Identity Management in Federated Telecommunications Systems

Rui L. Aguiar
Institute of Telecommunications
University of Aveiro
Portugal
ruilaa@det.ua.pt

Christian Hauser
Institute of Communication Networks and Computer Engineering
University of Stuttgart
Germany
hauser@ikr.uni-stuttgart.de

Jürgen Jähnert
Computing Center
University of Stuttgart
Germany
jaehnert@rus.uni-stuttgart.de

Antonio F. G. Skarmeta
Department of Information and Communications Engineering
University of Murcia
Spain
skarmeta@dif.um.es

Abstract

Future telecommunications systems will introduce a multitude of partly small network and/or service providers. For those providers to interwork, a coordinated organizational cooperation and standardization of the technology are crucial. One important aspect of standardization is about handling user identities. In the Daidalos architecture, users and user groups are considered equally. As there will be a multitude of identities per user, identity management is of utmost importance in modern telecommunications systems. Standardization in this area should comprise formats of user attributes of an identity representation, identity information exchange protocols and security standards for handling identity data.

1 Introduction

Telecommunications networks undergo drastic changes in their underlying paradigms in these days. One of the most important ones is that the infrastructures will undergo quicker development and innovation cycles. This is driven by a shorter time to market of new services and a quicker deployment of supporting functions. This need for faster evolution brings up smaller, specialized service providers and network operators, who don't have to provide for the full set of functionality ranging from the access networks over consumer services up to a full billing infrastructure.

More providers will boost the importance of cooperation among providers and federation in the sense of several providers working together to jointly provide a service. This calls for coordinated terms of cooperation from an organizational perspective and standardization from a technical perspective. One important aspect of standardization – which is often neglected as it is not a directly functional aspect – is how the providers talk about the user they are serving jointly.

Generally, it can be stated that this aspect of the user profile grows in importance in future systems as compared to today's systems. This is first of all due to the aspect of user-centric context-awareness. This means that the system handles user-related context in order to react best in every situation according to the user's needs. Another trend supporting this vision is the growing importance of user-related regulation. This is present in both directions – in the style of legal interception as well as in the style of data protection rules.

Usually, a user has many identities in the technical system. This happens for two reasons: First of all, a user uses different services and networks, which issue identities and secondly, users split up their data trace left in the system by using multiple identities. These identities must be managed by the system. The term identity management often raises confusion as it has two related but distinguishable aspects. First of all, the system itself must cope with multiple identities and at least to a certain degree handle those identities jointly in order to provide for single sign-on or at least one-stop billing. The other aspect is user support in choosing always the best suitable identity. This is a complicated task, which cannot be undertaken by users alone. In Daidalos – a European project of the 6th framework programme conducting research about future telecommunications systems providing a platform for pervasive services – both aspects of identity management play important roles.

In section 2, we will present federation needs in telecommunications systems in general. After that, section 3 will give a short introduction to the Daidalos architecture. Section 4 details on identity aspects in the architecture and the needs for standardization in the identity sector before section 5 concludes.

2 Federation in Telecommunications Systems

Federation describes the concept on how different actors in an overall service provisioning environment interact in order to provide a composed service to their customer. Most typically, federation is a concept, which is implemented between different administrative players in a future telecommunications market. Such a federation between administrative domains implies the setup of a trusted relationship and the sharing of various identities, attributes, and profiles with the purpose, to

enrich the service provisioning concept to the user and to bind the user to the own services which are typically more attractive for the users after federation.

Generally, there are several of federation, which range from a fully federated situation where the federated business entities exchange almost all desired details. In the other extreme situation, no information is exchanged at all. Between these two extreme positions, there is a wide range of flavours of federation possible, which could be individually defined by the two involved administrative business entities.

There are further aspects to be considered when talking about federation. One aspect is the way of establishment of the federation relation itself, which can be static or negotiated dynamically on request. Further, federation can be established between two service providers, which provide to the user the same service, but by implementing federation a larger regional area is covered. This case of federation is called horizontal federation. In a vertical federation scenario business entities at different points within the value chain cooperate in order to enrich the service a user can get at a topological location by an added value offered by the federated service provider.

From a technological point of view, in the Internet – and within Daidalos – the relevant standardization activities are the IETF AAA, which provide somehow the communication infrastructure dedicated to the information exchange required to establish and release the federations.

3 Daidalos Architecture

The Daidalos architecture is based on four fundamental assumptions, based on operator-driven visions of next generation telecommunications:

1. **All design will ultimately be made around the user, simplifying his needs.** The user-centric design is particularly important to offer complex technology for the increasingly technology-agnostic users. Context takes here a key part, as the key concept that will lead to service personalization. Identification is also a major aspect: “Who is the user?” in a particular situation, will be essential to understand what is the relevant context.
2. **The future telecom operator runs and operates enabling services for a huge number of users and service providers.** In a world where users are empowered (in all aspects of their life), the telecom operator is responsible for providing the necessary communication services. It takes the role of a service provider and offers services to its customers. Thus, platforms for securely handling context processing (per user) in scalable way are a challenge.
3. **Users have the final control of their communication needs.** Users must be free to change between service providers and between technologies, at their own will and risk. This concept, however, implies that the service provisioning environment cannot be considered to be simply a layer on the provider layer. The user may personalize both his environment and the actions to perform upon context changes.
4. **Services could be provided by multiple providers.** Service providers are not expected to be in specific locations in the network but are expected to have specific business relationships with the operator, identifying the objective contractual relationship expected between them. The fact that several major players will continue to exist in the future (e.g., mobile telephony operator, TV broadcaster), though potentially with different roles, increases the complexity of defining a network architecture. This assumption brings several added layers to the problem: trust relationships will be required not only between the user and the service provider, both also between service providers, and different levels of information exchange will exist between different service providers, addressing different users. Identification, context and trust management are here intrinsically intertwined.

Figure 1 presents a possible view of the architecture, where its more relevant entities are identified. In the figure, one can identify the “access networks”, the “multiservice IP network” already associated with the “service environment” (the central administrative cloud, with the Service Provisioning Platform). In reality, for a telecom operator, some of its key services are precisely the basic communication facilities. The figure further identifies a large set of technologies supported in the project, from unicast technologies (DVB), to traditional wireless technologies (TD-CDMA, WiFi, WiMax), but also encompassing self-organized environments (both sensor and ad-hoc nodes), and mobile networks.

Daidalos focuses on feasibility to provide the communications technologies to support all these information transport models, with an unknown number of business parties. In fact, it is to be expected that different types of access, potentially under the ownership of different entities, will be (nearly) always available.

Daidalos divides the overall next-generation network into administrative domains that can cooperate when there is a service level agreement and a trust relationship between them. Daidalos defines an inter-operator architecture termed Service Provisioning Platform (SPP) that allows the different components in the various domains to interact. The SPP is comprised of services for QoS, Network Management, Network Monitoring, Security, Authentication, Authorization, Accounting, Auditing, Charging (A4C), and Multimedia and provides the tools for creating services and applications on top of integrated heterogeneous access networks. In the access network, Daidalos separates the activities into 6 different modules: Terminal Mobility (TM), Moving Networks Integration (MNI), Ad-hoc Integration (AHOI), Quality of Service

(QoS), Security (Sec) and Broadcast (BC). These modules are deployed on various physical entities, such as mobile terminals, access routers, access points, home agents, or QoS Brokers.

Inter-operator modules are mostly deployed on border routers and the SPP. The exact deployment strongly depends on the business scenario (the architecture instantiation). Thus, modules will be placed inside different servers, in different administrative domains as a function of the overall interaction of the business scenario.

Daidalos further takes a service-oriented approach to pervasive computing. The pervasive support architecture consists of two parts: a service management infrastructure and an infrastructure running user devices. The former provides ubiquitous access to services. The functional entities termed PSM (Pervasive Service Management) run on top of the PSPP (Pervasive Service Provisioning Platform). The PSM discovers services available to a user at any time, composes atomic services into composed pervasive services, and provides runtime mechanisms to support the usage of the best available devices for each pervasive service. A part of the service management infrastructure includes the basic infrastructure for using multiple virtual identities for preserving user privacy. The user device infrastructure aims at supporting context-aware interaction with pervasive services. This infrastructure includes the functional entities Context Management (CM), Personalisation (P), and context-aware VID (virtual ID) management. This architecture provides for a set of enabling services to provide the best user quality.

Context aspects are an essential part inside Daidalos, and in fact are reinterpreted along the multiple layers. The pervasive support environment, takes in information coming from different layers (network availability, signal strength, user preferences), and processes it at different levels, in order to provide the best communications experience at each time. This is mediated by the Context and Personalization managers.

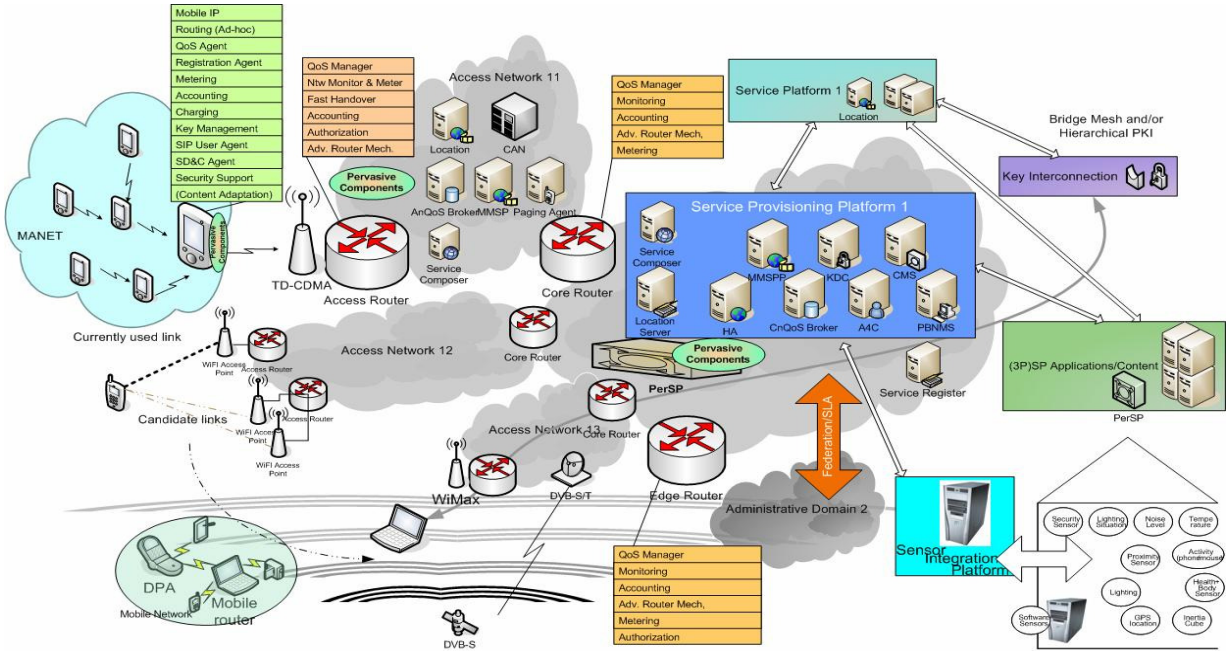

Figure 1 Daidalos Architecture

4 User Identities in the Architecture

As introduced above, operator scale networks will include in the future various relations between different entities, such as service providers, network operators or service consumers. Identity management solutions of multiple contracts with their corresponding consumer identities and its interrelation with service authorization associated require a significant work in the standardization in order to allow the interoperability and the seamless access. Additionally, new focus on aspects like privacy of the user on the one hand and on the other hand the integration of new entities, such as new administrative domains or value added service operators, has to be kept as simple as possible, still providing security among the participating entities.

The representation of the users in a telecommunications system is of great importance. This is not only due to the fact that service consumptions must be charged to a user, but also for the system to behave best and adapted for each user. Therefore, the central thing when talking about user representations is the so-called *user profile*. It contains all data that the system needs to know about the user.

Typically, this user profile contains first of all authorization information, i.e., which services/functions of the system the user is allowed to use. It is also wide-spread to include personalization information, i.e., policies to express how a specific service is to appear towards the respective user. With the advent of context-aware and pervasive services, there is virtually arbitrary information possible to be stored about the user, e.g., his location or the temperature around his place.

It is likely, that there will be a set of information for virtually each service, in the future. Thus, it does not make sense, to store all this information about a user in a common place, but many services will hold their relevant part of the user profile instead. On the other hand, there will be information of relevance to many services, which will most likely be held centrally. Moreover, it can be that dynamic parts need a different storage than rather static attributes of the profile. Therefore, Daidalos chooses an approach of a virtual user profile that is physically distributed among many local databases in different federated operators and/or service providers. This is depicted in Figure 2. It shows three parts of the profile at two operators and at a service provider. This builds up logically the overall profile known about the user. As examples for entries serve personalization policies, authorization policies, handles to an account to be charged to or context information.

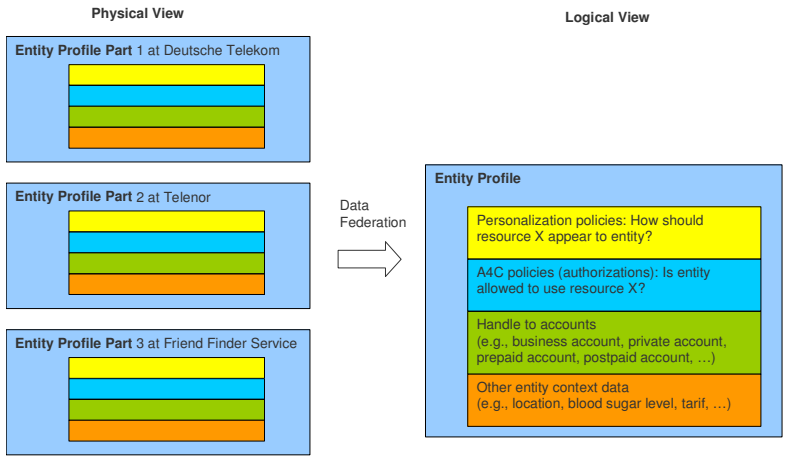

Figure 2 Logical entity profile and its physical parts

In a telecommunications system, groups play growing role. This is not only due to the growing importance of community services, but also a result from the integration of broadcast networks and services, which is often referred by the term "triple play". The system must know about groups the same things like about ordinary single users, i.e., authorization information, personalization policies, context information, etc. Therefore, Daidalos does not distinguish between a single user and a group of users. Therefore, Figure 2 shows *entity profiles*, with an entity being a single user or a group of users. For this vision to come true, the underlying communication system must be adapted, which will be done in Daidalos.

In context-aware systems, privacy plays a central role. A common approach is to allow users to act under multiple virtual identities. Thus, it is possible to reveal only the amount of information to a service, which is really necessary for a specific service provision. On the other hand, the user can use many services, without leaving a too detailed data trace by linking all information that is known at those services. This results in the following scenario of Figure 3. On the left hand side, the different parts of the entity's profile *(EPPs)* can be seen, which result in the overall entity profile in the middle. On the right hand side, there are three *entity profile views (EPVs*). In each view, there are pieces of the entity's profile, which can physically come from profile parts at different providers. Such an entity profile view is a virtual identity.

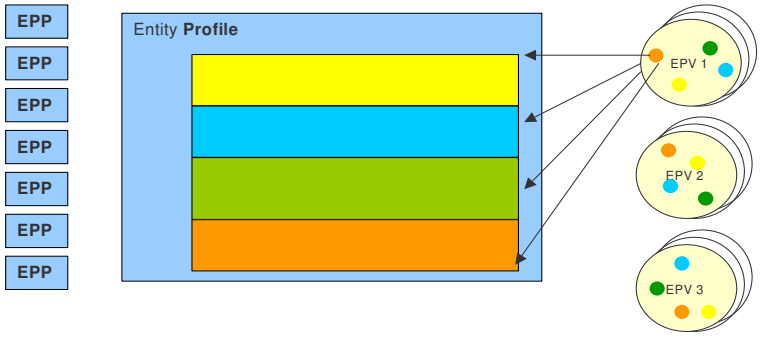

Figure 3 Entity profile views as partial view on the entity profile

Of course, the approach of multiple virtual identities can only be successful, if all parts of the system support it and don't impose the usage of identifying information, by which different virtual identities of a user could be linked. In a first place, this requires a new communications infrastructure, but it also requires the use of specially designed identifiers for the authentication/authorization/accounting/auditing/charging (A4C) infrastructure. In Daidalos I, an approach was chosen that gives differently looking identifiers for all virtual identities, which can only be linked to a single user account by the home operator, which is in charge of accounting and billing [1]. This approach might be changed in Daidalos II, the second phase of the project.

There exist different standardization efforts for federated scenarios. Two of them that have a significant support are the authorization frameworks of Shibboleth [2] and Liberty ID-WSF [3]. Both define a federated identity management with assertion of user rights within a community of trusted partners based on SAML [4]. User's security and privacy are

important in both architectures, but they are more related to application services or either web services. Although some modifications could be done to them, especially Shibboleth, we understand that Daidalos although reusing some of the concepts introduced by them, aim to go further in the ideas of virtual identities not only for privacy issues but also to support dynamic services provisioning, where network services are just of special interest for a telecom-oriented project like ours.

In a federated environment, in which several operators and/or service providers work together in order to provide a service to the user, it must be assured that those operators understand each other with respect to the entity profile data to be exchanged and managed in general. Moreover, it might make sense to streamline policies for the handling of entity profile parts. As the exchange of entity profile data is highly sensitive with respect to confidentiality but also integrity, strong security standards are needed for the protection of this subsystem.

During standardization in the identity area, the peculiarities of this topic must be taken into account. As we showed in this section above, identities must not always be restricted to user identities but can and most likely will in near future also stretch on groups of users. As shown in the architecture section, it must also be possible to identify service providers and operators as well as the services and networks, they are offering.

In order for federated service providers to jointly serve their customers, they first of all need to have a common notion of the entity they are referring to. That starts by a standardized structure of identifiers and other attributes of the identities. There is a broad range of attributes from authentication material over network related parameters up to service related parameters. An option is to standardize a framework and to leave the details up to different specialized standardization bodies for the different areas. If there will not be a common world-wide standardization but rather several ones, mapping functions between those standards must be agreed in order to allow operators following different standards to federate. Next to the structure of this identity data, the semantics are also important, calling for some standardized ontology.

Knowing, what to exchange and how to interpret this data is not sufficient. Also the terms of the exchange process have to be agreed on calling for standardized protocols – for requests and for updates. From the security perspective, the pure exchange protocol is still not sufficient, but a complete security framework is necessary standardizing, e.g., access control and other protection measures for the management and handling of this sensitive identity data.

As identity data often ranges into very personal areas of the users' lives and on the other hand this often is a valuable business secret of service providers, the exchange of this data calls for external regulation. This is for sure in the direction of data protection rules restraining the exchange but it might also be the enforcement of the exchange of certain attributes in order not to restrict competitors from entering the market. It might also be that laws will (and partly already do so) require that all data pertaining to a user have to be made available to this user. For a federated telecommunications system of international scale, coherence of laws in this area is an important base, which is not given to date.

5 Conclusions

Future networks pose new challenges to Service Operators, Service Provisioning Platform Operators and Access Network Operators by introducing multiple administrative domains and federations, as well as by introducing users having multiple identities and maintaining multiple sessions on different devices. The main advantages of introducing a standardized infrastructure for identity management are:

- Standardized exchange of security information between different administrative domains,
- seamless terminal and session mobility across different domains,
- federation of services and third party providers to allow a broader scope of service to end user,
- easy integration of independent services into the security and identity infrastructure.

In distributed networks users have multiple contracts with different providers, using various identities. Hence, a very flexible identity management has to be provided covering different levels of security and privacy within future networks. A user can choose, which identity he wants to use to authenticate and register for value added services.

6 References

[1] B. Weyl, P. Brandao, A. F. Gomez Skarmeta, R. M. Lopez, P. Mishra, C. Hauser, H. Ziemek, "Protecting Privacy of Identities in Federated Operator Environments", IST- 14th Wireless Mobile Summit 2005.

[2] http://shibboleth.internet2.edu.

[3] http://www.projectliberty.org.

[4] Ph. Hallam-Baker, E. Maler (eds.), "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", OASIS Standard, Version 1.1, September 2nd 2003, http://www.oasis-open.org.