overview of each variant and discusses their deficiencies and vulnerabilities. First, the IEEE 802.16d standard security was based on PKMv1 [8] which required the SS to authenticate to the BS but not the other way around leading to potential *Man-in-the-middle (MITM) attacks*.

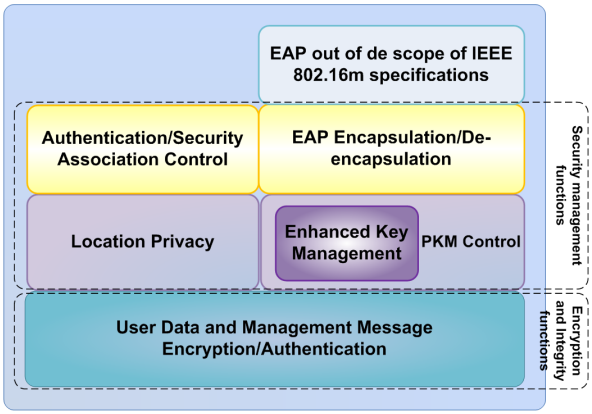

Fig. 1. Functional blocks of the IEEE 802.16m security architecture.

Furthermore, this protocol was vulnerable to *replay attacks* and did not support integrity protection of management frames, exhibiting a risk of *denial-of-service (DoS) attacks*. In order to counter these security issues, PKMv2 was proposed and adopted by the IEEE 802.16e standard, which revised the original authorization protocol to provide mutual authentication, introduced an additional message to provide SS acknowledgment and required three-way authentication based on X.509. Therefore, both the SS and the network entities, that are the BS and the access service network-gateway (ASN-GW), are, in this version, required to authorize and authenticate each other. Moreover, PKMv2 protocol supports the use of RSA to perform key cryptography exchange, which requires the mobile stations to identify themselves using either a manufacture-issued X.509 certificate or an operator issued credential, such as a subscriber identity module (SIM) card. Regarding the digital certificate it should contain the mobile station public key and its MAC address. This kind of certificates allows to validate user's identity on the WiMax network.

After a successful authentication, the mobile terminal negotiates with the serving BS a cryptographic suite for each provisioned service flow. However, this enhanced version is still vulnerable to an *intervalling attack*, in which an attacker impersonates a legitimate SS [9]. Finally, in IEEE 802.16m a new protocol called PKMv3 is proposed, which adds an extensible framework for previous PKM supporting key agreement in multi hop relay for broadband wireless access. However, this version does not consider dynamic multi-hop connection between BSs and Relay Stations (RSs), and cannot defend the network against some security attacks as IP spoofing. Some proposals which may help to address this problem can be found in section IV.

2) Authentication and Authorization: In few words, authentication is a mechanism to determine that a user sending a message is really who he claims to be. Authorization is the process responsible for assigning privileges to users that would govern the access control that would determine what services or resources a user may

access. These processes typically involve three kinds of entities: 1) a client or supplicant, which resides in the mobile station; 2) an authenticator, which can reside in the base station or in a gateway; and 3) an authentication server.

WiMAX allows the use of X.509 digital certificates together with RSA encryption or Extensible Authentication Protocol (EAP) to perform user authentication and access control. However, enforcing security and privacy in inter-domain scenarios or managing users among different operators are security topics that need to be addressed in order to deliver services in a secure fashion regardless the administrative domain. IdM systems have become indispensable to provide a seamless and secure user experience when dealing with high distributed services provided through different networks as in 4G scenarios. Furthermore, IdM infrastructures reduce the complexity of service deployment and maintenance in wireless environments, such as WiMAX, where network operators need to integrate mobile and fixed telephony together with Internet and business services that might belong to different trust domains. Finally, user personalization is one of the most outstanding topics in service provision requiring security and privacy.

IdM provides mechanisms like Single Sign On (SSO), which allows users to authenticate once when accessing several services, to obtain personalized contents or services without providing any additional information. This sort of user management is adequate for providing tailored services to users that might require cooperation of the access network provider, for instance, for assigning different QoS according to their preferences and needs. Moreover, IdM systems deal with privacy by controlling which attributes are disclosed to each service.

Since new mobile devices with increased capabilities allow users to access services everywhere, giving complete freedom to the end user it is necessary to manage user preferences, security, privacy and personalization as a whole involving services and providers. Unfortunately, WiMAX is not currently able to give this improved experience to users. Therefore, new paradigms, as the one we are proposing in this article must be defined in order to make WiMAX a suitable technology for accessing multiple domain services in a user centric, dynamic and secure manner.

III. IDENTITY MANAGEMENT FRAMEWORKS

There are several disjoint approaches to Digital Identity: user-centric, federated, or corporate. However, the actors in an identity management scenario can be classified as follows:

- The Principal, or end user, who has a particular digital identity. He interacts (usually via an user agent, typically a web browser), with a Service Provider.
- Service Provider (SP), which provides services and takes decisions based on the information that is provided by a third party about a particular subject. SPs are sometimes called Relying Parties.
- Identity Provider (IdP), which focuses on enforcing authentication and managing the identity information, which can be shared with various SPs.

Identity Management is available in several flavours; there are formal standards, open source technologies or openly published specifications covering different approaches. However, the most prominent effort towards a formal definition has been bought by SAML [10] that defines a security assertion language over which IdM technology can be built. SAML is tightly coupled to several federated identity or user-centric identity specifications and implementations, like the Liberty Alliance Identity Federation Framework [11], WS-Federation [12] or Shibboleth [13]. InfoCards [14] is the most outstanding user-centric identity approach. InfoCards, with the aid of SAML, defines a framework to proffer users full control over their identity information, as well as, their authentication mechanisms. Our proposal combines the benefits of SAML and InfoCards technologies for better identity management in WiMAX networks.

1) Security Assertion Markup Language (SAML): defines an XML based framework that allows to express assertions about an identity, including attributes, authorization and/or authentication information of a subject with the aim to facilitate relations between different security domains their users. This specification defines four key elements: *Assertions*, which carry statements about a Principal as asserted by an IdP and can be related to authentication, attribute exchange or authorization; *Protocols*, which describe the sequence of request-response messages governing the exchange of Assertions; *Bindings*, which define how SAML Assertions and request-response protocol messages can be exchanged between entities using a given underlying communication protocols (such as HTTP, Diameter, SIP, etc.); and *Profiles*, which define the specific sequence of messages and the Bindings required in each case to complete the use cases defined in the standard. Variations of the same profile can be obtained for each combination of use case and Binding. Finally, note that SAML is highly flexible, which allows all its components can be extended.

2) Information Cards: Infocards constitute the digital metaphor of the cards we carry every day in our wallets (e.g. credit cards, id card, driving license) and we use in transactions in our daily live. The same concept or metaphor can be extended to the wallet itself, so, as we have digital cards, we also have “digital wallets” or, in terms or user-centric nomenclature, Identity Selectors.

Identity selectors allow users to manage their cards selecting the most appropriate credential as when we show our driving license to a police officer or the library card to the clerk and not the other way around. So the user decides when to submit, what, and to whom. As we have mentioned before, InfoCards is a user-centric identity technology that allows users to select among their multiple identities inside their identity portfolio to identify themselves to services. Thus, users can manage in a comprehensive way their different electronic identities mimicking the real life. It brings more transparency, though the SP may obscure its

purposes, or use different identities, making difficult to the user to understand what and why are required.

Regarding identity selectors, in [15] two types of InfoCards are specified: *Personal* or *Self-Issued* (claims about the user itself, e.g. phone number, e-mail address, web address); and a *Managed Information Cards*, issued by Identity Providers. The latter can be auditing, non-auditing, or auditing-optional to accommodate the needs of different business models. There are several implementations of this concept as Windows CardSpace [16], Higgins project [17], Open Source Identity Selector [18] or Bandit [19].

In addition, InfoCards support several data formats and authentication methods such as XML, SAML, and OpenID. InfoCard-based identity management systems typically use Web Services Security protocols (WS-*) and SOAP. WS-Trust [20] is preferred protocol to obtain and exchange security tokens. Moreover, the integrity of the tokens is preserved using an XML-Signature that is part of the WS-Security [21] protocol.

IV. IDM ARCHITECTURE FOR SECURE PERSONALIZED SERVICE PROVISION OVER WIMAX

A. Objectives and Requirements

Our proposal pursues to overcome the limitations of current user management in WiMAX: providing an identity framework that copes with the needs of the different actors as users, network operators, roaming networks and application service providers, maintaining a high security degree, and achieving a better personalization. The objectives can be summarized in:

- Comprehensive identity management: allows users to safely manage their own identity information, such as changing passwords, subscription status, the choice of opting for mobility, changing roaming authorization, modifying user profiles.
- Basic security primitives: provides privacy, confidentiality, integrity, authenticity.
- Seamless interaction among entities: Our architecture enables interaction with third party applications, as well as, secure exchange of authentication credentials and personal profiles with the visited network operator and application service providers, to deliver secure and per-sonalized services in a transparent manner even during roaming.
- Simple configuration: our solution minimizes configuration tasks from user side. Regardless the access network provider or the terminals, users would access consistently to their services that would be personalized according to their user profiles. In such a way, users profiles are no longer tied to network identifiers. Users would keep their identity as an overlay regardless the access network provider.
- Interoperability: The identity management system relies on open standards in order to facilitate the interoperability with other systems. Our system uses EAP, InfoCards and SAML. The latter is the only open standard and is characterized by its high flexibility, so compatibility is assured.
- The identity management framework must exchange identity information in a seamless, efficient and scalable manner.

B. Proposed Architecture

In this section we describe the functional architecture of the proposed WiMaX security infrastructure. It is important to note that our proposal does not substitute but complements existing WiMAX security solutions. As can be seen in Figure 2, our system consists of federated entities with the following roles: 1) the Network Service Provider (NSP) defined in WiMAX, with some identity extensions; 2) the Content Provider, which provides different kinds of content (e.g. multimedia, voice over IP) that requires different QoSs; 3) the SAML Identity Provider (IdP), which vouches for the identity of a user and supports several authentication mechanisms (e.g. InfoCards, user/password, digital certificates, EAP-AKA (U-SIM) and 4) the User, which interacts with the NSP and the IdP through his devices (using an identity selector). SAML messages exchanged among entities are encapsulated as EAP payloads and transported over Diameter. The idea is to offer security services, multiple factor authentication and flexible user profile management, which enables to facilitate for instance QoS management and service personalization in a robust and flexible manner.

For the practical realization of this solution we divided our system into a series of interconnected software blocks that distribute all the functionality in a modular fashion. To dive deeply into the details of these modules, we provide an individual explanation of each one in the following sections. Note that, the SAML Identity Provider (IdP) located in the home network operator domain is not part of the WiMAX security infrastructure itself since handles user authentication and profiles on behalf of any service. Finally, it must be also noted that Fig. 2 only sketches out the additional components defined in the NSP.

1) Session Management module (SM) is responsible for retrieving the user profile, the subscription profile and the device profile, as well as, maintaining an adequate session context at each moment. Furthermore, this module performs tasks related to linking a user profile defined in an InfoCard to a session identifier and it may check several profiles in order to determine the most appropriate content for a specific service (e.g. encoding). Note that the SM can be located at the WiMAX Home Network Service Provider or as part of an external SAML IdP. In the first case, it communicates with the Service Personalization module in order to carry out the user profile exchange. Otherwise, if this logical block is collocated with the IdP, it is responsible for verifying and managing SAML authentication assertions and attribute statements issued by the IdP. This module communicates with other modules handling authentication and attribute exchange services, as well as, the User management module. Moreover, this module requests the user profile and the device profile to the Identity Provider and matches user's

identity with the subscription profile policy and any other enforced IdP security policy.

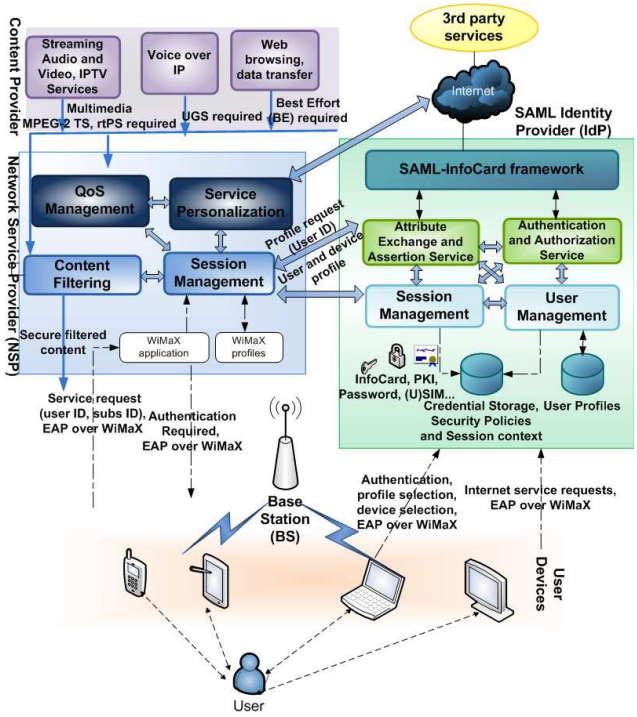

Fig. 2. Security Architecture for Service Personalization in WiMAX.

2) Personalization Service module (PS) receives the user profile from a profile store, which is an extension of the 3GPP HLR / HSS (extended HSS), thereby enabling its use as a standard [23] one or with additional identity management capabilities. Moreover, the extended HSS may request to increase or modify privileges or perform customization according to security policies defined in the SAML IdP. Furthermore, this module interacts with the SM module for retrieving information from service/user data and other services to personalize the WiMAX service. Note that, the degree of personalization depends on the information disclosed by the user in his profile that will be governed by the credential chosen using the identity selector.

3)QoS Management and Filtering: The QoS Management (QoSM) module plays a similar role as the Proxy-Call Session Control Function (P-CSCF) entity in NGN architectures and is in charge of dealing with quality of service features. It extracts the necessary QoS information in order to find out an appropriate mapping to WiMAX parameters. The IEEE 802.16/WiMAX standard defines a QoS framework for different classes of services. The following describes the main types of supported services, each of which has different QoS requirement:

- ***Unsolicited grant service (UGS)***: suitable for traffic with very strict QoS constraints for which loss and delay need to be minimized (e.g. voice over IP), because the UGS service allows BS to allocate a fixed amount of bandwidth to each of the connections in a static manner, supporting constant-bit-rate traffic.
- ***Polling service (PS)***: the amount of bandwidth required for this type of service is determined dynamically based on the required QoS performance and the dynamic traffic arrivals for the corresponding connections. This service supports traffic for which some level of QoS guarantee is required (e.g. real time applications).
- ***Best Effort Service (BE)***: the amount of bandwidth allocated to BE services depends on the bandwidth allocation policies for the other types of services seen before. Therefore, this service is suitable for traffic with no QoS guarantee (e.g. web, e-mail).

Moreover, the QoSM module sends parameters to the WiMAX resource controller, which is the Connectivity Service Controller at the ASN. To do this, it has to interact with the IdP for performing session establishment or modification, authentication and authorization of users, as well as, the negotiation of media attributes (e.g. QoS parameters). The *QoS Management* module communicates with the *Personalization Service* module to provide a personalized QoS taking into account user preferences, subscription profile and security features.

Finally, the QoS parameters, the user profile, the subscription profile, the device profile and the security policies can be taken as inputs to compose a secure filter, which allows presenting content according to users and devices requirements.

4) User Management (UM) module is in charge of managing users' profiles according to their preferences, storing credentials and enforcing security policies. It allows users to generate their own InfoCard (*Personal* or *Self-Issued*), which can be stored in his device for personalization. These information cards can be issued and managed by the SAML IdP and they may contain some network parameters subject to verification. Note that we assume that applications not needing stringent security requirements, such as blogs, forums, news services, would trust self-issued InfoCards.

One of the main advantages of using InfoCards is that they give users more control over the process of disclosing their attributes to services. In addition, attribute information obtained from InfoCards, allows the UM module to build or complete the user profile. However, apart from infoCards, other types of credential (e.g. username/passwords, digital certificates, or GBA) can be stored. Thus, the UM module enables the IdP to act on behalf of the user and authenticates to the different applications providing an easy and seamless navigation experience.

Security policies are defined by a configurable set of rules that evaluate conditions based on profile attributes in order to deny or grant permissions for a subject to access particular services. For instance, different delegation or security policies rules can be established depending on, for instance, whether the user is on his personal or work network.

Therefore, when the *User Management* module receive a request for fetching a profile (which contains a user

identifier) from the SM module network service provider, if the user does not have a valid context session, the request would be redirected to the IdP for requesting authentication. Then, the user authenticates, selects the attributes to disclose in his profile (or a predefined user profile or card) and selects the device (or leaves it to the default). Finally, the UM module retrieves the corresponding user and device profiles and obtains an applicable security policy.

V. USES CASES

In this section, we present some potential use cases that inspired the proposed infrastructure. These use cases might give an idea on how the user experience can be improved when he accesses to a wide range of high-quality and high capacity IP-based services and multimedia applications while maintaining full backwards compatibility with the existing WiMAX system:

1) Personalized content: All the content (social networks, multimedia applications) can be displayed according to the preferences of the user accessing to the WiMAX network. This is achieved through the SAML IdP, which provides services for user authentication, user profile management and device profile selection. User authentication can be performed by either third party credentials such as PKI or user/password or IdP (managed infoCard). In addition, a device can be explicitly selected by the user or automatically selected according to the context and preferences. The user, device and subscription profile are associated under a WiMAX session linked to a specific user identity and can be used for accomplish service and content personalization.

2) Personalized QoS and service mapping: The quality of service can be automatically o explicitly selected by the user according to his preferences if it is permitted by the network (e.g congestion level, allocated bandwidth). For instance, if the user is in a meeting and he must communicate with his partners through video conference, he can explicitly request a service mapping to the WiMAX UGS to provide a constant bandwidth for that traffic. Or, if the user is checking his mail at home, BE service class could be mapped automatically.

3) Profile and network roaming: A user can move his profile between different devices, for example exporting his Information Cards. Furthermore, our infrastructure allows user to change his profile when changing his usual location. On the other hand, the proposed IdM framework offers users greater control over their privileges allowing to define per-provider profiles supporting so the nomadicity of users.

VI. RELATED WORK

The IEEE 802.16 standards and WiMAX Forum documents centre their security on the device or on a user identifier avoiding further personalization. As we have discussed, access control, authorization and personalization are crucial for a better user experience. Moreover, with the advent of complex resource control services, new attack opportunities have aroused [24], such as DoS attacks. Moreover, service and billing frauds can take place if there are third-parties masquerading as legitimate ones.

Regarding mobility, the IEEE 802.16 security design has not yet considered dynamic multi-hop connection between mobile Relay Stations (RSs) and BSs. Another important aspect that current WiMAX standard does not address well is mesh next hop trustworthiness. The additional dimensions of RS mobility and multi-hop connection create various security vulnerabilities such as IP spoofing. Moreover, mesh operation mode and mobility add more complexity to key management. Therefore, there are necessary security protocols for dynamic networks that address the trustworthiness of the next-hop BS/RS. Several works, which deal with distributed and dynamic trust relationship in wireless and pervasive environments, can be found in the literature. In [25] a distributed trust relationship (DTR) model for mobile BWA networks is proposed as an extension of the IEEE 802.16 security protocol. This approach defines a framework, which uses a polinomial-based key distribution to enhance the establishment of a mutual networking trust relationship between any two networking entities; as well as, the multi-hop security authentication among mobile RSs and BSs.

Another interesting proposal [26], illustrates a decentralized trust management model for pervasive computing that could be adapted to operate at network level. Eventually, it must be noted that, in WiMAX, security threats and vulnerabilities apply to both the physical and the MAC access control layers. However, nowadays there are no efficient techniques to prevent physical layer attacks, such as jamming or scrambling. For that reason, WiMAx security focuses mainly on the MAC level [27].

VII. CONCLUSIONS AND FUTURE WORK

The proposed identity management infrastructure combines the benefits of IdM frameworks as SAML and InfoCards to achieve seamless and secure service personalization in a WiMAX scenario. As far as the WiMAX security features are concerned, in this paper we have reviewed its security architecture and have identified some weaknesses in regard to user management and digital identity management. With the introduction of the SAML Identity Provider, we have designed a user-centric architecture that allows to deal with authentication, user profile and device profile management for better identity management in WiMAx networks. It is important to note that our proposal does not substitute but complements existing WiMAX security solutions, while enabling secure personalization of services and improvement of user experience. Finally, we have analyzed unsolved challenges in WiMAX security, such as DoS attacks, service and billing frauds and we have presented some approaches which try to address secure mobility issues.

As future work, we are focusing on the integration of our IdM infrastructure in LTE since currently it is highly deployed compared to WiMAX. Moreover, LTE provides the necessary building blocks, as EAP-AKA, therefore we believe that our proposal could complement LTE authentication mechanisms to provide a better user experience. Further research could include a deep study on LTE security to identifying limitations that can be covered

with identity management. Finally, we aim to test the performance of the proposed identity system.

REFERENCES

[1] M. Deruyck, W. Vereecken, E. Tanghe, W. Joseph, M. Pickavet, L. Martens, and P. Demeester, *Comparison of power consumption of mobile WiMAX, HSPA and LTE access networks*, 9th Conference on Telecommunications Internet and Media Techno Economics (CTTE), june 2010.

[2] IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems", IEEE Press, 2004.

[3] IEEE 802.16-2005, "IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005.

[4] IEEE Std 802.16m, "Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Broadband Wireless Access Systems - Advanced Air Interface", IEEE Press, 2011.

[5] P. Rengaraju, L. Chung-Horng, Q. Yi and A. Srinivasan, "Analysis on mobile WiMAX security" , Science and Technology for Humanity (TICSTH), 2009 IEEE Toronto International Conference, September 2009.

[6] B.Aboba, L.Blunk, J.Vollbrencht, J.Carlson and H.LevKowetz, *Extensible Authentication Protocol (EAP)*, IETF RFC 3748, June 2004.

[7] IEEE 802.16m -09/0034r3, "IEEE 802.16m System Description Document", December 2010.

[8] D Johnston and J. Walker, Overview of IEEE 802.16 Security, IEEE Security & Privacy, magazine May/June 2004.

[9] C. Huang and J M. Chang, "Responding to Security Issues in WiMAX Networks". IT Professional, 2008; 10(5): 15-21.

[10] Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., Scavo, T.(eds).: Security Assertion Markup Language (SAML) V.2.0 Technical Overview. OASIS Comittee Draft 02. March, 2008.

[11] LA.: Liberty ID-FF Protocols and Schema Specification. Available at http://www.projectliberty.org, September 2011.

[12] WS-Federation.: Web Services Federation Language version 1 1. December, 2006.

[13] Internet2.: Shibboleth Architecture. Available at http://shibboleth. internet2.edu. April 2011.

[14] Information Cards.: Information Cards Foundation, 2009. Available at http://informationcard net/, September 2011.

[15] A. Nanda and M B. Jones (eds.):Identity Selector Interoperability ProfileV1.5. July 2008.

[16] Microsoft Windows CardSpace. Available at http://msdn.microsoft.com/ enus/library/aa480189.aspx, April 2011.

[17] Higgings.: Higgins Open Source Identity Framework. Available at http://eclipse.org/higgins/ , March 2010.

[18] OSIS: Open Source Identity Systems. Open Source Identity Systems Wiki. Available at http://osis.idcommons.net/, April 2011.

[19] Novell, The Bandit project. Available at http://www.bandit-project.org/, April 2011.

[20] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, and H. Granqvist: WSTrust 1.3. OASIS standardd. March 2007.

[21] A. Nadalin, C. Kaler, R. Monzillo and P. Hallam-Baker (eds.): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS standard Specification. February 2006.

[22] WiMAX Forum, "Network Architecture Stage 2-3" Re 1, v1.2. Available at http://www.wimaxforum.org/resources/documents/technical/release, September 2011.

[23] WiMAX Forum, "WiMAX Forum Network Architecture", Pre-Release 8 3GPP Interworking, November 2011. Available at http://www.wimaxforum.org/sites/wimaxforum.org/files/technical document/2010/ 12/WMF-T37-008-R016v01 PreRelease8-3GPP-IWK.pdf, September 2011.

[24] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks. Globecom Workshops", 2007, IEEE, Nov. 2007, Page(s):1 - 6.

[25] A. DeCarlo, J. Portny, S. Tyler, B. Xie, R. Reddy and D. Zhao, "Distributed trust relationship and polynomial key generation for IEEE 802.16m networks", (2009) *Proceedings* - 2009 IEEE Mobile WiMAX Symposium, MWS 2009.

[26] F. Almenrez, A. Marn, C. Campo, and C. Garca, "PTM: A Pervasive Trust Management Model for Dynamic Open Environments. In First Workshop on Pervasive Security, Privacy and Trust PSPT'04, 2004.

[27] M.Barbeau, "WiMax/802.16 Threat Analysis", Procceding of the 1th ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet '05, ACM Press, Page(s):8.-15, 2005.