FIDIS

Future of Identity in the Information Society

Title:	"D11.11: Next Generation Networks"
Author:	WP11
Editors:	André Deuker (JWG, Germany)
	Denis Royer (JWG, Germany)
Reviewers:	Kai Rannenberg (JWG, Germany)
Identifier:	D11.11
Type:	Deliverable
Version:	0.80
Date:	Sunday, 23 August 2009
Status:	Final
Class:	Public
File:	fidis-wp11-del11 11 Next_Generation_Networks.final.doc

Summary

Next Generation Networks are confronted with many expectations, such as integrating the Internet with its plethora of services with the reliability of the originally telephone oriented telecommunications networks, including the provisions for reliable mobile communications. On top of this comes the integration of real-time media services such as radio and television is on the agenda adding to the complexity of the endeavour. For these complex NGN services and the underlying infrastructures reliable management of personal data is fundamental.

This deliverable gives an insight to typical NGN services and their relation to individuals, their data, and their identification. It shows, that compared to previous identity dependant services and applications, in the NGN even more and additional types of user information are collected and processed, and gives examples of corresponding opportunities, such as better "Quality of Experience", and risks, such as a the vanishing of opportunities for anonymous media consumption. Consequently identity management needs to be multilaterally secure, while it gets even harder for users to manage their increasingly complex profiles. This raises the need for identity management strategies, methods and tools supporting users and for NGN service providers supporting these user-centric strategies, methods and tools. Given the complexity of the NGN sphere major standardisation challenges occur.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieked Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	28.05.2009	• Initial release (Denis Royer)
0.2	29.05.2009	• Reworking of initial contributions (especially JWG)
0.3	16.06.2009	• TUB Contribution - Draft Fikret Sivrikaya (TUB), Seyit Ahmet Camtepe (TUB)
0.4	25.06.2009	• TUD Contribution – Draft
0.5	26.06.2009	• Editing Intro & Conclusion (JWG)
0.6	27.06.2009	• Added contribution by VUB (Els Soenens)
0.7	22.08.2009	• Completion of the Introduction, Revision / Update of the Conclusion, Added Executive Summary - Kai Rannenberg, André Deuker (JWG)
0.8	23.08.2009	• Finalisation of the Deliverable – André Deuker (JWG)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	André Deuker (JWG)
2 (Introduction)	André Deuker (JWG), Denis Royer (JWG),
3 (Scenarios)	Seyit Ahmet Camtepe (TUB), André Deuker (JWG), Martin Meints (ICPP), Piotr Micinski (JWG), Denis Royer (JWG), Fikret Sivrikaya (TUB)
4 (Quality of Experience and User-Centricity in NGNs)	Seyit Ahmet Camtepe (TUB), Fikret Sivrikaya (TUB)
5 (NGN Management and Semantics)	Seyit Ahmet Camtepe (TUB), Fikret Sivrikaya (TUB)
6 (NGN Services - Case Study: Semantic IPTV)	Seyit Ahmet Camtepe (TUB), Fikret Sivrikaya (TUB)
7 (Privacy Threats in NGN)	Stefan Berthold (TUD), Rainer Böhme (TUD), Stefanie Pötzsch (TUD)
8 (Conclusion)	Kai Rannenberg (JWG)

Table of Contents

1 Executive Summary

Next Generation Networks (NGNs) are confronted with many expectations, such as integrating the Internet with its plethora of services with the reliability of the originally telephone oriented telecommunications networks, including the provisions for reliable mobile communications. On top of this the integration of real-time media services such as radio and television is on the agenda adding to the complexity of the endeavour.

Already before the advent of NGNs the goal of enabling user mobility was one of the major endeavours of new services and technologies. However it is still an important factor for the development of new architectures, as mobile communication has still not reached the standard of fixed-line communication (e.g. with regard to bandwidth) while new mobile services, such as mobile social networks and mobile and ubiquitous commerce show the importance to have information and communication services enabled for mobile usage.

At the same time it can be observed that the market segments of telecommunications and audiovisual media (especially entertainment), are converging and gradually melting together, as more and more service providers are basing their business models on Triple and Quad Play services. This includes cable television and high-speed Internet access as well as landline and mobile telephony. This, together with the technical evolvement of mobile networks, creates the opportunity for the provision of additional (NGN) services.

Interaction with social networks can take place by using a (smart) phone, one's vital signs can be analysed by healthcare professionals while one is out shopping (m-health), one can buy the food needed for dinner, while using the bus home; just to mention a few examples. Such services have the potential to create additional value for users, as they contain services tailored towards the needs of the individual recipient. This includes personalised information (including news and events tickers, traffic announcements, disaster warning), personalised offers from advertisers, mobile payment capability, or home automation solutions. For these complex services and the underlying infrastructures reliable management of personal data is fundamental.

This deliverable thematically introduces into NGNs by providing a set of typical scenarios reflecting important aspects and characteristics of NGN services. Based on this it focusses on the concept of "Quality of Experience" – the end-to-end service quality from the perspective of a user. This is an essential aspect especially when personalised services based on different sources of users' identity are brought into place. As a consequence network management and semantics get ever more important. Referring to the presented scenarios and a case study on a Semantic IPTV multimedia platform, the deliverable provides a section on privacy risks in NGNs, which identifies, describes, and discusses risks based on the exemplary case of IPTV mass media.

The analysis shows, that compared to previous identity dependant services and applications, in the NGN even more and additional types of user information are collected and processed. An example of a corresponding opportunity is a better "Quality of Experience" based on fast and robust access to personal data; an example for a risk is the vanishing of opportunities for anonymous media consumption.

Consequently identity management needs to be multilaterally secure, allowing appropriate access user to data while enabling privacy of users (e.g. anonymity) and effective abuse prevention. At the same time it gets even harder for users to manage their increasingly complex user profiles.

One conclusion is the need for identity management strategies, methods and tools supporting users and for NGN service providers supporting these user-centric strategies, methods and tools. Given the complexity of the NGN sphere the corresponding requirements need to be implemented in NGN standardisation. This is an additional challenge to standardisation in the general area of Identity Management, as NGN standardisation takes place in the ITU-T Study Group 13 "Future networks including mobile and NGN" while the Lead Study Group on Identity Management in ITU-T is Study Group 17 "Security".

2 Introduction

Mobility is one of the major goals of new services and technologies. New mobile services, mobile social networks, mobile and ubiquitous commerce, are parts of the tendency to push information and communication technologies into the mobile world. Thereby, software developers and product consumers have the opportunity to enjoy services as if they were at home. For example, social networks can be interacted with by using a (smart) phone[4], one's vital signs can be analysed by healthcare professionals while one is out shopping (m-health), one can buy the food needed for dinner, while using the bus home etc. Similarly, the re-definition of the concept domestication puts the attention to the way people get used to and use ICT products:

> *"…the word domestication does not mean 'inside the house'; public space could be analysed as a counterpart to regulation of ICT in the home, in more subtle way"* (Haddon, 2003)

However, in the recent years another highly remarkable trend could be observed in telecommunication and audiovisual entertainment market segments. Both segments have been converging and gradually melting together, as more and more service providers have begun basing their business models on Triple and Quad Play services, including cable television, high-speed Internet access, as well as landline and mobile telephony. The convergence of business models leads to a similar development on the level of infrastructure. Formerly separate networks are being connected to create a global Next Generation Network (NGN), in which services are provided on a data packet basis. One advantage of this development is the ability to use the bandwidth and infrastructure efficiently, which creates the opportunity for the provision of additional services. Such services have the potential to create additional value for users, as they can contain information (including news and events tickers, traffic announcements, disaster warning), personalised offers from advertisers, mobile payment capability, home automation solutions, etc.

The field of mobile services in NGN is somewhat special. As Srirama et al. state (Srirama , 2006), there are some "characteristics unique to the mobile paradigm, the increased complexity of emerging handheld devices, the greater sensitivity to security and load related problems in wireless infrastructure and increased complexities of scale." Due to these characteristics the development of mobile services is time consuming and expensive. From an economical perspective one can see that revenues are needed and these seem to be based on processing location data. However, a part of user's identity necessarily has to be divulged for every service. This applies especially for context aware services, in case of which a significantly more detailed input is required, as they are essentially based on a relatively broad choice of user information. Depending on the type of provided service, it can include current geographical location, personal preferences, possible activities, bank account, place of residence, and many more.

[4] For details on this cf. FIDIS deliverable D11.8 on Mobile Communities.

From a user's perspective applications and services will be the interface to judge on the quality, usage and security of next generation mobile networks. Therefore this deliverable will focus particularly on selected services and applications that are prone to simplify and enhance everyday tasks, and allow implementing identity management models that reduce the risk of abuse to a minimum.

The remainder of this report is organised as follows: The deliverable gives a thematic introduction into Next Generation Networks in **Chapter 3** by providing a set of scenarios that are considered to reflect important aspects and characteristics of these networks. The scenarios are based on the authors' experiences on development patterns of predecessor technologies and substantiated by insights from literature and previous FIDIS deliverables.

NGNs will be "meta networks" providing a multitude of services over a common infrastructure, replacing the individual service-specific independent networks. The infrastructure used in delivering a service to the user will typically be owned and maintained by different providers. The user is expected to have an increased number of options with increased dynamism for choosing among connection and service providers.

In such an environment, the end-to-end service quality observed by the user. This, termed as "Quality of Experience", is described and discussed in **Chapter 4**.

One of the major challenges in NGNs lies in the integration, analysis, and usage of vast amount of management, and management-relevant (identity) information contained in the heterogeneous environment that the all-IP aspect of the NGN brings along. **Chapter 5** on NGN management and semantics stresses on the goal to let the network nodes utilize the knowledge about themselves and their working environment for the more efficient functioning of the service provisioning that they are involved with.

In **Chapter 6** a case study on Semantic IPTV is presented to demonstrate and underline these insights that is, together with the scenario on "Semantic IPTV" in Section 3.5, the baseline for the analysis of NGN privacy threats in the subsequent chapter.

Within **Chapter 7** emerging challenges for privacy and data protection that have been presented in the course of the previous chapters are discussed. The analysis especially focuses on the case of personalised media over converged delivery channels, but similar threats also emerge in the other scenarios presented.

Chapter 8 of the deliverable sums up insights and implications of the deliverable and puts emphasis on solution approaches for NGN identifiers as well as on requirements on the parties involved in NGN services raising the issue of related standardisation.

3 Scenarios

In this chapter five scenarios describe typical usages of NGN services and properties:

1) Intelligent Home Solutions;
2) Public Network Computing;
3) Marketing;
4) Semantic IPTV.

3.1 Intelligent Home Solutions

One of the most interesting and promising NGN-scenarios is the development of intelligent home solutions. NGN will soon allow connecting virtually every house appliance and entertainment device into one network, accessible not only from inside the house, but also from practically any point on the globe. The possibilities that arise this way are broad:

- A house owner can turn up heating or air conditioning upon ending his work, so that the temperature is at comfortable level as he reaches home.
- While on vacation, he can turn the lights or other house appliances on and off to simulate presence of persons in the building. Further security can be achieved by checking if all potentially dangerous appliances have been switched off and that the alarm system has not been set off.
- When teenage children are alone at home, parents can have full control, ensuring that their offspring does not access forbidden content, either in television or with a computer, does not bring themselves or the house in danger, stay out for too long, etc.
- With a front door camera, it is also possible to monitor if there were any missed visitors.

All the described and numerous further intelligent home solutions can be extended with the context sensitivity and identity management factors, bringing them to a further level of user comfort and safety from abuse.

A service provider, preferably in cooperation with a security agency, could allow users to set up a profile defining the behaviour of their house in various situations. For example, a location profile of the user could be created to conclude his activities from daily movements. When the system recognises that a user is leaving of his office as the end of work and return home, adequate light and heating configuration will then be initiated automatically.

Similar mechanisms can activate the vacation-mode. After detecting that user movements deviate from his daily routine and that his distance from home is substantial, alarm system will be set to a higher alert level, the security agency notified of his absence to monitor the house more carefully, and lights, as well as appliances turned on and off to simulate presence in the house. The simulation is, at best, based on true activities of the house owner, but slightly different every day, so that the potential burglars do not recognize it as a pre-recorded program. Suspicious activities inside or around the house might be forwarded to the security agency responsible for monitoring the house.

Collecting input from entire neighbourhoods would help the agency to become an overview of the situation in particular sectors. It is also thinkable, that several agencies are involved in protecting a single neighbourhood. This would require a shared database, which gathers all

relevant information about a neighbourhood and make it accessible for every authorized member in order to better cooperate and protect the area. On the other hand, information contained in such databases would be very sensitive and dangerous in case of a leak. For this reason, it is vital to ensure proper restrictions in access to the data, as well as reliable identification and authentication of authorized persons. In worst case, someone intending to burgle houses in the area might receive a comprehensive list of which houses are most appropriate for this purpose, due to the absence of the owner and the estimated time of his return. Data sent to and received from the house owner by the intelligent home solutions provider should be handled in equally confidential manner. Failing to do so is a further threat to his security. What is more, it should be guaranteed that he is the only person to have access to the control panel of the house and change the settings of service. This would be a fairly easy task, provided that the control panel was only physically accessible and placed inside the house. However, in the discussed case, the panel should be electronically accessible from any access point of the NGN, including mobile ones. Therefore, reliable authentication procedures are vital.

3.2 Public Network Computing

Another promising scenario, where the implementation of identity management into the NGN becomes important, is the extension of Public Network Computing (PNC). According to CNN (Walton, 2006), the number of private and corporate websites on the Internet exceeded 100 million in 2006 and has been growing ever since. A substantial percentage of the sites is available online thank to provision of disk space and processing power within the concept of PNC. Further services that would not exist without its support include blogs, e-mail accounts, instant messengers, portals allowing users to share their media and other data with friends, and even diverse online communities that allow users to create their own profile to share with other visitors of the particular community's website.

The diffusion of most of these services is remarkable, in some cases almost reaching full market saturation (like in case of e-mail), while in numerous other cases it is constantly increasing. A significant number of providers offering PNC services bases their business models on generating revenues from advertising, thus being able to provide services to their end users free of charge. As a result, the already mentioned popularity of such services can be observed and the business model proves to be successful enough for many further companies to take it up.

The broad variety of services and providers allows to satisfy virtually every preference of the user. On the other hand, differences between competing services are often limited to graphics of the user interface and several minor features, not affecting the main functionality of the service. In effect, users with similar backgrounds are likely to choose different offers and an individual person might need to register with a number of online communities and instant messaging communicators in order to be in contact with all of his friends.

The problem of multiple accounts also occurs in case of e-mail. An average individual is provided with mailboxes by:

- Its employer,
- Educational institutions,
- Internet service providers,
- Online communities, and

- A choice of other service providers.

A further private e-mail account is not rare, maintained because of its unique features or an address that the user can relate to. Taking into consideration that the entity, which set up and hosts a particular e-mail account also communicates with the user over this channel, certain confusion is inevitable. Avoiding chaos is possible by forwarding messages from all accounts to one chosen account or using e-mail software, which allows retrieving messages from multiple accounts. However, using the capabilities of NGN and identity management, a more efficient solution is thinkable. A PNC service combining an e-mail client and account management tools would allow the users to receive e-mails, which are relevant at a particular moment. Unlike the traditional e-mail client software, the service would make the messages from every user account accessible from any device with network access.

The basic idea is uncomplicated and already implementable. Namely, all user's messages should be retrieved into one selected account, which might be one of user's already existing e-mail accounts or an external one, used for messages gathering only, and not as an independent e-mail account (i.e. without an assigned address). The retrieved messages would then be tagged or moved into different folders in order to make it retraceable, which account they came from. Moreover, additional software could scan their contents for particular phrases, which allow assuming the urgency of the analysed message, finding topics that can be interesting for the user, as well as eliminate spam. The true innovation of this service would however be the applying of user context data, supported by the opportunity of setting up his personal preferences, so that some messages are immediately sent to a predefined device (push service), whereas solely a notification about the arrival of others is sent. Messages with low urgency level can even be left without notification. As an example, while an individual is at work, his service might be set up to push messages concerning his project directly to him, notify him of other incoming business messages and ignore the private messages, except for the most urgent ones, e.g. including information about health condition of family members. In such services, a reliable context recognition engine is of exceptional importance, as it is vital to distinguish between, for instance, a business trip, where similar settings apply as on usual workdays, and vacations, where the very opposite is the case. Furthermore, an intuitive user interface should be created, which would allow adjusting all the settings, as well as read, delete and answer the e-mail messages.

A similar idea can enhance the interaction with online communities. The first and most important step would be to create a service, which would allow accessing the data of all the online communities the person is registered with, using a single logon. It should give the users the possibility to learn about the activities of their friends from various communities at a single glance, easing the bilateral communication and allowing them to stay up to date with each other's lives. Providing the service with context awareness, it would gain the capability of notifying the user of events that might interest him, and doing it at the right time. All the notifications could for example be set up to wait until the user finishes his work.

Further utilization of such two-step principle of service is possible in regard to instant messaging. Similar to the scenarios concentrating on e-mail and online communities, the idea is to enable the usage and management of multiple accounts with just a single logon and through a single interface, as well as forwarding messages and notifications to a user based on his context. The critical requirement on this PNC-service as a whole would be to support accounts from the three described scenarios and be expandable to easily include accounts not only from newly emerging online communities and instant messengers, but also accounts from other online services, such as Internet auction and shopping platforms, as well as

traditional services, like voicemail or fax. Such combination would make an excellent enhancement of unified messaging, mentioned in chapter 3.2.

Being able to carry out operations that include numerous accounts from different online services, using a single logon would definitely be convenient and save a significant amount of time, but there is another aspect of such service that needs to be taken into consideration. As it is expected to access a number of external accounts without the requirement that the user signs on to every one of them separately, the relevant login data, including passwords, has to be stored on the servers of the service provider. In this case, the service provider needs to be a trusted entity that will not sell or abuse the fragile data. What is more a high security level needs to be guaranteed, so that the data is safe from theft and manipulation.

3.3 Marketing

Identity management and context sensitivity are bound to have a deciding influence on the future of marketing. Knowing where an individual is, what he is doing, what his preferences are, and being able to combine this information with the current time and data from geo information systems, would enable the advertiser in possession of such information to promote exactly the products the individual is most likely to buy. In contrary to traditional advertising, including printed media, radio and television, such targeted approach would have a considerably higher success rate. The advertiser would not have to pay for contacting millions of individuals who are distant from considering buying a specific product.

A problem might arise while mining for the relevant data. Individuals might be reluctant to reveal their context information to advertising agencies. However, a service can be offered that will provide utility to the consumers, for which they possibly will be prepared to exchange some of their context data. A mobile extension of price comparison engines can serve as an excellent example of such service. Presently, it is possible to access a basic version of the discussed engine via a mobile telephone, while shopping in a department store, to compare the price of a product of interest with the offers in online shops. Augmenting the service with the capability to retrieve and process user's location, the outcome of a price query could be enriched with offers from other traditional shops, which are within a defined distance from the user's position. At this point, revenues can be generated on the pay-per-click principle. The service provider would charge the shops an adequate fee in the moment that user is entering the shop's site, in case of online shops, and in case of traditional shops – while accessing their address data or using this data in a routing service. For better control of the latter scenario, a direct link to a cooperating routing services provider might be enclosed. Depending on the cooperation conditions, additional revenue can be generated at this point. The most lucrative option would however be to offer the placement of hyperlinks to participating shops on top of the results list in exchange for considerably higher pay-per-click rates. Such revenue model has proven to be exceptionally successful in case of Internet search engines.

There are further extensions, which are likely to contribute to the desirability and successfulness of the discussed service. Firstly, barcode reading software can be used to make the user input faster and more comfortable. There is software available, which allows smartphones to scan and process data from special mobile barcodes. However, in this scenario a barcode reader is needed that would be able to work with traditional barcodes, present on the boxes of virtually every product, which might be interesting for a price comparison engine. What is more, such reader needs to be compatible with a wider range of mobile devices. Using the Java platform can serve as the right solution, additionally offering the

possibility to use the reader as an online application, without the need to install it on the user's device. Secondly, a profile of the price comparison user can be created to analyze what sort of products he is interested in. This information makes it possible to provide the user with targeted advertising, presenting him information about products he is likely to buy, true alternatives to his first choices, as well as shops where he can buy the products he is interested in. This way, prospective customers are more likely to respond to the advertising, thus making it an even more promising alternative to traditional media.

3.4 Semantic IPTV

Bob gets fascinated as he rethinks the development from black and white TV set to Semantic IPTV, which takes an important part in his daily life. With incredible bandwidth and mobility provided by underlying NGN, IPTV is not only for entertainment with its advanced functionalities such as Live TV, Video on Demand (VoD), Flashback, and Lean-Back-Mode; it also provides personal information management and advanced communication and sharing functionalities. Bob benefits and enjoys Personalised and Semantic Advertisement, TV Program overview (Electronic Program Guide – EPG, per day and per channel on the left side), and Favourites (Searched by left side VoD categories / tag view; stream displayed in the middle). Communication functionalities such as Instant Messaging (event box), User-Recommendation and Channel-Chat help Bob to share the joy with his family and close friends. Despite of all these functionalities, Semantic IPTV is incredibly usable:

- Bob logs in to his IPTV system.
- Bob views **live TV** (triggered by channel list).
- Bob views **live TV** (triggered by left side EPG view).
- After a while he opens the VoD view
- … and **searches** a Video (by tag cloud/text) and selects it (**VoD**).
- A short **personalized video advertisement** is shown before the stream starts.
- At the end of the video, the client automatically switches to **lean-back-mode**, to provide a continuous personalized mediastream. Here the lean-back-mode shows a football game in live TV.
- A goal is scored in the football game Bob is watching. Bob activates a **Flashback**, to keep the goal as a highlight. The flashback is added to his **EventBox**.
- In the background the flashback is delivered to Bob's buddies automatically, according to Bob's prior preference settings.
- Alice logs in.
- Whereupon Bob is informed via a notification.
- In Alice's EventBox all missed events are shown. Alice picks the Flashback Event of Bob to watch it. The video preview is shown.
- Being interested, Alice starts playing the item. Thereupon she sends Bob an **Instant Message** "thanks, very cool goal!"

- Alice adds the currently watched Bob's flashback item to her **Favourites**.
- Alice opens from left side favourites (VoD) view
- … and filters her favourites
- … then grabs from her favourites a different football goal video and sends it as a recommendation (**User-Recommendation**) to Bob.
- Alice selects the **Live TV view** where she chooses a live program (Series) and starts playing it.
- Bob receives a **notification** about this event.
- Alice joins to the **channel-chat** by clicking an icon in the Eventbox.
- In the channel chat there are already several messages, and adapting to the context an appropriate advertisement will be shown (**Semantic Advertisement**).
- In the channel-chat the user is notified about a previous program of the currently watched series. Alice is interested in and looks in the **catch-up archive** (EPG in the past) for this program (or she uses the **reference** given in the chat respectively).

In such a system, an enormous amount of personal information can be leaked and misused by malicious parties unless it is protected with appropriate Identity Management Systems.

4 Quality of Experience and User-Centricity in NGNs

Next generation networks will be "meta networks" providing a multitude of services over a common infrastructure, replacing the individual service-specific independent networks. The infrastructure used in delivering a service to the user will typically be owned and maintained by different providers. The user is expected to have an increased number of options with increased dynamism for choosing among connection and service providers.

In such an environment, the end-to-end service quality observed by the user, usually termed as the "quality of experience", will be a key measure in both users and providers' perspectives. On the other hand, user-subjective evaluation of "quality" requires users to express their preferences, priorities, usage context, etc. either explicitly or implicitly (as inferred by the system). This in turn creates a strong relation between **identity** and **usage characteristics**, which may increase the privacy concerns over identity.

This chapter elaborates the term *quality of experience*, its definition, and the models for its assessment in order to provide some technical insight on its possible connections with user's *identity*.

4.1 Quality of Experience / Quality of Service – The Terminology

QoE (Quality of Experience) mainly relates to the subjective valuations of service delivery by end users. According to DSL Forum TR-126 (Digital Subscriber Line Forum), QoE and QoS (Quality of Service) are two different concepts:

- **QoE** is the overall performance of a system from the point of view of the users. QoE is a measure of the end-to-end performance at the service level from the user perspective and an indication of how well the system meets the user's needs.
- **QoS** is a measure of performance at the packet level from the network perspective and performance of other devices involved in the service. QoS also refers to a set of technologies (QoS mechanisms) that enable the network administrator to manage the effects of congestion on application performance as well as providing differentiates service to selected network traffic flows or to selected users.

Both technical and non-technical parameters must be considered in order to infer the QoE experienced by the end users. Non-technical parameters usually require subjective user evaluations with methods such as surveys or dynamic user feedback provision methods made available on the user device. In the following, we provide a short overview of QoE models and a more concrete evaluation example in the video application domain.

4.2 QoE Models & Evaluation

There is no general standard on evaluating and expressing QoE. However, there have been recommendation documents or publications that suggest mainly application-specific QoE metrics, objectives, and considerations. Among those, the Technical Report 126 of the DSL Forum (Digital Subscriber Line Forum) is a good source of information on QoE for the three basic services composing the so-called "triple play services". Before briefly summarizing the findings and recommendations there for a sample service type, we first list the main elements that have an important effect on the user QoE in general.

- **The end user devices** such as an iPhone, Android G1/G2 phone, Blackberry Handset or laptop with a 3G Modem:. The performance of the device, its CPU, memory, and other

physical characteristics may have a major influence on the user quality of experience. It is also useful for operators to know those aspects in order to maximize QoE.

- **The application** running on the terminal is of paramount importance, determining the actual network requirements for a satisfactory QoE level. We will delve more into this in the rest of this section.
- **The radio network** of the operator is usually the bottleneck in terms of capacity, coverage, and mobility aspects, and hence can greatly influence QoE.
- **Operator's application servers** can also have an effect on QoE. Content servers, various gateways, MMSC (Multimedia Messaging Service Center), and streaming servers are typical examples of serving entities. The connection of these servers and their amount on the network might impact QoE as well, such as high latency at peak usage times due to insufficient content servers.
- **Price & billing** is one of the major factors in determining the user satisfaction level for most user groups, therefore could be regarded as part of the QoE specification. High prices for services or billing errors can negatively influence a subscriber's QoE.
- **Network security** has also a big influence on QoE, with the major issues of data hacking attempts or malicious software such as viruses. QoE can greatly drop when subscribers do not feel that the network is secure.
- **Privacy** is an increasingly common concern in today's digital society. Users would like to ensure that their identity, communications, and digital actions are well preserved from being exposed or misused by unauthorised parties. Therefore privacy is an important aspect of QoE specification for most services.
- **The core network** components, though not visible directly to subscribers, also have a strong effect on the end-to-end service quality experienced by the user. The core network can affect subscribers' QoE by affecting connection aspects, such as latency, security, and privacy.

We now briefly overview **QoE** objectives and **assessment** models for Entertainment Video using an example based on **TR-126 of DSL Forum** (Digital Subscriber Line Forum)**.**

4.3 QoE Assessment in Entertainment Video

The Entertainment Video application category comprises video on demand (VoD), broadcast video and premium video content (e.g. pay per view) services. Entertainment video includes:

- Broadcast channels
- Specialty or premium channels
- On-demand content including movies, time shifted broadcasts, network PVR, live and recorded special events such as PPV, etc.

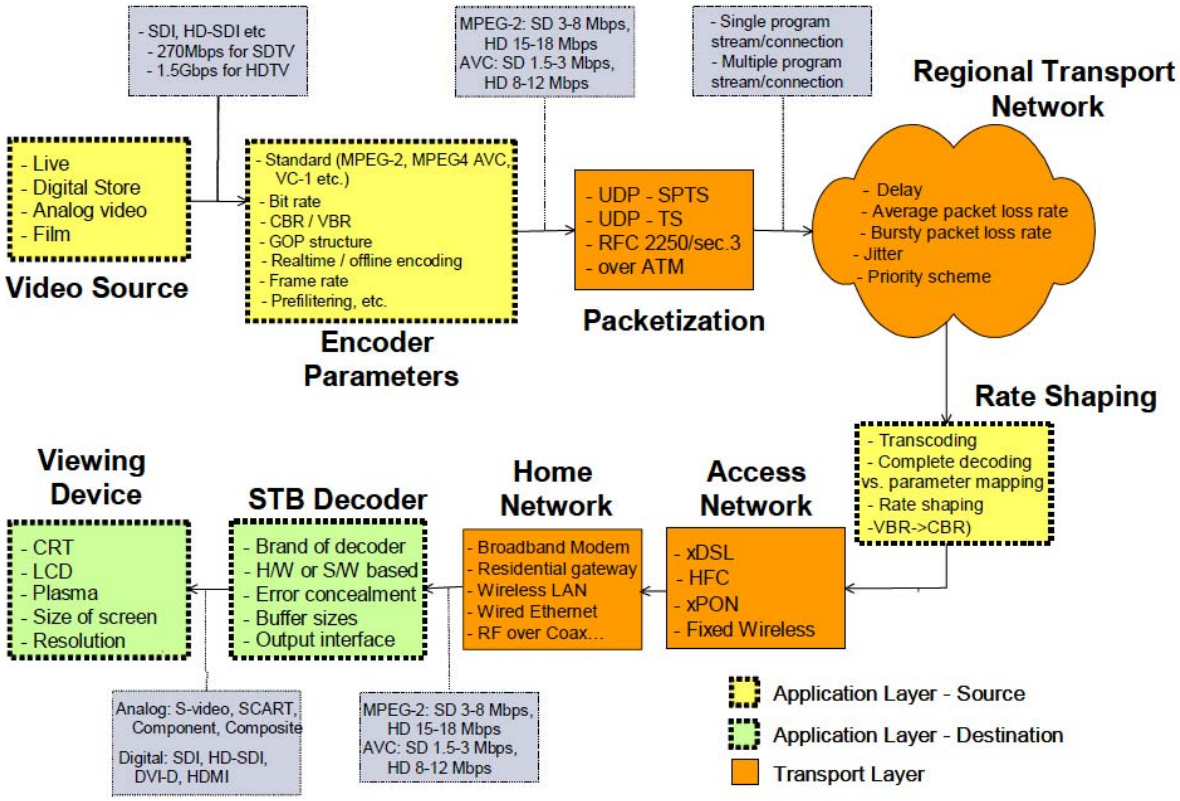

Figure 1. End-to-end Video Services Delivery System (Digital Subscriber Line Forum)

As shown in **Figure 1**, there are many factors influencing the QoE for the end user. These factors are classified into three groups as Source Application Layer, Destination Application Layer, and Transport Layer, as indicated in the figure.

The video picture quality contributions to QoE can be measured in three ways:

- **Subjectively** using a controlled viewing experiment and participants who grade the quality using rating scales such as Mean Opinion Score (MOS)
- **Objectively** at the service layer – using electronic test equipment to measure various aspects of the overall quality of the video signal (e.g. PSNR – Peak Signal to Noise Ratio)
- **Indirectly** – using measurements of network impairments (loss, delay, jitter, duration of the defect) to estimate the impact on video quality, where there is an established relationship between QoE and QoS.

4.3.1 Subjective video quality measurement

Subjective evaluation using human viewers to rate the video quality can provide the most accurate assessment of video quality from the perspective of a service provider's customers. Subjective evaluations are done either informally or using formal techniques. Informal evaluation of video quality is often done by service provider craftsperson on site and technical experts ("golden eyes") in the video system head end or during commissioning. These skilled experts often have years of experience in knowing what to look for. Unfortunately these "golden eyes" may not always be available, may not provide repeatable results, and may not reflect the preferences of the service provider's customer population. Formal subjective evaluations use tightly controlled environments and many carefully qualified experiment participants who view various video clips and rate the quality.

Generally television subjective video picture quality tests are performed following the guidelines established in ITU-R Recommendation 500 (ITU-R, 2002)32 known as "Rec 500". Rec 500 provides detailed guidelines for standard viewing conditions, criteria for selection of subjects and video test sequences, assessment procedures and methods for analyzing the collected video quality scores.

The complexity, time and costs of subjective video quality evaluation has driven many researchers to attempt to create models of human video assessment in an attempt to replicate the scores given by subjects in an objective tool. These so called Perceptual Video Quality Measurement (PVQM) algorithms have undergone significant improvement in recent years but much remains to be done.

4.3.2 Objective video quality measurement

Objective video quality measurement techniques, although not as accurate as subjective video quality measurement, offer a good compromise to conduct video quality assessment tests. Objective video quality measurement tests can be performed quickly to support fine tuning of network variables.

A growing concern of video researchers and broadcasters is the assurance and maintenance of an acceptable service quality level for the distribution of video programming. In 1997, the ITU created the Video Quality Experts Group (VQEG) to address video quality issues, in particular the development and standardization of accurate objective methods for estimating subjective video image quality. Traditional analogue objective measurement systems, while still necessary, are not adequate to measure the quality of digitally compressed video systems. With the shift in technology from analogue to digital and from synchronous to packetized transport, the types of visual artefacts have changed. To properly assess these new artefacts, new objective methods need to be developed and standardized. Many of VQEG participants are also active in the ITU-T SG9 and SG12 and ITU-R SG6.

The goal of the VQEG is to evaluate and recommend objective video quality measurement techniques and feed the final recommendation to ITU and other bodies for standardization. Selection of an objective quality measurement technique for a particular application consists of four parts:

- Definition of the test conditions including test material, type of codecs, channel conditions, viewing environment, test results analysis criteria, etc.
- Proposals of objective quality measurement techniques including the executable code to perform quality measurements. The evaluation process is open to all creators of objective video test methods.
- To ensure fair testing of proposed methods an Independent Lab Group (ILG) defines and conducts the subjective testing and processing of data through the models. ILG members include Verizon/USA, CRC/Canada, Nortel/Canada, Intel/USA and FUB/Italy.
- Finally the subjective and objective testing results are compared, and correlation analysis undertaken to select best objective quality measurement technique(s).

4.3.3 Indirect Measures: Network Impairment Parameters

The Network Impairment method uses packet network parameters such as packet arrival time, delay, jitter, loss, impairment duration, and sequence number to extrapolate the video quality. Once the other evaluation tools are used to set tolerance for network performance based on QoE goals, these network parameters can then be monitored to provide a relatively cost-effective indication of the contribution of network behaviour to video quality.

5 NGN Management and Semantics

The telecommunication network management practices are strongly rooted in those of monopolistic telecom operators. The liberalization of the operators has only changed the landscape from the perspective that there were more closed operators rather than one closed operator. As a result they are usually centrally managed, poorly integrated with outside components, and strictly isolated from external access. On the other hand the IP world has been about internetworking - IP stands for Internetworking Protocol - from its conception on. Furthermore the exposure of the users to the prolific Internet services means that similar service models will have to be provided by the NGNs, which otherwise risk to be turned into mere bit-pipes The clash between these two opposite approaches of Internet Services and NGNs poses important challenges especially in the management of NGNs.: In order for NGNs to be economically viable, they should provide similar user experience with Internet services, albeit in a more managed and reliable manner.

The foremost challenge lies in the integration, analysis, and usage of vast amount of **management, and management-relevant information** contained in the heterogeneous environment that the all-IP aspect of the NGN brings along. The sheer size of this information makes a central management scheme, which was relevant for the telecom operator centric era, insufficient, if not irrelevant. The goal is to let the network nodes utilize the **knowledge** about themselves and their working environment for the more efficient functioning of the service provisioning that they are involved with. The main inefficiencies that need to be addressed in the scope of NGN networks are the interdependence of functionalities such as routing and access control, the limited scope of management information within operator borders which limits the ability to offer personalized end-to-end management of service provisioning. There are mainly three lines of research that could be identified in this area:

- **Improving Current Practices**: The industry funded research and development in the network management area can be put into this category. There has been efforts to integrate the concepts of Web Services to improve the current network management schemes to support the challenges of NGN (Lopez de Vergara et al., 2003).
- **Evolutionary Approaches**: These approaches are identified by their novel use of cross management boundary information, divergence from the telecommunications operator management practices, and application of new paradigms to the networking protocols. However, they do not require absolutely new networking hardware or software, and are based on the premise that the successful evolutionary ideas would force the changes in the networking hardware and software naturally (Strassner et al., 2006.).
- **Revolutionary Approaches**: These mainly academic research directions pose the question of how one would have designed the Internet, being given the possibility to start from scratch. With this setting, it is possible to develop architectures that require new hardware and software as well as new management mechanisms (Clark et al., 2003.).

The use of semantics and ontological concepts is seen as a viable solution for the emerging management issues in *open networks of the future*. As explained in the previous section, those networks will be user-centric in nature, based on a common standardized QoE framework. Moreover, the users in converged NGNs will be much more flexible and dynamic, having real-time roaming capability among different network providers without fixed contractual agreements. In such a scenario the **identity** of users should be transparent among network

providers while respecting users' privacy. Moreover, all the information related to their QoE characteristics, as explained in previous section, should be in a common format and accessible to all providers. Hence, a common semantic information store is required for NGNs, which involves data from different levels and entities of the network, including the identity-related information.

The rest of this chapter builds up on this observation to provide an overview of existing approaches in the literature to provide such functionality in communication networks.

5.1 The Knowledge Plane

In (Clark et al, 2003), Clark et al. envisioned the Knowledge Plane (KP), a distributed cognitive system augmenting the Internet's current architecture by a separate plane that relies on cognitive techniques. The proposed architecture of the KP tries to marry the advantages of the current Internet, like its openness to new applications and decentralized structure, to the new concept of a network that (re-)configures itself given high-level instructions. This is motivated by the high configurational overhead of network administration that is performed manually on a low-level (i.e. per router configuration of routes, policies) and its limitation to operator domains. Instead, the network should have a high-level view of its design goals, understand what it is being asked to do and take low-level decisions accordingly. To fulfil this sophisticated goal, knowledge representation, learning and reasoning techniques are employed to allow the KP to be aware of the network and its actions in the network.

The KP as presented by Clark et al. is a theoretical concept and to be realized, significant research is recognized to be necessary. However, as a start important attributes of the KP as well as research challenges that must be solved are discussed.

The most important attributes of the KP are the global perspective to correlate observations from different parts of the network, the compositional structure that enables two previously unconnected networks to merge their perspective upon connectivity and the unified architecture - a single unified cognitive system that is based on knowledge forms the KP instead of distinct mechanisms that are based on the task to be performed. Furthermore, it is stressed that the design goals of the envisioned system can be only reached with the proposed architecture, opposed to integrating the cognitive functionality into the management plane.

The KP is proposed to use cognitive techniques since it must cope with incomplete, inconsistent or malicious information and has to perform appropriately dealing with conflicting high-level goals (e.g. of two competing providers), which is not possible with analytical solutions. Instead, it must be able to learn and reason, i.e. compose existing knowledge to draw new inferences and beliefs.

5.2 Sophia: An Information Plane for Networked Systems

In (Wawrzoniak, 2004), Wawrzoniak et al. proposed an example network Information Plane called Sophia that has been deployed on PlanetLab. Sophia is a distributed system that collects, stores, propagates, aggregates and reacts to observations about the network's current condition. It is motivated by the management challenges of complex overlay network infrastructures like PlanetLab. To meet this challenge, the distributed system collects information about network elements, evaluates statements about network state and reacts according to conclusions drawn about the information. This functionality is realized by 3 components being a distributed set of sensors that report data, a distributed declarative

programming environment to evaluate logic statements and a distributed set of actuators to perform local actions.

Sophia's approach to decentralized management can be seen as a distributed expression evaluator, with statements that are given in a declarative logic language.

Performance demands in Sophia are met by caching evaluated expressions and sensor reports, scheduling of expression evaluation in advance for timely results and by planning an evaluation to be performed in the network close to a dependency on another node. Furthermore, in order to function in the presence of failures, the evaluation of expressions can be deferred until dependencies are resolved while the partial results can be used.

In contrast to the Knowledge Plane discussed in the previous section, learning algorithms and other AI techniques are not used within Sophia and thus Wawrzoniak et al. call it an implementation of an Information Plane.

5.3 A Clean Slate 4D Approach to Network Control and Management

In (Greenberg et al, 2005), Greenberg et al. propose a complete refactoring of the architecture of the Internet following a design referred to as 4D after the architecture's planes decision, dissemination, discovery and data. It is argued that the fragility and management difficulties of today's data networks stem from the complexity of the control and management planes and the way they are integrated in routers: The decision logic is implicitly embedded in routers via the distributed control algorithms that are running on them, while management protocols are built on the side to monitor and configure them. Thus a design is proposed that singles out the decision plane which is then responsible for the network configuration of an AS, satisfying AS-level objectives, and controlling operation of the data plane. Besides handling packets based on the decisions of the decision plane, the data plane gathers and delivers state information to the discovery plane. The dissemination plane links the decision entities to the routers and switches. Furthermore, it carries the state info gathered by the discovery plane of the network elements towards the decision plane, and the management decisions to the data plane. Finally, the discovery plane discovers the physical elements in the network, identifies them, gathers their state and identifies the relationship between the identified elements.

The 4D architecture has been styled along three design principles: a network-wide view of the topology and traffic is available to the decision plane which implements network-level objectives (opposed to low-level configurations) by exerting direct control on the operation of the data plane.

Greenberg et al. state that their research on the 4D architecture is still in an early stage, consequently the nature of their proposal is more of a theoretical nature, listing several research challenges to be solved before implementation.

5.4 FOCALE Autonomic Networking Architecture

In chapter 2 of (Mahmoud, 2002) and a series of papers (Strassner, 2002), (Strassner et al, 2006), (Strassner et al, 2007), Strassner et al. introduced their conceptual model of an autonomic networking system called FOCALE (**F**oundation **O**bservation **A**ction **L**earn r**E**ason). It is recognized that the traditional network management based on human monitoring and intervention is not suitable for communication networks that become increasingly dynamic, heterogeneous, less reliable and larger in scale. Instead the vision of autonomic network management is pursued with self-governing systems that dynamically adjust services

and resources and that are able to sense and interpret context changes to adapt management policies accordingly. To achieve this the behaviour of network devices is captured in finite state machines that allow to determine the current system state based on the monitored information (context), compare if this state equals the desired state and perform reconfiguration if not. This procedure is realized with two control loops, one responsible for monitoring, the other for reconfiguration of possibly multiple network entities (e.g. to resolve failures caused by mis-configuration of multiple devices). To enable reasoning on network configuration, FOCALE makes use of ontologies to model the information that is available in vendor specific data models of network devices and enriches the derived ontological representation of these facts with the semantics that are inherent to them. Furthermore ontologies are used to obtain new knowledge by inference, for example an SNMP alert that triggers an inference process to determine a set of users whose SLA's are affected.

Opposed to the Knowledge Plane proposal, FOCALE defines two new planes, a management and an inference plane, that maintain compatibility with legacy devices and applications. A prototype of FOCALE is under development at Motorola Labs.

5.5 Runtime Semantic Interoperability for Gathering Ontology-based Network Context

In (Keeney, 2006), Keeney et al. argue for a paradigm shift in network management that moves from answering "how"-questions like "how can I configure a router for my needs" to "what" questions, "what do I want from my network". This involves migrating management intelligence from network administrators to the network elements while the operating staff should specify required network goals and constraints. The envisioned autonomic network then collaborates dynamically based on acquired network knowledge and acts in order to meet these goals and constraints. This paper deals with efficient delivery of network operation knowledge to the nodes that will use this knowledge as context information to take management decisions. The Knowledge Discovery Service (KDS) is based on ontological representations, which promotes a graceful evolution. The knowledge is transparent to the nodes providing and consuming knowledge.

6 NGN Services − Case Study: Semantic IPTV

IPTV has tremendous potential in enhancing the experience and benefits of multimedia based entertainment, communication, and advertisement services from the perspective of both users and providers. Service providers, will have increased control of their channels and content with IPTV and will be able to offer innovative services to their users. The current delivery mechanisms through cable or satellite transmit a whole set of channels to the user premises, limiting access to only the authorized content within that comprehensive set (with the limiting usually based on encryption of the streams). This moves the control of content access completely to user side, and there are many exploits of this scheme allowing users to obtain receiver boxes with software to decrypt and access all available content at the end of the cable or satellite receiver. Due to the one-way communication nature of these delivery systems, there is no way to detect such exploits, which completely takes access control out of the hands of the content providers. On the user side IPTV provides an integrated service environment, loaded with extra features for increased social interactions. Semantic IPTV will enable personalized and easily accessible multimedia content and communication features for its users.

The main enabler for Semantic IPTV is to create a semantic space that describes the content, context, and user preferences. Unlike the passive audience of standard television broadcast, Semantic IPTV users should be able to search for and easily access the content they want to watch, just like they can access textual data on the Web. Moreover, personalization services enable automatic transformation of user benefits and interests into recommendations or even personalized channels that are generated on-the-fly from all available streams.

This chapter provides a more detailed view on the scenario of Section 3.4 with a focus on personalization and recommendation aspects of IPTV services in NGNs and briefly presents an architecture that allows functionalities described therein.

6.1 Personalization and Recommendation

Personalization is the approach of providing an overall customized, individualized user experience on the basis of profile and context information associated with a user or a group of users. Personalization requires the ability to select content satisfying the preferences of users. The fundamental question is, if a given user should be provided with a particular piece of information (Jokela and Sulonen, 1999). Applying personalization features to IPTV services like EPG, nPVR, Parental Control or Targeted Advertisement increases the value of these services not only for the user, but for all players in the IPTV value chain. In this section, taxonomy of personalization approaches and their applicability in the semantic IPTV context are presented.

Today's upcoming IPTV services provide an increasing amount of video content and accessible TV broadcasts to users. Potentially every media resource on the Internet will be accessible by IPTV users. Therefore there is a need to assist people in selecting the appropriate content and to filter all the irrelevant or even annoying content. As we have discussed before, personalization systems meet the requirement to select content satisfying the preferences of users. But the application of personalization features to IPTV is not only desirable from users' perspective. As stated in (Friedrich et al., 2008) "the dream to address single users or groups of them with the same interest with personalized or so called targeted advertisements has always been on the wish lists of broadcasters and content providers so far". Other IPTV related services that are very suitable for personalization are the electronic

program guide (EPG), personal video recorder (PVR) functionalities and parental control. Personalized EPG focuses on recommendation of upcoming live broadcasts tailored to the users' interests in the TV program, while a personalized PVR supports automated recordings of relevant broadcasts as well as recommendation of stored videos. Parental Control provides content filtering to protect users (especially children) from improper content. The approach in Semantic IPTV is to apply a smart recommender system to the IPTV infrastructure to provide this kind of personalized services.

According to Friedrich et al., the IP Multimedia Subsystem is a perfect architecture to deliver personalized and IPTV services. They propose the integration of a so called "IPTV service personalization function", into the IMS, which is "used for gathering information on user behaviour, the processing of user profile data and manual user ratings and for generating content recommendations". As the heterogeneity of networks and the diversity of user end-devices grow with the convergence of broadcast and communication services, there is a demand for IPTV personalization features (even from a content agnostic view). The provisioned service should adapt to the user's end device capabilities and network characteristics representing the user's context. To achieve context-aware personalization, IPTV standard bodies focus on next generation infrastructures (like the IMS) that are in charge of networks and user context parameters. Besides this, the deployment of IPTV over IMS and the convergence with communication services brings along social relations between users as a valuable source for recommendations. These social relations are especially useful for collaborative-based techniques.

The collaborative-based personalisation is completely independent of any machine-readable representation of the items that are recommended. It therefore works without metadata descriptions of IPTV content. It solely relies on the similarity between users. This similarity can be derived from social networks as well as it can be derived from comparison of user profiles. Users with a certain degree of similarity are so called peers, building a peer group, which represents the source for recommendations.

With the high diversity of content provided by future IPTV services, the social relatedness of content recommendation should gain importance. On the other hand the constitution of peer-groups by the recommendation systems helps users to find others with similar interests and to extend their social networks. From a providers perspective these peer groups can be used to maximize the effect of an advertisement, more effectively reaching the advertised product's target audience increasing advertising revenue potential. It also benefits end-users as advertisements are more in line with their interests and view preferences. Together with content recommendation, targeted advertisement enhances the value of IPTV as a powerful medium.

6.2 Semantic IPTV − A Reference Architecture

As the IP Multimedia Subsystem (IMS) provides a platform for converged, personalized, and controlled person-to-person and person-to-content communication services in next generation networks (NGN), it represents a well-suited infrastructure to run unified IPTV services. This section describes an IMS-based IPTV implementation developed at the DAI-Labor of Tech. Uni. Berlin, called *myMedia*, in order to demonstrate and explain the architecture and components that could realize the Semantic IPTV concept.

The semantic IPTV approach in *myMedia* utilizes the IMS to initiate and control IPTV services, provided by a dedicated application server (AS) in conjunction with a Media

Resource Function (MRF). Moreover, standardized service building blocks such as the OMA XDM Enabler and the Presence Enabler are used. But the main focus is a smart semantic recommender that allows enhancing the IPTV user experience.

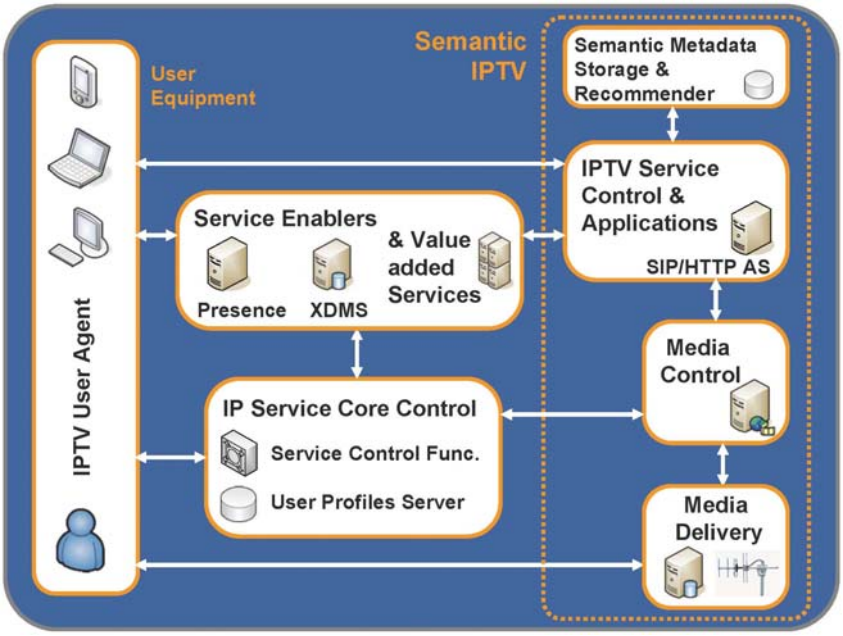

Figure 2. A high-level overview of *MyMedia* Semantic IPTV components

A high level view of the infrastructure and interaction of the components developed for the semantic IPTV services is depicted in Figure 2. The infrastructure consists of a client and several server-side components. This chapter reviews only a few identity-related components followed by the main application termed as IPTV user agent.

6.2.1 IPTV User Agent

The IPTV User Agent is the user's interface to the Semantic IPTV system. The IPTV User Agent is based on a full-featured SIP phone (SIP UA), packed with basic functionalities like audio and video telephony, contacts and presence management, instant messaging and call transfer.

Figure 3. Semantic IPTV components – User Agent

The SIP UA architecture is enhanced with the support of IPTV application server to provide the user a rich, interactive, personalized TV experience including the following features:

- Live TV, Video on Demand (VoD), Private Video Recorder (PVR)
- Recommendation System for Live TV and multimedia content
- Personalized multi-stream view
- Session transfer between devices
- Enhanced Electronic Program Guide (EPG) and multimedia content guide
    - Personalized recommendations selections
    - Enriched EPG data through our semantic approach
- **Social interaction**
    - Buddy recommendations
    - Content rating
    - IPTV presence (See-What-I-See)
    - Cinema chat (Content based chats)

6.2.2 Presence Server

While the Presence Server is a special SIP application server used to manage service- and user-related presence information (e.g. availability, status, situation), in the IPTV context the presence server also holds valuable context information like the program currently watched by a user or information about devices that are currently available. This presence data builds the basis for stream transfer between devices (video follows) and personalization services.

The presence server implementation follows the Open Mobile Alliance Presence Enabler specification and the SIP SIMPLE standards. It supports SIP based subscription and notification mechanisms for presence events, allows publishing presence information and interacts with the XDM Enabler to manage the data persistently.

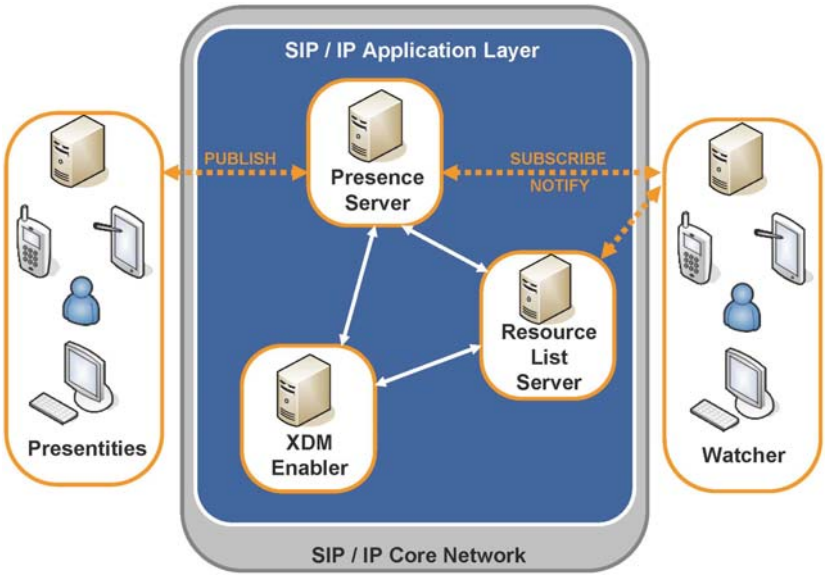

Figure 4. Semantic IPTV components – Presence Server

The Resource List Server (RLS) functionality allows single presence subscriptions on a group of entities that result in an aggregated notification with the requested data. The integration of this function helps saving bandwidth, which is especially useful in mobile scenarios.

As the presence data has to be protected to ensure privacy issues, the presence server supports an authentication mechanism based on the watcher information event package that allows a user to grant presence information access permissions to a watcher.

6.2.3 Smart SPIT avoidance System

Concerning the telephony feature of the Semantic IPTV framework, a Smart SPIT (Spam over Internet Telephony) avoidance system is necessary to guard users and services from malicious and unwanted communication attempts.

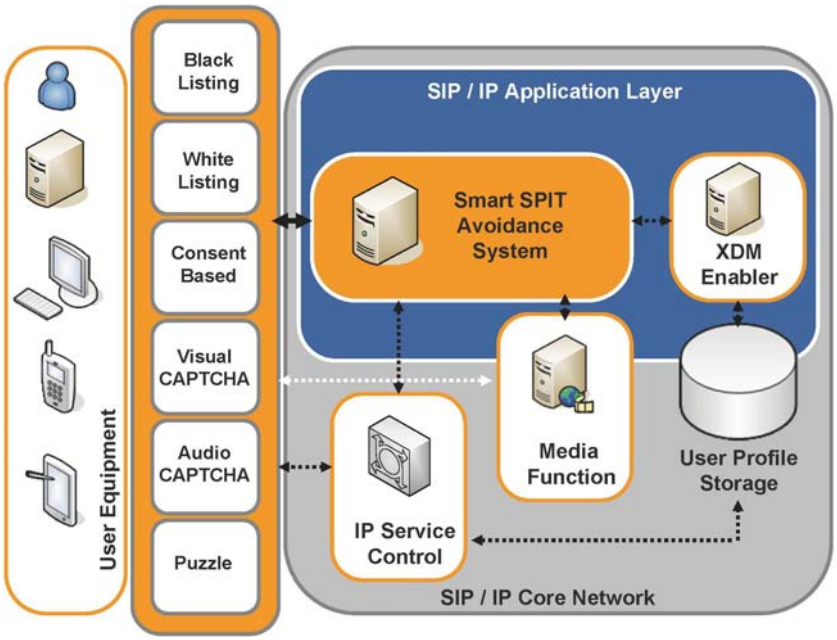

Figure 5. Semantic IPTV components – Smart SPIT Avoidance System

The Smart SPIT avoidance System provides several different standards-based mechanisms, which ensure that the overall infrastructure will not be misused for SPIT. It is subdivided into dedicated components realizing these mechanisms and can be easily extended to address upcoming techniques to combat SPIT. The components that are already implemented follows next.

Black-listing and white-listing -- The black- and white-listing approach is a simple to use mechanism to decide if a communication attempt should be blocked or not. The System automatically manages black- and white-lists and provides users with their own manageable lists.

Visual and Audio CAPTCHA -- CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. It is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.

Consent-based Framework -- This framework allows users to grant or deny SIP entities permission to communicate with a given set of users. Without such consent, it is possible for SIP to be used for malicious purposes, including amplification, and DoS (Denial of Service) attacks.

Puzzle -- The puzzle module is used to raise the costs for SPIT attacks so that it is not worthwhile anymore. This is done by challenging a client with a computationally complex problem that, for instance, takes time or processing power to be solved.

7 Privacy threats in Next Generation Networks[5]

This chapter discusses emerging challenges for privacy and data protection in conjunction with NGNs as outlined in this Deliverable. To keep the analysis concise and focussed, we concentrate our exposition to the case of personalised media over converged delivery channels (cf. scenario "Semantic IPTV", Section 3.4and Chapter 6). Nevertheless, similar threats emerge in other scenarios as well.

7.1 Anonymous media consumption – A vanishing privilege?

Progress in information and communication technology is about to change the shape of our media society: while in the past, electronic mass media, such as television and radio, was distributed over true *broadcast channels* (i.e., everybody potentially receives everything) with subordinated *local selection* of preferred content, the adoption of IPTV and other alternative packet switched distribution channels creates, as a side-effect, network traffic data that reveal which recipient watches what content where and at what time. Although this information is not always evaluated to date, its sheer existence might whet the appetite to capitalize this information.

Moreover, a similar development is observable for traditional print media, such as newspapers. The vanishing number of subscribers and ads revenues (mainly due to classified moving to the Internet) forces publishers to other distribution channels for news than printed paper (BBC, 2009). Many of the new approaches, despite often all but economically successful, make use of point-to-point communication channels. Again, this goes along with a loss in privacy for the audience: while it was possible (and socially accepted) to buy a newspaper containing a bundle of articles anonymously and then select locally, which article one actually reads, point-to-point communication and personalized media services reveal detailed information about the identity of the reader, his or her reading habits, and allows to draw inference on personal interests or political standpoints.

Both examples highlight that the opportunities offered by new technology for the distribution of news in a society also have their downsides when it comes to the privacy of its users. In the following we will argue that the notion of users who lose privacy is far broader than the (already large enough) audience, and thus new privacy threats might endanger vital parts of the media system itself.

7.2 Threat scenarios

To further analyse the abstract privacy fears stated so far, and to narrow them down to more concrete threats, in the following we sketch an imaginary integrate media platform. Although imaginary, blueprints for such platforms exist in the minds of technology developers and media executives. Their feasibility has also been explored in various research projects, for instance the IP project MESH (http://www.mesh-ip.eu/?Page=Project). Using such an imaginary platform allows us to identify stakeholders and derive from their interests what kind of incentive they might have with respect to exploiting the data available in the platform or its underlying infrastructure.

[5] This section is based on a talk at the MESH Summer School on Multimedia Semantics 2008, Chania, Crete.

7.2.1 Integrated media platform

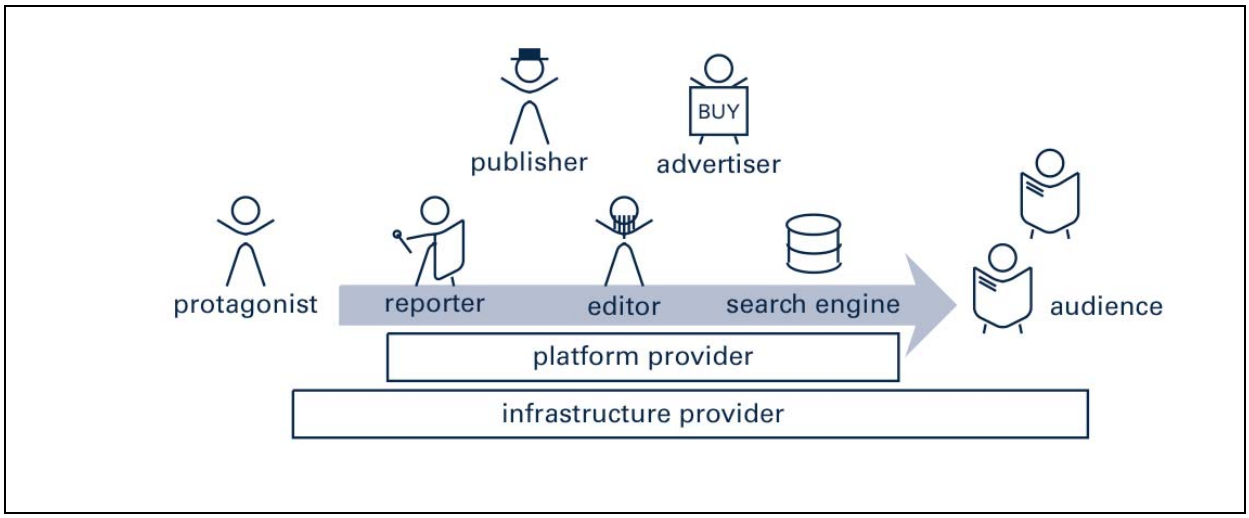

Figure 6. Integrated media platform as an example for NGN in mass media

Figure 9depicts a stylized model of what we call *integrated media platform*. The main purpose of any media system is to convey information about relevant events and their **protagonists** to a larger **audience**. This information flow is visualised by the dark gray arrow. In the traditional media system, several stakeholders contribute to this flow of information:

- **Reporters** do research and gather information in the field. They also interview protagonists and other persons acting as sources.
- **Editors** revise and double-check the research of reporters and edit them into pieces of news (typically articles).
- **Publishers** own and manage media firms. They usually leave their editors some freedom on the contents, but are certainly interested in the success of the business. This mean they have to cater the needs of advertisers (who pay for attention by the audience) and they must ensure that the media product has a sufficiently high circulation. This has been a source of conflict in the past, and we will later show that naïve use of new technology may leverage the conflict surface.

The vision of an integrated media platform uses NGN to combine all information systems in the media production and distribution system, which have individually appeared over the past decades. Broadly speaking, it comprises the communication infrastructure between disperse reporters (correspondents) and the editorial office, joins the content management system with the editorial desk, a (semantic) search engine, and personalized news portals catering for the preferences of each individual reader. Realising this vision creates some additional stakeholders, namely:

- A **search engine** is introduced as a kind of secondary gatekeeper between the editor and the audience (traditionally, the editors has been perceived as "gatekeeper" who selects the relevant news and separates it from noise (White 1961)).
- The **platform provider** operates and further develops the distributed application that connects the news gathering process with media production, delivery and ultimately consumption.

- The platform itself is based on an even broader general-purpose communication infrastructure, notably the Internet. The **infrastructure provider** maintains and administers this infrastructure.

In this setup, obviously a lot of personal data including detailed access and usage traces are generated and probably stored. Storage of information is sometimes necessary for technical reasons, e.g., routing, resilience, and anomaly detection. Other reasons to store are functional requirements (user preferences to feed recommender systems; general convenience features) or for documentation. But apart from these uses of data storage, quite a number of threats emerge if it is disclosed to the wrong persons. Hence, we will exemplarily outline the three most pressing threats that come to our mind.

7.2.2 Audience at risk

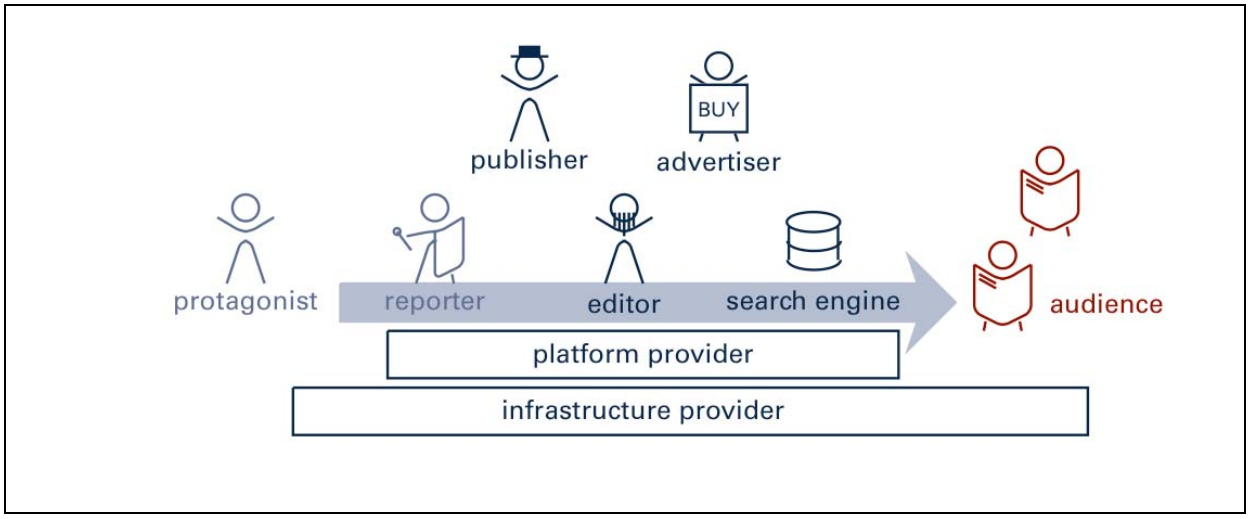

Figure 7. Audience preferences monitored by media industry

The first threat which is outlined here compromises the privacy of the audience. Persons in the audience select media contents according to their personal interests and opinions. The content selection (particularly, if applied to a very fine-grained content structure) reveals personal information about the person, e.g., newspaper articles will be selected according to political attitudes (see also the theory of selective exposure (Klapper 1960)). A detailed log of content selections may contain, besides the actual selection, the time of request and possibly also the duration of access. The privacy of the audience (on the right hand side in Figure 9) is the more compromised the more personal information is collected by observing the selection of contents over time, i.e., by profiling persons in the audience with regard to their opinions, preferences, and habits. In our setup, four parties may benefit from profiling the audience, the search engine, the editor, the publisher, and the advertisers. All of them may use the data for maximising their profits, e.g., by means of price discrimination (Odlyzko 2003).

7.2.3 Sources at risk

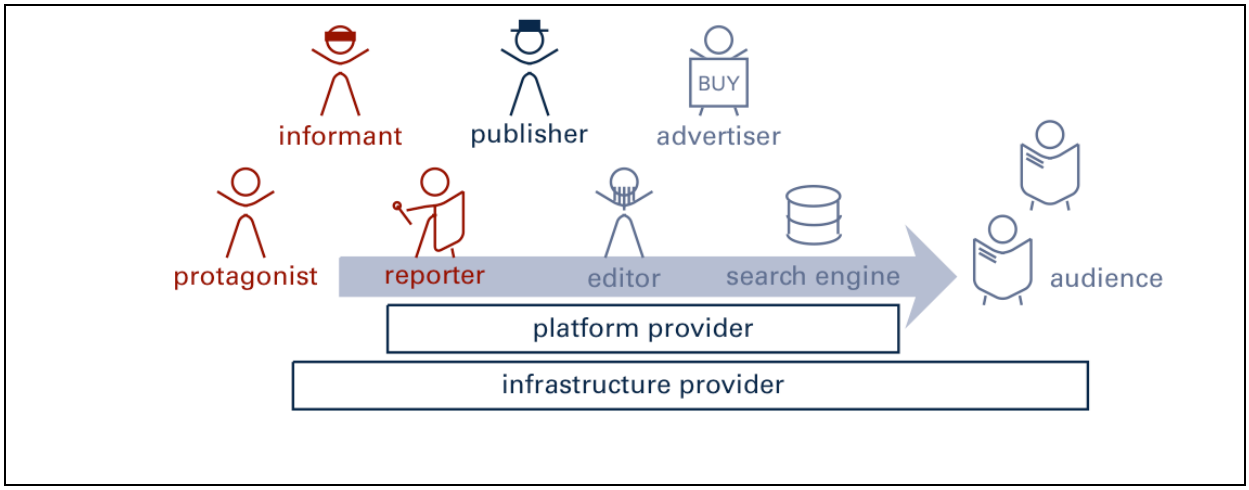

Figure 8. Compromise of confidentiality of sources endangers news gathering

The second threat we are going to outline here is compromises the privacy of the sources (on the left hand side in Figure 9). Following the newspaper example, a reporter uses a number of different sources to create an article in the traditional way, including information from known protagonists and anonymous informants. The article is revised several times before the editor gets the complete draft, which makes it impossible for him to track back which information comes from which particular source. Using the integrated media platform each single edit of an article or other content is recorded and therefore traceable. The "history" of an article development compromises the privacy of sources, as the edit records may easily be matched against phone call or e-mail records. Positive matches may reveal the link between source and article content to anyone who has access to both, the edit records and the communication records. The linkability between information and its source is not only a problem for the informants and protagonists, but for the journalists as well, since the sole possibility that this technology puts the source at privacy risks may intimidate and stop informants and protagonists from talking to the media.

7.2.4 Journalism at risk

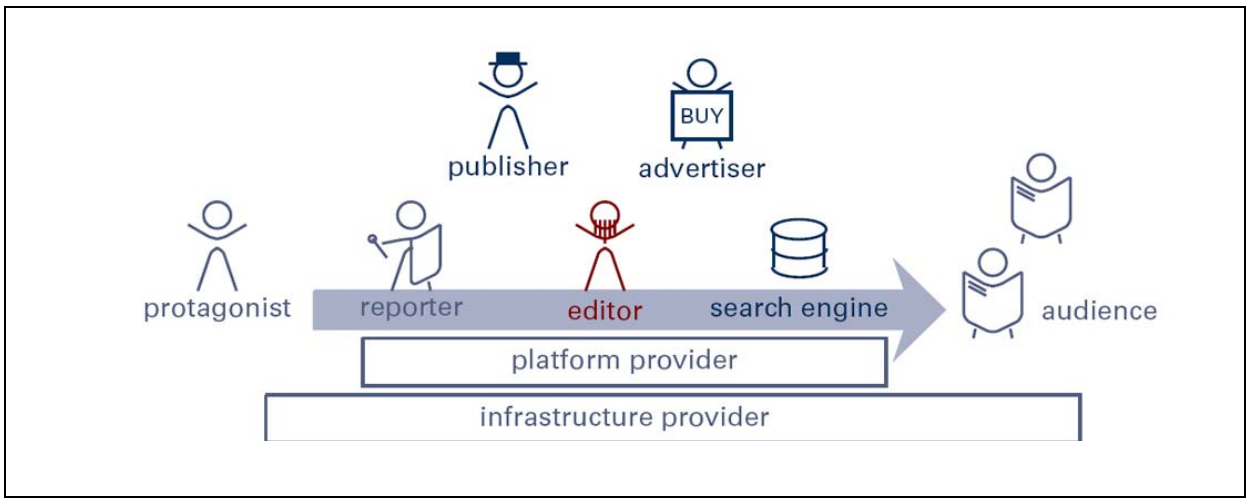

Figure 9. Panoptic newsrooms endanger free media

The third privacy threat concerns the independency of journalism (depicted by the editor in Figure 9). The more data traces exist due to the integrated media platform, the more the connections and decisions made by the editor inside the newsroom can be tracked back by all parties that might be interested, e.g., publishers or advertisers. Both have economic interests and can influence the opinions that are stated in the contents of the integrated media platform. Besides bias in the published contents, the decreasing of diversity is a problem. Diversity means that different opinions make their way trough the mass media. The more detailed audience ratings are available to publishers and advertisers the less freedom will be given to editors for journalistic experiments. From the economic perspective of publishers and advertisers, it is most preferable to provide only mainstream contents that should guarantee a great share of audience members that are regarded as most relevant for advertising.

7.2.5 Discussion of threats

Two important questions arise in a discussion about the previously sketched threats. First, how realistic are the threats? And second, how relevant are they for the society at large?

Focussing on the first question, three points need to be considered: First, conflicting interest pertain t all kinds of social interactions where different stakeholders have different opinions and goals. Thus, such conflicts will be transferred also to an integrated media platform. Second, historic evidence shows, that every opportunity for abuse has been taken, sooner or later, and this is even more so, if the abuse is not likely to be detectable as in the case of data abuses. Third, the more interests and the stronger the considered interests the higher is the risks of abuses.

The analysis of the second question (the relevance of threats for the society at large) also leads to three arguments: First, opinion building is one of the main functions of the independent media system and this is an essential foundation of democratic systems (Easton 1965). Second, media has a "watchdog" function. Media communicates not only political opinions, but also controls private entities by pointing to problems and blaming organisations that do not behave in a socially accepted way. This can result in conflicts with advertisers, for instance. Third, it is often postulated (though rarely substantiated in behavioural sciences) that individuals who are aware of the fact that they might be observed change their behaviour. They would behave more conformingly when they know that they are watched. This leads to a reduction in the diversity of opinions in society.

Even if we can assume that the integrated media platform and its stakeholders are trustworthy, privacy still could be compromised by external influences, inter alia,

- Backdoors and vulnerabilities in standard software,
- Data leaks by contractors (outsourcing),
- Rogue employees and former employees,
- Mistakes by employees,
- Employees vulnerable to social engineering,
- Blackmail and extortion,
- Future owners (e.g. after hostile take-over),
- Authorities (exposed to same list of risks), and finally the unlikely event of a

- Regime change.

Given this threat analysis it becomes evident that in order to protect privacy in NGN, blind trust is not enough. It requires a trustworthy, multilaterally secure and privacy-friendly information and communication system infrastructure. The building blocks of such an infrastructure have been described in previous FIDIS deliverables. The most important building blocks are trusted (and trustworthy) end-user devices, mainly described and discussed in Deliverable 14.3 and 3.9, encryption, coarsely surveyed in Deliverable 16.3, distributed trust, anonymous communication and pseudonymous communication, surveyed and discussed in Deliverable 13.1 and 16.3, and simplicity in design and implementation.

Trusted architectures may assure that only those actions are performed by the devices which are actually intended by the users. This can be used to (provably) suppress data acquisition, for instance by device-local selection of newspaper articles instead of selective requests. Anonymous communication, e.g. JAP (JAP Anon Proxy), can be used to distribute mass media while avoiding the danger of increasingly detailed profiles. With pseudonymous communication it is in addition possible to establish feedback channels in a privacy-friendly manner.

Finally, it needs to be said that combinations of these building blocks may be useful for mitigating privacy risks in certain situations. They cannot solve all problems created by poor system design or privacy-hostile organisational structures, though.

8 Conclusion: An outline of a Next Generation Identity Management model

All of the services discussed in the previous chapters depend on efficient identity management. For most of them, fast and reliable management of personal data is fundamental. The scenarios have also shown, that compared to previous identity relevant services and applications, in the NGN more and additional types of user information, e.g. on TV interests and habits, are collected and processed. Therefore, privacy of users and effective abuse prevention need to be guaranteed. Considering the large amount of data about individuals, identity management needs to be highly effective and efficient, as well as multilaterally secure. At the same time it gets even harder for users to manage their increasingly complex user profiles. Therefore the requirements discussed in this conclusion cannot claim to be complete.

8.1 Issues and Solution Approaches for NGN Identifiers

As a first step, unified identification criteria need to be chosen, which would be unique for every subscription and have the potential to be used in any of the discussed services. In case of mobile telephony, the IMSI is used for this purpose, allowing to identify a mobile subscription globally, e.g. to bill it with the appropriate roaming fees.

At the same time it must be ensured, that individuals are not forced to link all of their interests to a single subscription identifier, as this would produce an extremely rich personal profile, even richer than in the telecommunication services so far. Approaches to secure the interests of relying parties by firmly binding these rich profiles to individuals via “Identity Planes” covering several network layers or by continuous directory checks can be extremely dangerous for user’s privacy. Therefore it is important to overcome the unilateral security approach of just securing the interests of relying parties and to follow a more multilateral approach considering the security of users. Therefore to protect themselves users will either need to have the opportunity to maintain several subscriptions or to have distinct identifiers (e.g. pseudonyms) supported by one subscription.

Taking into account, that ever more identifiable entities (e.g. intelligent household appliances) will be part of the NGN, the current IMSI number may well not be sufficient. It could be succeeded by e.g. MIPv6 addresses. The range of these addresses then also allows that subscribers can indeed be provided with multiple identifiers, whose utilization can be specified by the subscribers themselves. One identifier could be used as business address, another one for private contacts; a further one can be used as the identification for intelligent household appliances, etc.

If more and more physical entities get globally unique identifiers, this offers the opportunity to link them to organizational entities, e.g. companies, municipalities or individual households. This opportunity will come with the challenge to actually determine the relation of a physical entity to some organization. For shared goods, e.g. in communities, this may not be too easy.

If users have to manage several identifiers they need supporting tools. IMSIs are bound to SIM chip cards with usually one IMSI being related to one SIM card and vice versa. Besides providing robust security this allowed users to associate each identifier with a tangible item. These 1:1-relations are getting more complex now. The development already started with the introduction of several (physical) SIM cards related to one telephone number (identifier) to

allow the parallel usage of one telephone number in several phones, e.g. a car phone and a mobile. At the same time a plethora of identifiers can make it difficult to maintain one physical token per identifier. Managing several identifiers from one physical device can therefore be an attractive solution. This can revive the concepts of personal security assistants or wallets, that had already been discussed some years ago, but so far not been used heavily (with the exception of laptops carrying many identifiers and identity credentials for different accounts and services). A relevant functionality of these wallets is to enable the users t present the right identifier at the right occasion.

8.2 Requirements on the parties involved in NGN services

The NGN services discussed require that the involved parties trust each other to some degree. Given that in communication networks the parties are represented by (virtual) identifiers the trust must be related to those identifiers, e.g. by associating an identifier with an amount of (prepaid) money. This is relevant for operators of e.g. payable NGN IPTV services that want to be sure to receive payment from their users. In any case service providers want to be able to act as "Relying parties" being assured about the properties of their customers.

At this point, the introduction of third parties (sometimes called "Identity Providers") can be useful, as they can confirm the credibility of the parties participating in a service or transaction. Users then need to be protected from third parties misusing their privileges. This holds especially for situations, where every usage of a service requires identity confirmation, as this builds a usage profile with the "Identity Providers" that can severely affect users' privacy.

Therefore "Identity Providers" should not be involved in every transaction users pursue. Also they should provide credentials rather than "identities". These credentials should be strong enough in themselves to deliver enough assurance without "calling back" to the credential provider. Cutting down on the need of online verifications of credentials seems to be unnecessary given the multiple communication options in NGN. However it is the more necessary the more personal (or even intimate) the NGN services become.

Relying parties need to develop policies to manage the acceptance (or not-acceptance) of credentials in line with their own risk management, stateside regulation, and their aim to win and keep (privacy sensitive) customers.

Given the complexity of the NGN sphere the corresponding requirements need to be implemented in NGN standardisation. This is an additional challenge to standardisation in the general area of Identity Management, as NGN standardisation takes place in the ITU-T Study Group 13 "Future networks including mobile and NGN" while the Lead Study Group on Identity Management in ITU-T is Study Group 17 "Security".

9 Bibliography

Clark, David D.; Partridge, Craig; Ramming, J. Christopher and Wroclawski, John T. A knowledge plane for the Internet. In: *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 3–10, New York, 2003. ACM.

Deveson, M. Crisis in the US newspaper industry. In: *BBC News*, 27 February 2009, online at http://news.bbc.co.uk/1/hi/world/americas/7913400.stm.

DSL Forum Technical Report TR-126.

Fatemi, Nastaran. Mpeg-7 in practice: analysis of a television news retrieval application. In: *J. Am. Soc. Inf. Sci. Technol.*, 58(9): pp. 1364-1366, 2007.

Friedrich, O.; Seeliger, R. and Arbanowski, S. Interactive and personalized services for an open IMS-based IPTV infrastructure. In: *Proc. Seventh International Conference on Networking ICN* 2008, pp. 302-307, 13-18, April 2008.

Germanakos P., Mourlas C., & Samaras G. "A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems." Proceedings of the Workshop on 'Personalization for e-Health' of the 10th International Conference on User Modeling (UM'05). Edinburgh, July 29: 67-70, 2005.

Greenberg, Albert; Hjalmtysson, Gisli; Maltz, David A.; Myers, Andy; Rexford, Jennifer; Xie, Geoffrey; Yan, Hong; Zhan, Jibin and Zhang, Hui. A clean slate 4d approach to network control and management. In: *SIGCOMM Comput*. Commun. Rev., 35(5): pp. 41–54, 2005.

Haddon, L. Domestication and mobile telephony. In: J. E. Katz (Ed.): *Machines that become us: The social context of personal communication technology*, pp. 43-55. New Brunswick, NJ: Transaction Publishers, 2003.

JAP Anon Proxy. http://anon.inf.tu-dresden.de, accessed 23 June 2009.Easton, D. A system analysis of political life. Wiley, New York, 1965.

Jokela, Marko Turpeinen Sami and Sulonen, Reijo. Agents in delivering personalized content based on semantic metadata. 1999.

Keeney, J.; Lewis, D.; O'Sullivan, D.; Roelens, A.; Wade, V.; Boran, A. and Richardson, R. Runtime semantic interoperability for gathering ontology-based network context. In: *Network Operations and Management Symposium*, 2006. NOMS 2006. 10th IEEE/IFIP, pp. 56–65, 2006.

Klapper, J. T. The effects of mass communiation. In: *Free Press*, New York, 1960.

Lopez de Vergara, J.e.; Villagra, V.A.; Asensio, J.I. and Berrocal, J. Ontologies: giving semantics to network management models. In: *IEEE Network*, V17(3), pp. 15-21, 2003.

Lopez de Vergara, J.E.; Villagra, V.A. and Berrocal, J. Applying the web ontology language to management information definitions. In: *CommunicationsMagazine, IEEE*, 42(7): pp. 68–74, July 2004.

Mahmoud, Qusay. Cognitive Networks: Towards Self-Aware Networks. In: *Wiley-Interscience*, 2007.

Martinez, Jose M. Mpeg-7 Overview (version 9). In: *Technical report, International Organisation for Standardisation*, October 2004.

Odlyzko, A. Privacy, Economics, and Price Discrimination on the Internet. In: N. Sadeh (Ed.): *ICEC2003: Fifth International Conference on Electronic Commerce*, pp. 355-366, 2003.

Siller, M. and Woods, J. Using an agent based platform to map quality of service to experience in conventional and active networks. In: *Communications, IEE Proceedings*-, 153(6): pp. 828–840, Dec. 2006.

Snoek, C. G. M.; Huurnink, B.; Hollink, L.; de Rijke, M. ; Schreiber, G. and Worring, M. Adding semantics to detectors for video retrieval. In: 9(5): pp. 975-986, Aug. 2007.

Strassner, J.; Agoulmine, N. and Lehtihet, E. FOCALE: A Novel Autonomic Networking Architecture. In: *Latin American Autonomic Computing Symposium (LAACS)*, 2006.

Strassner, John. Den-ng: achieving business-driven network management. pp. 753–766, 2002.

Strassner, John; Foghlu, M. O.; Donnelly, W. and Agoulmine, N. Beyond the knowledge plane: An inference plane to support the next generation Internet. In: *Global Information Infrastructure Symposium*, 2007. First International GIIS, pp. 112–119, 2007.

Wawrzoniak, Mike; Peterson, Larry and Roscoe, Timothy. Sophia: an information plane for networked systems. In: *SIGCOMM Comput*. Commun. Rev., 34(1): pp. 15–20, 2004.

White, D. M. The 'Gatekeeper': A Case Study In the Selection of News. In: L. A. Dexter and D. M. White (Eds.): *People, Society and Mass Communications*, pp. 160-172 London, 1961.