



Identity Driven Mobility Architecture

Alfredo MATOS¹, Ricardo AZEVEDO², João GIRÃO³

¹*Instituto de Telecomunicações de Aveiro, Univ. Aveiro, 3810-193 Aveiro, Portugal*

Tel: +351 234 377900, Fax: +351 234 377901, Email: alfredo.matos@av.it.pt

²*Portugal Telecom Inovação, Aveiro, Portugal, Email: ricardo-a-pereira@ptinovacao.pt*

³*NEC Laboratories Europe, Heidelberg, Germany Email: joao.girao@nw.neclab.eu*

Abstract: This paper describes an identity based mobility architecture, which relies on the Identity Management System for mobility decision and execution. This is achieved by clearly separating mobility into a two step procedure: decision and action. The decisions are outsourced on the Identity plane, while the action (moving) is carried out by a protocol agnostic mobility architecture.

Keywords: Mobility, Actuation, Policies, Architecture, Identity Management.

1. Introduction

It is becoming clear that Identity will play a major role on the Future Internet. It provides a wealth of features, such as new semantics for the network, enhanced user centric capabilities, and a rich information environment with unrivalled levels of privacy, security and. The SWIFT [1] (Secure Widespread Identity for Federated Telecommunications) project is taking advantage of such features and applying identity not only as an application layer technology, but as a network driving force that can couple different layers [4], focusing on a user centric network. The resulting paradigm, according to the Swift framework [3], is that most network information is identity bound turning identities into the new communication endpoints [13].

In spite of this transition, mobility still focuses on devices and associated physical conditions. Until recently, the most important information for mobility was the device's signal strength, coupled with available networks. For the Future Internet we need to consider a plethora of factors like user preferences, user and network policies, service information, permissions or network conditions, resulting in a wider set of requirements [2].

The common denominator drops to identity, where most information is now directly or indirectly tied to the user identity, elevating the IdM system to the driver seat of the network, and consequently, mobility. Having identity at the core of the mobility architecture enables a user centric approach to information and policy distribution capabilities: the identity framework naturally fits a control view of mobility, since it stores many of the user's and network's policies, along with relevant user attributes, accessible on demand. Such benefits have already started to be uncovered as stated [17] and [15], where identity centric networks begin to show their value for both network and user.

We propose to bring identity to the core of mobility management by separating the control process for mobility from the action of moving between networks or devices. The guiding concepts for such separation are discussed in Sec. 3 while Sec. 4 details the emerging paradigms, leading to the architecture presented in Sec. 5. We conclude the paper in Sec. 6 by discussing the benefits and drawbacks of such solution.

2. Related Work

When considering mobility management, the natural bias is towards the operational aspects. In such landscape, attention is mostly devoted to classical mobility solutions, of which Mobile IPv6 [5] and derivatives have become the standard approach. These solutions focus almost entirely on the operational aspects of device mobility, and can be considered a tool that solves one aspect of mobility, but does not provide a strong framework for handling the informational and control aspects of mobility. Similarly, other mechanisms enable different types of mobility, like the Session Initiation Protocol (SIP) [8], which can be used to implement terminal, service, session and even personal mobility, but again only targeting operational aspects. From the previous protocol examples, we can acknowledge that there is no common approach that aggregates different mobility protocols, thus creating a gap on how to integrate them together both in control and operational views.

An architecture that introduces identity as a main actor in the network is the Host Identity Protocol (HIP) [7]. It provides a method of separating the identifier and locator roles of IP addresses by introducing a new Host Identity name space, based on public keys that represent the host's identity. While HIP is operational in nature and does not provide a mobility decision framework, it shows how useful identity information can be in the network. This already enables some form of integration with Identity Management as addressed in [15]. However, a formal framework that integrates a common mobility driver is missing, whether based on Identity or not.

A recent standardization effort was focused on information distribution for handover mechanisms. IEEE 802.21 [14] defines media independent handovers (MIH) functions that enable a low level information distribution mechanism to assist the mobility process. By using the Media Independent Information Service (MIIS) it provides a network oriented approach for information distribution, which enables mechanisms for information distribution for the handover process, but fails at providing a cross layer mechanism given its narrow applicability. This is another useful tool in mobility management, but not a vertical control layer. By manipulating 802.21 as a tool, the mobility extensions presented in [12] try to gather as much input as possible both on the network and on the terminal, covering Quality-of-Service and network related user preferences to perform "smarter" mobility decisions. While interesting, and a step in the right direction, this solution falls short of the cross layer approach that is required for the Future internet. Such solutions leverage the operational aspects of the different protocols, but do not make a strong argument for a common and vertical mobility and informational management layer.

Most of the aforementioned solutions fail acknowledge what we see as a requirement: it's not about moving devices, it's about the user and user centric processes. Mobility is just an action like any other that requires a strong control layer that does not focus on signal quality or similar metrics but that on a cross layer approach that empowers the user and the Future Internet.

3. Identity Centric Mobility Management

Identity brings forth advantages to user and service interaction. The concepts that stem from identity management architecture revolve around enhanced security and privacy as part of the core system value. The SWIFT framework [3][17] expands on these concepts to provide a cross-layer architecture with a vertical notion of identity, which goes beyond current IdM systems, SAML [16] based architectures, the current standard for IdM, rely on the generation of pseudonyms for each service, breaking the user identity into small pieces that are presented at different providers. In SWIFT, these pseudonyms are not restricted only to the service provider, but rather compose a complete identity, that encompasses all layers. As the user interacts with different services the user assumes different (virtual) identities

(e.g. work profile or family profile), as described in the Virtual Identity (VID) Framework [4]. The VID framework systematizes the approach that a user has many different identities, instead of a single information set. Each of these virtual identities has different preferences, attributes, credentials and policies, leading to a volatile environment, where interaction are defined per virtual identity, even on a network level. Consequently, every network interaction is influenced by identity information, a key concept of the VID framework, where identities are the real endpoints of the communication. In this ecosystem, the IdM system gains a new dimension by defining itself as a core technology.

3.1 – Identity Management Architecture

When referring to IdM systems, we are considering a specific subset of entities that provide the basic IdM functions: strong authentication and authentication between all the involved entities; secure attribute exchange and information storage; policy oriented mechanisms as privacy and decision enablers for the aforementioned functions. These key issues define the tools that will be required for building the mobility architecture.

The SWIFT Identity Management architecture¹ [3] is a SAML 2.0 [16] based system with cross layer functionalities, enabling authentication, access control and a distributed policy environment. It's composed of three primary entities:

- **Identity Aggregator (IdAgg)**: The IdAgg stands out as the coordinating entity for all user related information, and is present in every identity provider's domain. It stores the user's VIDs and pseudonymized references to all user information (e.g. attributes or authentication context). It knows where such information is stored (even though not storing it itself for privacy preservation purposes), by interacting with the remaining SWIFT entities.
- **Authentication Server (AuthS)**: The AuthS provides the key authentication related features for the end user and associated information. It stores policies, authentication contexts, and any relevant information to provide important features like authentication, access control and Single-Sign-On.
- **Attribute Server (AttS)**: The AttS is the central information repository which stores user related attributes, allowing the retrieval and storage of user information. It stores user information, referenced by pseudonyms thus protecting user privacy.

For the mobility architecture, both the AuthS and AttS can be directly reused, but the IdAgg, given its central role, should be the core entity for the mobility aspects. Also noteworthy is that part of the lure of IdM systems is the creation of distributed policy environments [9], where policies play an important role in the framework, for access control, information, context or networks, among other resources.

These features determine the basic components of the IdM Infrastructure that will have the most active role for the mobility management functions.

3.2 – Identity Driven Mobility

As mobility becomes less about maintaining sessions and more about enabling a better user experience, it is this user centric characteristic that turns mobility into an identity driven process. The paradigm is becoming about user centric information, and applying network functions towards user needs, rather than centring the mechanisms on the network itself. As such, a plethora of vectors contribute to the decision of where a terminal attaches and whether it is necessary to change point-of-attachment. To accompany the shift, it becomes clear that the mobility functions must be defined according to the notion of identity. It should be possible to formulate identity dependent mobility decisions. We rely on a rich

¹ For more information on the SWIFT IdM architecture please refer to [17], [3], [10] and [1].

information set and the application of mobility protocols as tools transformed into a cohesive architecture by a vertical IdM layer.

To provide a rich information environment we use the attribute server as storage for mobility and user related information, rather than creating protocol dependent entities that store only a subset of information (e.g. MIIS server in 802.21). The dynamic nature of the information that contributes to the handover and mobility decisions implies the use of an adaptive structure (not the semi-static information types defined by current protocols) since we cannot presume to define all the information that will be important for mobility in the Future Internet. Also, the information can be shared across different protocols, rather than a protocol-specific silo.

Focusing on the protocol tools, no single protocol has proven to be superior to others, especially considering different layers. Therefore, we must acknowledge that in the future internet there will one single protocol, but many, performing there individual functions. This will create a need for a coherent control layer that will naturally fall on the IdM plane.

Finally, a key issue for using the IdM as a primary element in the mobility management architecture is that there is a tight authorization and access control, which is particularly interesting when defining complex mobility scenarios that involve multiple network providers with different identity-dependent attributes, such as Quality-of-Service or technology availability.

4. Splitting Mobility into Control and Action

We propose a clear definition of mobility as a two-step process, consisting first, the decision and second, the actual process of triggering and executing mobility. While the decision process that will guide user or session movement is ultimately protocol independent, mobility management is clearly linked with the protocols used at different levels in the network. The entire mobility decision process forms the control layer, while the process of triggering mobility, i.e. determining the necessary actions and performing them, is the actuation layer. This lead to the separation shown in Figure 1 where we can see the mobility process divided in two layers: the Mobility Control Layer and the Mobility Actuation Layer. A brief description of each layers are presented next (a complete description and discussion can be found in [10]).

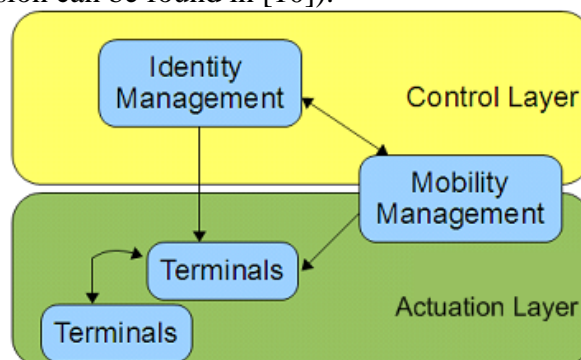


Figure 1 – Control and actuation duality

4.1 – Mobility Control Layer

The first part of the proposed mobility management scheme is protocol independent, serving a dual purpose: it acts as the information repository for storage, and as the decision plane, based on cross-layer information focusing on mobility as a policy based mechanism.

Acting as the information repository the control layer is concerned with both static and dynamic information. Static information can be characterized as capabilities or features of

user (e.g. preferences), network (e.g. contracted bandwidth) and devices (e.g. display size). On the other hand, dynamic information deals with the surrounding environment or conditions (e.g. network load or user location) and policies that define the guidelines over capabilities and environment. Consequently, the identity control layer should act as the information hub for all data relating to mobility protocols and decisions.

The entire information collected from the network and user, should then be coalesced into a relevant control pattern that establishes what actions should be taken (policy trigger and driven), to enable the mobility processes, conveyed the results of the policy executions as mobility decisions, pushed into the actuation layer.

This high level process is shown Figure 2 where a “control decision” taken in the identity management component is translated into an “action” of moving the session from one identity to another, establishing a barrier between control, and all the necessary function, and the action of moving the session between identities.

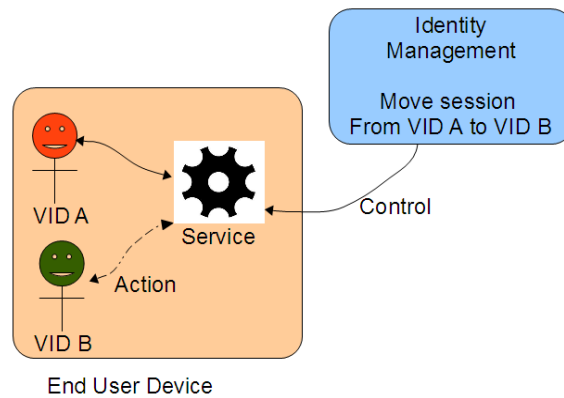


Figure 2 – Mobility Management split into Control and Action using IdM

4.2 – Mobility Actuation Layer

The high level mobility process decisions are outsourced to informed components relying on identity management. But, once a decision is sent from the control layer, it will need to be converted to protocol actions as also highlight in Figure 2. Consistent with the two step process, the actuation layer is able to determine what actually needs to be done in results of a decision, and how to realize those actions. This is achieved by introducing a protocol independent adaptation layer, and a protocol dependent action enabler:

- Generic Actuation Layer (GAL): Provides high level abstractions that can be used in mobility centric decisions, and breakdown generic identity driven decisions into protocol and layer oriented decisions
- Protocol Actuators: Take the executions of the GAL and propagate them as protocol specific operations.

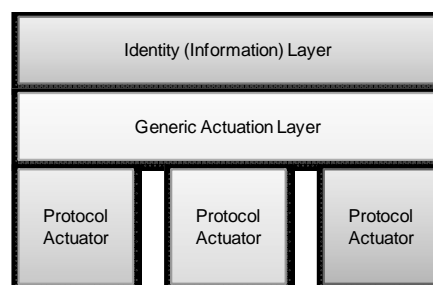


Figure 3 – Generic mobility and identity abstractions.

By taking advantage of semantics capable of describing the mobility process, in generic terms, the identity management components are able to apply policies, and convey

decisions to the mobility management components. But, the semantic should not be focused on specific mobility action that must be taken. Therefore, the GAL converts the high-level decision, by clearly identifying the available identities, sessions and devices, into actions that fit the granularity of the mobility protocols. This allows mobility to be expressed independently of the protocol and a parallel course of action towards the protocol actuators, which provide the functions and triggers to directly cause their mechanisms to be operated.

From an abstract approach, we must provide a common semantic approach to mobility, enabling the dissemination decisions, understood at the GAL, that translate into particular protocol actions.

5. Generic Mobility Architecture

Control and actuation define the two concepts which become the cornerstone of the proposed identity driven mobility architecture. However, the strength of this approach relies on the translation of these concepts into feasible entities that are transposable onto the Swift architecture. Moreover, these abstract roles will allow modelling the mobility process encompassing multiple protocols and still remaining consistent through a common control.

5.1 – Architectural Components

The basic assumptions for defining the generic entities are that control is done through information and decisions, while the actuation process is the enforcement of the decisions originating in the control layer. The specified requirements can also be observed in generic access control frameworks, from which we reuse the decision and enforcement concepts resulting in the three entities describes below:

- **Mobility Information Points (MInP):** The entity that stores information that is pertinent to the mobility process. It stores domain related information depending on the level it operates. These entities can be distributed across the network, targeting several, already mentioned, IdM specific functional boxes, as well as user devices, for user generated information. This can be the attribute server, the identity aggregator or a new (distributed) component.
- **Mobility Decision Point (MDP):** This is the entity that gathers both the static and dynamic information, executing the decision process controlling mobility. This entity can be distributed over the network where mobility information has relevance. A few examples are the access network, the local mobility domain, the global mobility domain, as well as the device for user centric information and mobility events.
- **Mobility Enforcement Point (MEP):** The mobility enforcement point should interact with the decision point, by sharing the abstract interface layer to that effectively bridges the decision into protocol operation. This should be mostly network entities, protocol specific, and the user devices, which will be part of the focus of the actual mobility process.

This approach enables us to model the entire mobility process, while reusing the entities and protocol which are already in place. Mobility is triggered by MEPs which use GAL to collect and transform network and user event into the correct mobility semantics. Mobility decision request is sent to MDP which based in information collected from MInP, decides if a mobility action may be performed. If the result is to perform a mobility action the inverse flow happens, after receiving the decision, from the MDP, GAL translates mobility semantics to specific mobility protocols and finally MEPs execute the necessary changes in the network to accomplish the mobility task.

5.1.1 Identity control plane for mobility

Given that the previously defined entities are generic, we can treat them as roles, which already deployed entities can perform. Based on the two critical roles (decision and enforcement), we divide the control plane into an information management component, and a policy execution component, assumed by each relevant entity on the network.

Most of the mobility decision process can be offloaded to network entities, residing in the control plane, which has access to cross-layer information. But, this is not the sole case where mobility decisions occur. When the local network or visited domain also controls the mobility within its networks, leading to network based mobility management, they are also mobility decision points. They do so by leaning upon network conditions which will not directly involve information residing on user's IdAgg, turning the local mobility management entities into a specialized MDP, which focus on specific aspects of the network. Further examining the proposed organization, the terminal too can be a mobility decision point, apply user policies and inter-provider policies that do not concern a single network provider or even Identity Provider. The control plane for mobility then results in a selection of decision and enforcement points scatter through the IdM system, the mobility system and the terminal (which is a part of both), as better understandable in Figure 4, where the defined elements interact through control primitives.

However, it should be noted that policy evaluation can be a daunting task, taking much longer than a few seconds. For particular cases, where movement decisions are time bound, there should be fallback mechanisms or deadlines for policy execution (similar to real time operating systems) assuring a valid response in useful time.

5.1.2 Mobility Actuation Plane

The actuation plane involves different entities, and implies the extended use of the GAL to transform the control plane decisions into actual protocol operation at the MEP. Figure 4 presents the mobility management backend and the terminal interacting through the defined abstractions. There are enforcement points in all entities involved in the mobility process (i.e. signalling and operations), that is the mobility management system in usage, and the terminals on the user end. The GAL will then transform these commands into the appropriate protocol actuators. Where required the protocol actuator passes the commands to the involved terminals.

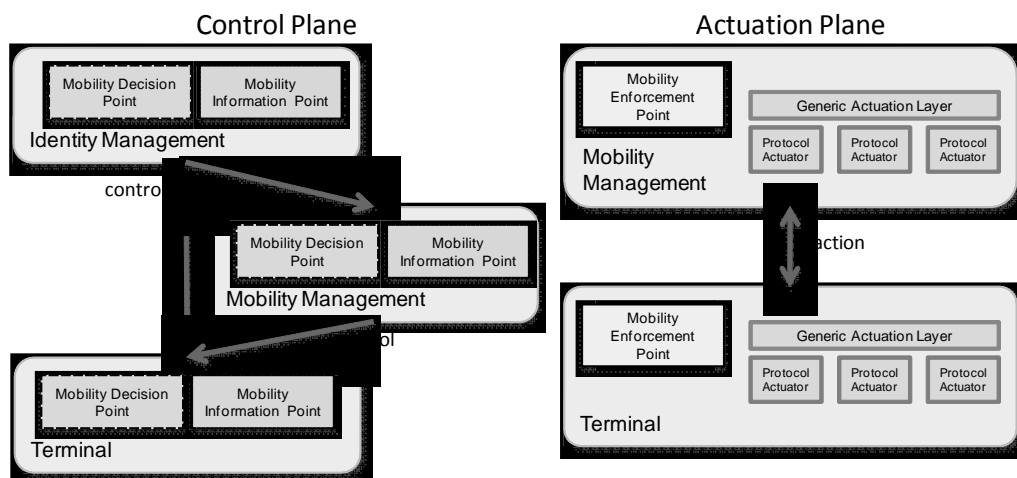


Figure 4 – Control (left) and Actuation (right) plane views

The protocol actuators, closely coupled to the MEP, provide the actual modular view that enables our proposed architecture to act as a control blanket over current and future

mobility solutions, protocol wise. Therefore, each protocol actuator should correspond to a different technology (e.g. MIPv6, HIP or SIP), with the benefits of reusing currently established protocols, and setting the performance similar to current systems. In fact, performance issues become orthogonal to the management system, given that the modular system cannot improve the performance of each individual building block.

5.2 – Architecture Instantiation

The described architecture is capable of modelling most mobility scenarios. However, for the SWIFT specific instantiation concrete decisions on the mobility process must be made. Following the reasoning in Sec. 5.1, we assign the designated roles to SWIFT entities and protocol entities, further clarifying the abstract definitions.

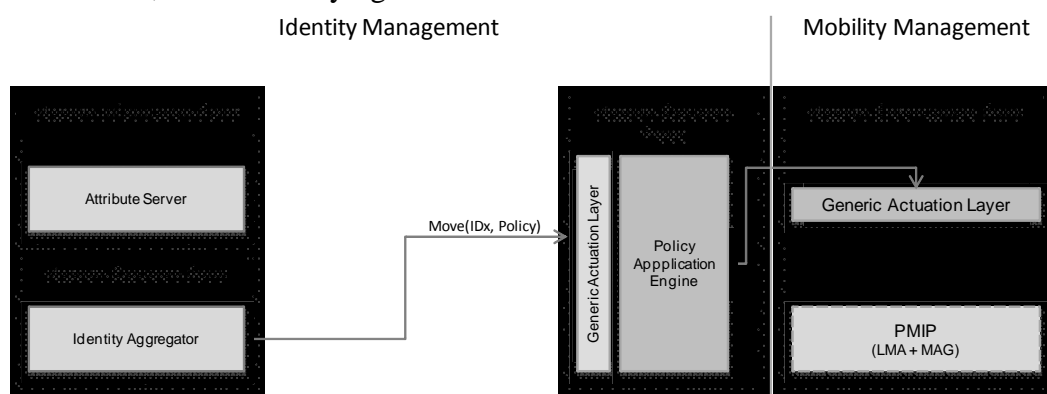


Figure 5 – Example Instantiation

The central element, in the scenario, is the Identity Aggregator, acting as the Mobility Decision Point, by controlling the mobility process, based user’s identity (preferences and contracts) and associated policies, and network status. Such information is collected from the Attribute Server, which takes on the role of MinP. The policy engine, part of the SWIFT architecture, is scattered between the MDP, which acts as the policy decision point, and the MEP, which acts as the Policy Enforcement Point (through the application engine), thus disseminating and enforcing mobility related decisions and policies.

For the mobility protocol, we employ PMIP [6] as the primary mapping protocol due to its network based approach for handling mobility, which allows outsourcing mobility decisions to the network. Therefore, both PMIP entities (the LMA and the MAG) compose a single protocol actuator connected to the MEP.

When mobility is triggered by PMIP, the LMA uses the GAL to convert the event into the correct semantics and to request a mobility decision to the IdAgg (acting as MDP). The IdAgg collects the necessary information (e.g. user attributes, network information or policies) from the AttS (acting as MinP). If the result of the information decision is to perform a mobility action, e.g. change point of attachment, provider, or session condition, then the IdAgg will format the resulting decision and distribute the appropriate decisions to achieve the desired state in the network, which will be processed at the MEP by the policy engine. The resulting actions will be sent to the correct GAL, where they will be transformed from the mobility semantic decision into the correct protocol action and towards the LMA/MAG. This process summarizes the nature of the mobility process in the architecture.

6. Conclusion

The example presented already allows us to see how the mobility semantic is used across different SWIFT elements, taking full advantage of the strong policy oriented

mechanisms scattered through the network. In this scenario, mobility is in fact a true distributed policy application, realized by the actuation layer which provides the movement primitives. It's also clear that the hierarchical policy approach provides great flexibility when it comes to mobility management. However, the presented architecture should take into account the possible overhead of such distributed functions, and act accordingly to comply with mobility (time) requirements, especially considering that individual protocol performance remains unchanged by this approach. The overall performance of the actuation layer depends on the individual modules (protocols), which is as an orthogonal issue.

But, as the semantic definitions evolve, the mappings between the generic entities and the real entities will start to become more apparent. In future iterations of the architecture the generic entities, or roles, should be replaced entirely by SWIFT entities, and the entire mobility process should be fixed. This means that in spite of having a generic enough architecture, for instantiation purposes several roles must be clearly defined within each realization of the generic architecture, such as at which levels are the decision outsourced by the terminal, and how does the local network contribute to those decisions while preserving the user's privacy. Currently under definition are the functional interfaces, and concrete messages that permit such interactions within the mobility framework.

References

- [1] FP7 IST SWIFT - Secure Widespread Identity in Federated Telecommunications. <http://www.ist-swift.eu>.
- [2] Matos, A. (ed.): Gap Analysis and Architecture Requirements, SWIFT Deliverable 202, 2008.
- [3] Girao, J. (ed.): First Draft of the Identity-driven Architecture and Identity Framework, SWIFT Deliverable 203, 2008.
- [4] A. Sarma, A. Matos, J. Girão, R. Aguiar, "Virtual Identity Framework for Telecom Infrastructures", Springer Wireless Personal Communications, Special Issue on "International Mobile Telecommunications", 2008.
- [5] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004
- [6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6 (PMIPv6)", RFC 5213, August 2008
- [7] R. Moskowitz, P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006
- [8] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002
- [9] M. Lischka et. al: Deductive Policies with XACML. 2009 ACM Workshop on Secure Web Services, Chicago, Illinois, USA, November 2009
- [10] Azevedo, R. (ed.), SWIFT Mobility Architecture, SWIFT Deliverable 403, August 2009
- [11] J. Manner, M. Kojo (editors), "Mobility related terminology", RFC 3753, IETF Informational RFC, June 2004
- [12] M. Almeida, et al. "Mobility with QoS Support for Multi-Interface Terminals: Combined User and Network Approach", Proc. 2007 Proc. IEEE Symposium on Computers and Communications (ISCC'07), Aveiro, Portugal, Jul 2007.
- [13] A. Matos and R. Aguiar, "Mobility aware paths: The identity connection", in Special Sessions of the 11th International Symposium on Wireless Personal Multimedia Communications, (Lapland, Finland), WPMC '08, September 2008. ISSN 1883-1192.
- [14] IEEE Std 802.21-2008, "IEEE Standard for Local and metropolitan area networks - Part 21: Media Independent Handover", IEEE, Jan. 21 2009.
- [15] M. Barisch, A. Matos, "Integrating User Identity Management Systems with the Host Identity Protocol", International Symposium on Computers and Communication 2009, Tunisia.
- [16] OASIS eXtensible Access Control Markup Language (XACML) Version 2.0, February 2005, OASIS Standard
- [17] Gabriel López, Cánovas, Antonio F. Gómez-Skarmeta, Joao Girao, "A SWIFT Take on Identity Management," Computer, vol. 42, no. 5, pp. 58-65, May 2009, doi:10.1109/MC.2009.141