Wifi roaming

Robert, Romain; de Villenfagne, Florence; Jost, Julien; Dinant, Jean-Marc; MANULIS, Mark; LEROY, Damien; KOEUNE, François; BONAVENTURE, Olivier; QUISQUATER, Jean-Jacques; Ker, Caroline; Poullet, Yves

Published in:
International Journal of Law and Information Technology

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

International Journal of Law and Information Technology © Oxford University Press 2008; all rights reserved.
doi:10.1093/ijlit/ean016

WiFi Roaming: Legal Implications and Security Constraints

Romain Robert [1], Mark Manulis [2], Florence De Villenfagne [3], Damien Leroy [4], Julien Jost [5], Francois Koeune [6], Caroline Ker [7], Jean-Marc Dinant [8], Yves Poullet [9], Olivier Bonaventure [10], and Jean-Jacques Quisquater [11]

Abstract

WiFi technology has become the preferable form for mobile users to connect to the Internet. The growing popularity of WiFi-enabled devices and the increasing number of WiFi networks guarantees that this trend will continue in the future. Since a single network provider is usually not able to ensure WiFi coverage for its own users across many geographic locations the WiFi roaming technology appears to be the promising solution. A special attention upon the practical deployment of WiFi roaming should be paid to possible threats coming from the misuse of technology. In this light we analyze various legal implications that might become relevant due to the deployment of WiFi roaming and discuss several risks and problems related to the security during the establishment of roaming connections between mobile devices and the Internet.

[1] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[2] UCL Crypto Group, DICE, Louvain-la-Neuve, Belgium.
[3] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[4] IP Networking Lab, Dept CSE, Louvain-la-Neuve, Belgium.
[5] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[6] UCL Crypto Group, DICE, Louvain-la-Neuve, Belgium.
[7] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[8] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[9] Centre de Recherche Informatique et Droit, FUNDP, Namur, Belgium.
[10] IP Networking Lab, Dept CSE, Louvain-la-Neuve, Belgium.
[11] UCL Crypto Group, DICE, Louvain-la-Neuve, Belgium.

1 Introduction

During the last years, the number of WiFi networks and devices has quickly increased, both in office and home environments. Many laptops, mobile phones and gaming devices contain a WiFi interface and in many environments, WiFi is becoming the default Internet access technology. The ubiquity of WiFi combined to the needs of users to be always connected leads to the interesting research area of WiFi roaming which investigates possibilities for network owners to provide Internet connection via their own WiFi access points to the mobile devices coming from other WiFi networks.

1.1 *Application Scenarios*

WiFi roaming is a service which can be deployed in various application scenarios, also with respect to the economical benefit of its users. In the following we present several use cases for WiFi roaming distinguished along its deployment in private, business, and academia areas.

1.1.1 *WiFi roaming in private households*

In urban areas many households today operate own WiFi networks with own broadband connection to the Internet. Therefore, a relatively cheap solution for the cities to setup areas of wide WiFi coverage with Internet access is to use the availability of these privately operated networks[1]. Setting up such a system would require cooperation among the households in such a way that each cooperation participant who shares own network connection with its guests should also be able to use the connection offered by other participants in response. The initial realization of this approach can be found in Fon[2] which is operated at the commercial basis.

1.1.2 *WiFi roaming in business*

In business area the use of WiFi roaming is especially promising since business relationships among the companies today require employee mobility. Project meetings and cooperative work would benefit from the deployment of the WiFi roaming technology among the companies.

A special use case where the WiFi roaming solution becomes interesting is the business sector of Internet providers. In each country there are usually several providers offering WiFi Internet access to their customers. However, there are only few providers that are capable to establish wide coverage areas. Therefore, many of them focus on specific points of

[1] N. SASTRY, K. SOLLINS, and J. CROWCROFT, 'Architecting Citywide Ubiquitous Wi-Fi Access', *HotNets-VI*, 2007.

[2] Fon, http://www.fon.com

interest, e.g. airports, hotels, etc. Obviously, customers of one provider would benefit from the ability to use the Internet access offered by some other provider. The idea of using WiFi roaming among the Internet providers is comparable to the successfully deployed roaming in mobile telecommunication networks, e.g. GSM.

1.1.3 *WiFi roaming in academia*

In academia, especially in universities and research institutions WiFi roaming technology would provide enormous benefits due to the frequent exchange of research personnel and students. Research stays are often of short duration so that the decrease of the respective administrative overhead appears to be the desired goal. The solution developed by eduroam[3] allows employees or students affiliated to some educational institution which takes part in the cooperation to use the WiFi connection offered by another such institution with the very low administrative overhead.

1.2 *Research challenges in WiFi roaming security and legal liability*

A large number of technical mechanisms and industrial standards developed for (wireless) communication networks offer flexibility for the design of WiFi roaming solutions. However, these mechanisms and standards have been designed to fulfill particular technical tasks and have, therefore, own advantages and shortcomings when deployed in the real world with additional non-technical constraints such as misbehavior of users and legal responsibilities of operators.

It appears to be a challenging research task to design appropriate mechanisms for the realization of WiFi roaming in specific deployment environments such that the final solution is not only practical with respect to technological constraints but also provides sufficient protection against security threats and legal prosecution. Note that protection against these threats deserves especially strong attention due to the increasing misuse of the Internet connections for a variety of illegal activities.

From the security point of view sharing a WiFi connection comprises many risks and threats, both for the network and for the mobile devices. These risks may include traditional denial-of-service attacks, injection of malware, and sniffing of the sensitive information communicated by parties that are involved in the WiFi roaming process. Although in the past many WiFi access points have been configured without requiring any authentication from the connecting devices making the life of intruders easier, nowadays the trend moved towards protected networks for which various technical standards (IEEE 802.1X, 802.11i (WPA)) are available and supported by the majority of the access points and devices.

[3] eduroam, http://www.eduroam.org

Another aspect that has a strong impact on security of WiFi roaming is the trust relationship among the WiFi networks and devices participating in the roaming process. In this context trust means that trusted parties have some pre-agreement concerning certain services that they have previously committed to provide to each other. This makes trust closely related to the ability of participants to authenticate each other before providing the agreed service. Note that well-reasoned trust assumptions between the WiFi networks can be regulated through the adequate legal contracts and contribute to the overall efficiency of WiFi roaming solutions making them more practical, and thus widely acceptable. In general, less trust involves a need for more complex security mechanisms.

Legal issues related to WiFi roaming may arise with respect to the need for identification of end users, formerly established relationship between the respective participating networks, but also related to the drafting of the contractual documents to be concluded between the parties involved in the process. Especially, liability and caution obligations of network owners might represent a serious concern due to the increasing misuse of the Internet by its users, e.g., up- and download activities for the illegal contents including copyright-protected digital information and child pornography. The question raised here is related to the network owners' obligations and liability for allowing access to the Internet through their network. Investigation on potential forms of liability cases and recommendations of protective legal measures represent an interesting interdisciplinary research direction which may involve joint activities of lawyers and technicians.

Another significant research aspect of WiFi roaming worth being payed attention to is that network owners usually have expenses for purchasing their connection bandwidth. Therefore, it appears also important to identify benefits for network owners to share own connection with other parties. The lack of appropriate business models and incentives for network owners to participate in the WiFi roaming process may cause obstacles for a successful deployment of this technology in practice.

1.3 *Focus and organization*

In this paper we identify some general scenarios, use-cases for the deployment of WiFi roaming solutions among different WiFi networks.

The general WiFi roaming problem and notations used throughout the paper are described in Section 2.

In Section 3 we start with the simplistic WiFi roaming approach where an owner of a WiFi network grants a *direct* Internet access to a mobile device which remains under the administrative control of another WiFi network. For this scenario we differentiate between appropriate

security and legal concerns from the perspective of the participating WiFi network and mobile device, describe possible real-life deployment scenarios and sketch business models for the network owner to share own connection, and provide a brief description of technology which could be used for the practical realization. Additionally, we give an overview of currently existing solutions related to this type of WiFi roaming and analyze them with respect to the identified security and legal requirements.

Backed by the identified shortcomings of this naive approach, in Section 4 we focus on a more sophisticated scenario which assumes cooperation of the involved WiFi networks such that a mobile device obtains a *tunnel* access to the WiFi network which has the administrative control over this device. The actual connection to the Internet is then granted to this device from the network at the end of the tunnel. In short, the tunneled connection appears to be promising from the legal point of view. At the same time it involves more participants, and is, therefore, more challenging from the technical point of view. In the context of this tunneled WiFi roaming approach we proceed similar as in the previous case. We discuss various security and legal requirements from the perspective of all participants (this time including the network to which the tunnel is opened) give an overview of possible practical realizations using today's technology, describe and analyze available solutions with respect to the identified security and legal requirements.

We conclude our paper in Section 5 summarizing the advantages and disadvantages of both WiFi roaming approaches from the perspective of security and law.

2 The WiFi roaming problem

2.1 *Definitions*

Throughout this paper we use the following notations. By $N = \{N_1, \ldots, N_n\}$ we denote a set of WiFi networks that may be involved into the roaming agreement. Each network N_i is assumed to be responsible for the administrative control over the set of WiFi access points $AP_i = \{AP_{i,1}, \ldots, AP_{i,p}\}$ and WiFi enabled mobile devices $M_i = \{M_{i,1}, \ldots, M_{i,m}\}$.

An *authentication authority* denoted *AA* is an Internet service that can be questioned in order to authenticate a WiFi network as part of *N*. In the roaming process, it can be used by a guest network to verify the authenticity of the home network N_i of some mobile device $M_{i,k}$. Similarly, *AA* can be used by $M_{i,k}$ or N_i to check whether the guest network N_j is part of *N*. The authentication authority *AA* is assumed to be a trusted in the sense that it correctly authenticates participating WiFi networks. This service is not necessarily centralized; it may be a distributed hierarchy of *AA* servers, each administrated by one of participating networks.

2.2 *Main phases*

The WiFi roaming problem can be abstractly expressed as follows: some device $M_{i,k}$, having a *home network* $N_i \in N$, moves into the area covered by a *guest network* $N_j \in N$ and executes the admission procedure to obtain Internet access. In general, the whole process can be split into two phases described in the following.

2.2.1 *Registration phase*

We consider the *registration phase* as an interactive protocol between $M_{i,k}$ and N_i at the end of which both parties establish some security association (SA), that is $M_{i,k}$ and N_i obtain some information that they can use later to recognize each other as a hosted device and a home network, respectively. We also assume that *AA* is able to authenticate every network from *N*.

2.2.2 *Admission phase*

The actual phase of the WiFi roaming which should be executed between $M_{i,k}$ and a guest network N_j (possibly with the assistance of N_i and/or *AA*) in order to establish the Internet connection for $M_{i,k}$ is called the admission phase. We consider the *admission phase* as an interactive protocol between $M_{i,k}$, N_j, *AA* and N_i, which is invoked by the connection request of $M_{i,k}$ and at the end of which N_j decides whether to accept this request or to decline it. The two key arguments for the decision of N_j are the authentication of N_i as part of *N* and the authentication of $M_{i,k}$ as an actual mobile node registered at N_i.

For the authentication of N_i as a legitimate partner of the roaming agreement, there are three different approaches:

- N_j obtains necessary authentication information directly from $M_{i,k}$ (without interaction with N_i or *AA*).
- N_j obtains necessary authentication information directly from N_i (without interaction with *AA*).
- N_j contacts *AA* which authenticates N_i.

For the authentication of the mobile device $M_{i,k}$ as a device registered at N_i, we consider two approaches :

- N_j obtains necessary authentication information directly from $M_{i,k}$ (without interaction with N_i).
- N_j contacts N_i which authenticates $M_{i,k}$.

Once admission phase has been performed, we distinguish between two scenarios depending on the way by which $M_{i,k}$ is granted access to the Internet. In the first WiFi roaming scenario we deal with considers a *direct*

access, that is the Internet connection to $M_{i,k}$ is granted directly by the guest network N_j. Our second WiFi roaming scenario aims at a *tunnel access* such that N_j opens a tunnel between $M_{i,k}$ and its home network N_i and the actual connection to the Internet is then granted by N_i.

In the following we focus on the analysis of WiFi roaming admission scenarios with direct and tunnel access modes from the perspective of security requirements, various legal aspects, and some practical considerations with respect to the technical realization.

3 WiFi roaming with *direct access*

3.1 *Overview*

Fig. 1 depicts possible steps for the WiFi roaming process in the case of direct Internet access. The mobile device $M_{i,k}$ approaches the guest network N_j and connects to one of its access points $AP_{j,q}$. Then, a global access request is sent to N_j which can decide to accept or refuse it. This decision can be based on either a local authentication decision (steps 2 and 3 are void in this case) or a delegated one. For the delegated one, N_j contacts *AA* to authenticate the mobile home network N_i (step 2). If needed, N_i can be requested to assert that the mobile user does really belong to it (step 3).

We stress that the actual admission protocol may consist of several packet exchanges with intermediate local computations. It could also be possible that during step 2 *AA* exchanges data with the home network N_i in order to supply directly full authentication information to N_j.

$M_{i,k}$ is allowed to access the whole Internet if, at the end of the admission phase, N_j authorizes $M_{i,k}$ to use its own connection. Every subsequent message of $M_{i,k}$ to the Internet and every response will be forwarded by N_j accordingly (steps 4 and 5).

It is worth to notice that any host on the Internet sees $M_{i,k}$ as a host of N_j.

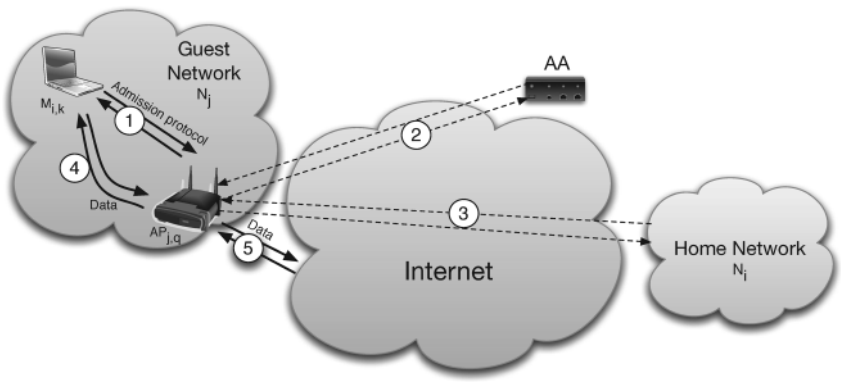

Figure 1. WiFi Roaming with Direct Access

3.2 Trust relationship between participants

The abstract WiFi roaming protocol with direct access to the Internet introduced in the previous section captures different realization scenarios depending on the assumed trust relationship between its participants $M_{i,k}$, N_i, and N_j. In the setting of WiFi roaming with direct access to the Internet we consider trust as a factor used by the guest network N_j in its decision on whether to grant $M_{i,k}$ the Internet access or decline the corresponding request. In fact, we assume that if some sufficient trust relationship between $M_{i,k}$ and N_j can be established then the connection will be granted. By sufficient trust relationship we mean the guarantees that N_j can obtain with respect to the provided roaming service. Hence, there is a link between the establishment of the sufficient trust relationship and the aspects of security and legality. From the security point of view the trust establishment process is closely related to the authentication of the mobile device towards the guest network whereas from the legal point the sufficiency of this trust relationship can be strengthened by the corresponding legal relationship between the guest and the home network.

3.2.1 *Trust relationship between Mi,k and Ni*

In general we assume that there is some pre-established trust relationship between the mobile device $M_{i,k}$ and its home network N_i as a result of the registration phase. In particular, this implies that N_i is aware of the identities of all $M_{i,k}$ and whenever N_i is asked to confirm $M_{i,k}$ as its hosted device it will act accordingly. This includes the case where some $M_{i,k}$ has been revoked by N_i so that after its revocation it loses the status of being a legitimate host of N_i.

3.2.2 *Trust relationship between Nj and Ni*

When dealing with the pre-established trust relationship between N_j and N_i we consider two distinct cases.

The first case assumes that both networks are untrusted, i.e., there is no pre-agreement between N_j and N_i concerning the roaming service. Speaking in terms of identities this case implies that neither N_j nor N_i can identify each other as legitimate partners for the roaming service. For this case we also assume that no third party, such as the authentication authority *AA*, exists that can be used to establish any indirect trust relationship between N_j and N_i. The existence of such *AA* is thinkable in scenarios where N_j and N_i are not aware of each other as roaming partners but have both pre-agreements with *AA* in that they agree to provide the roaming service to any network which also has such pre-agreement with *AA*. In particular, this case where N_j and N_i are treated as untrusted may apply in scenarios where no contracts for the roaming service exist and networks have to decide 'on the fly' whether to provide roaming to $M_{i,k}$ or not.

The second case considers that both networks are trusted, i.e., they share some pre-agreement that regulates the roaming service and are able to identify each other as legitimate partners for the roaming service. This pre-agreement might exist between N_j and N_i directly or via some third party as described before.

3.2.3 *Trust relationship between Mi,k and Nj*

For the WiFi roaming with direct Internet access we assume that whenever $M_{i,k}$ approaches the guest network N_j asking for a connection to the Internet there is no initial trust relationship between them. We consider the establishment of such relationship as the goal of the admission phase.

Whether this goal can be achieved or not depends much on the assumed trust relationship between the networks N_j and N_i. If the corresponding trust relationship is missing, i.e., N_j is not able to identify N_i as a legitimate roaming partner, then it is unlikely for N_j to be able to establish sufficient trust relationship with $M_{i,k}$. This applies in situations where users equipped with mobile devices approach some unknown guest network and ask for the Internet access.

To the contrary existing direct or indirect (via some authentication authority *AA*) trust relationship between N_i an N_j can be used for the establishment of the sufficient trust relationship between $M_{i,k}$ and N_j since one of the goals for N_j during the admission phase would be to identify $M_{i,k}$ as a legal host of N_i. Whether this identification requires assistance of N_i or can be done without any interaction between N_j and N_i is a matter of technical realization. The described case applies in scenarios where an employee of a company that has signed some regulatory contract for WiFi roaming service with another company approaches the network of that second company and requests the Internet connection.

3.3 *Legal aspects*

This first scenario based on a direct access to the Internet bears several legal issues that have to be taken into account to make a correct assessment before thinking about the scenario's actual implementation. The legal issues will obviously be linked to four main issues: liability issues, contractual issues, issues related to telecommunication regulation and data protection issues.

As a principle, one cannot conclude in advance that the direct access scenario will be one bearing more legal issues than the tunnel access scenario described in Chapter 4 of the present contribution. This is why it is of importance to make an in-depth analysis of the legal issues and their consequences at this stage. The same step will then be made for the second scenario (see Section). This will allow a correct comparison at a legal

point of view and allow us to conclude on the risks and opportunities, the pros and cons to implement one or the other proposed scenario in the real world.

In order to be as much comprehensible as possible, we shall subdivide the legal analysis by analyzing separately the four main themes already mentioned: liability issues (1), contract issues (2), telecommunication issues (3), and finally, data protection issues (4).

It is understood that the current paper is limited to a first outline of legal issues. They are being analyzed more in depth in the context of the research project of which this paper is a first result.

3.3.1 *Liability for illegal content*

When technically detailing the direct access scenario, one can easily identify that a high risk for the guest network N_j would be its possible liability in the case of a malicious use of the Internet by $M_{i,k}$. Indeed, as already mentioned, $M_{i,k}$ is seen by any host on the Internet as a host of N_j (see chapter 3.1. above) and not as a host of N_i. Would this mean that N_j will be liable for $M_{i,k}$'s behavior on the Internet? The answer to such question will of course heavily influence a company's decision on granting or not such direct access to an external host. As a principle, and on a European level, the solution is to be found in the so-called 'e-commerce Directive'.[4&5] This Directive states out two important principles regarding the liability and obligations of Internet intermediaries with respect to the information transmitted.

The first principle confirms that no information society provider (e.g. Internet intermediaries) shall be imposed a general obligation to monitor the information which they transmit or store, nor to seek facts or circumstances indicating illegal activity.

The second principle provides for an *exemption of liability* for certain intermediary services providers regarding the information transmitted when their activity is of a mere technical, passive and neutral nature. This exemption only applies to the service providers offering mere conduit, caching and hosting services.

In the direct access scenario examined here, we are of the opinion that the role of the guest network should be considered as a provider of mere conduit services. Indeed, under article 12 of the e-commerce Directive, a mere conduit service is defined as an

---

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal*, L 178, 17/07/2000, pp. 1-16.

[5] In Belgium, this Directive has been transposed in the Belgian Law on e-commerce of 11 March 2003 : la Loi du 11 mars 2003 (http://mineco.fgov.be/information_society/e-commerce/legislation/regulation/law_e_commerce_001.pdf) sur certains aspects juridiques des services de la société de l'information - *M. B.*, 17/03/2003.

'*information society service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*'.

The 'e-commerce Directive' provides that providers of such a mere conduit services shall not be liable for the information transmitted, provided that the provider:

1. does not initiate the transmission;
2. does not select the receiver of the transmission; and
3. does not select or modify the information contained in the transmission.

If all these conditions are met, the service provider - the guest network - will *not be liable* for the information transmitted, up and downloaded through its Wi-Fi access point by the user of the roaming services.[6] However, the Directive (and the Belgian law on e-commerce) also provides that this limitation of liability is without prejudice to the possibility for courts or national authorities of requiring the Service provider to terminate or prevent an infringement. Should this occurs, the guest network will of course be obliged to have an active control on $M_{i,k}$'s activity when using it's WiFi access point (e.g. by setting up a filtering system allowing to block access to some content).

3.3.2 *Contractual issues*

Trust and legal relationship between the networks N_i and N_j Neither statutory provision nor legal principles oblige different parties involved in a project to conclude an agreement in order to set out the legal basis of their relationship.[7] However, with respect to the trust relationships as described in the direct access scenario, one would argue that the existence of a pre-existing legal relationship between both networks would be an asset in order to precise the rights and obligations of these networks regarding the access that they mutually decided to offer to each other.

Indeed, the liabilities and obligations of both networks regarding, among others, the grant of access, SLA, prevention of hacking, data retention or appropriate diligence should be clearly stated in a binding document, in order to establish the specific roles of each network within the roaming system.

[6] The same reasoning can be applied for the liability of the home network: we also assume that its role can be limited to providing a mere conduit service and that it will then also benefit from the general liability exemption rule detailed above.

[7] Except in the case of the processing of personal data on behalf of another person considered as the controller of the processed data. In this case, the Data protection law requires that the parties conclude a written agreement stating out the obligations that must be followed by the processor.

In addition to the legal advantage of having a legally binding document between all parties involved, the technical specifications allowing N_j to recognize $M_{i,k}$ as an authorized user should also be gathered in a written document that should be accepted in advance by any involved party: this could allow $M_{i,k}$ to be certain that he can access the Internet through any guest network every time and at the sole condition that $M_{i,k}$ complies with the specifications established by the roaming procedure.

These specifications can also be made publicly available on the Internet, so that anyone can implement them on its hardware device to be able, technically, to access the Internet through a guest network. However, choosing this option will not necessarily lead to a legally binding obligation for the guest network to accept all potential end-users to access the Internet through their WiFi network.

Therefore, without a legally binding document between the networks at stake, the end-users of mobile devices cannot be guaranteed that they will be given access to the guest network, even if they meet all the specific requirements put forward to take part in the roaming network. This is still another point pleading for the existence of pre-existing agreements between the networks involved.

As already said here above, the relationship (also called the 'trust relationship') can either be performed by means of mutual agreements between every network operator, or by asking a third legal entity (AA) to conclude separate contracts with each operator.

This last option seems easier to set up since the operators do not have to know each other before granting mutual access to their respective networks. The third party (AA) could intervene as a trusted party whose function would be to make sure that pre-existing agreements exist between all networks that wish to participate in the roaming project. This way, any member of the participating networks could have the certainty to be able to access the other networks involved since proper binding documents are accepted by all the networks.

These documents shall therefore be enforceable by the trusted party (AA) towards the participating networks: (AA) shall be entitled to claim before a Court that the networks meet the technical, legal and operational requirements stated out in the document.

One can also imagine - through an appropriate clause - giving the home networks the right to take legal action towards the guest networks in case of violation of their roaming obligations. Therefore, N_i would no longer be obliged to address itself to (AA) in order to get the enforcement of N_j's obligations.

Legal relationship between $M_{i,k}$ and networks N_i and N_j It might happen that a document relating to the permitted and prohibited use of the Internet and the access to the home network already exist between the home network and its device $M_{i,k}$. This document can be e.g. an

employment agreement, which is a legally binding agreement where all rights and obligations of the employers and the employees are stated.

Therefore, $M_{i,k}$ could already be subject to an Internet and network use policy imposed by its home network N_i. In order to precise what usage will be allowed regarding the WiFi roaming solution, N_i could precise in this pre-existing document the conditions under which $M_{i,k}$ will be authorized to access a guest network. These precisions can for example consist of the obligation to use a hardware approved by N_i before accessing a guest network.

With respect to the need of an agreement between $M_{i,k}$ and the network N_j, we do not think that such an agreement is necessary since both networks can already rely on an existing document (either a bilateral agreement or a document signed with a third party (AA)) to make sure that their devices can access to other guest networks.

Specific contractual issues Some Internet providers' terms and conditions prohibit the resale or public distribution of the internet connection provided to the end user. Allowing third people to access the Internet via a WiFi connection could therefore constitute a breach of this contractual prohibition. As a consequence, the guest network N_j could be liable for breach of contract and its Internet provider could accordingly decide to disconnect N_j for non-compliance with the Internet access terms and conditions. Moreover, N_i and $M_{i,k}$ could also be held liable for contributory breach of contract in case they were aware of the prohibition to share N_i's internet access.

In order to avoid such a risk, the legal document binding the parties should impose the participating networks to warranty that they are allowed by their access provider to share their Internet access with users other than the regular members of Nj.

3.3.3 *Liability issues*

Providing a WiFi access through one's network is an activity that can raise some liability issues since potential hackers or end users can try to benefit from the network of roaming party in order to attack the system of another roaming party. We will hereunder resume the key elements of the civil liability regime in order to understand what risks are at stake in the course of the sharing of a WiFi network connection.

As general liability principle, a rule of reasonable prudence and diligence (a so-called 'duty of care') has to be observed by any person or entity in the course of its activities. The level of caution and prudence that has to be met depends on the risks and the nature of the activity. A lack of such caution and diligence shall be considered as a fault according to civil liability law. Obviously, regarding activities such as granting access to WiFi networks, the duty of care should be focused on security of the network.

As a consequence, networks operators can be held liable for any damage that is the consequence of a lack of precaution (such as, among others, apparent breach in the security system, or bad administration of the system) and that would not have occurred if appropriate measures were implemented.

Therefore, in order to identify precisely which network will have to take specific measures in order to avoid potential damages and security risks, proper specifications should be drafted in order to incorporate them into the documents legally binding towards the involved networks and referred to hereunder.

3.3.4 *Telecommunication issues*

A specific European regulatory framework[8] covers economic activities in the field of electronic communications (i.e. the conveyance of signals by electromagnetic means). This framework must be transposed in national laws. In Belgium it is (mainly[9]) transposed into the federal Law of 13 June 2005 on electronic communications.[10]

According to this (European and Belgian) regulatory framework for electronic communications, an *electronic communications network* means

> 'transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means,

[8] Mainly composed of six directives: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), *OJ* L 108, 24.4.2002, p. 33-50; Commission Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communications networks and services, OJ L 249, 17.9.2002, p. 21-26; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), *OJ* L 108, 24.4.2002, p. 21-32; Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), *OJ* L 108, 24.4.2002, p. 7-20; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), *OJ* L 108, 24.4.2002, p. 51-77; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201, 31.7.2002, p. 37-47, as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13.4.2006, p. 54-63.

[9] We have here to notice that the (cultural) Communities also play a legislative role in the field of electronic communications. They are indeed competent regarding broadcasting contents and the transmission of broadcasting signals while the federal State regulates other forms of transmission by electromagnetic means.

[10] Loi du 13 juin 2005 relative aux communications électroniques, M.B., 20 June 2005, 2nd ed. On this federal level are some parts of the Law of 21 March 1991 (M.B., 27 March 1991) still in application. If these two laws rule the market, the Belgian federal regulatory authority (IBPT) is mainly organized by a law of 17 January 2003 (*M.B.*, 24 January 2003, 3rd ed., err. 4 June 2003).

including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed'.

As an *electronic communications service* means

'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services […]'.

On this basis we can conclude that providing access to a WiFi network could imply the provision of an *electronic communications service* consisting in the conveyance of signals by means of an *electronic communications network*.

General authorization The national regulation may foresee a number of general conditions to be fulfilled by those who want to provide electronic communications services and to operate electronic communications networks. However these activities do not require any individual right but may only be subject to a 'general authorization'. This means that such economic activity may only require a prior notification and of course the respect of the regulation. A specific and individual authorizing decision from the regulatory authorities is therefore not needed.[11]

Promoting R-LANs The European Commission adopted a Recommendation in March 2003[12] urging to facilitate the use of WiFi networks or the so called Radio Local Area Networks (R-LANs) and therefore to allow the provision of R-LAN access to public electronic communications networks and services on a commercial basis under the least onerous system, i.e., to the extent possible without any specific conditions.

Public or private communications services or networks The regulatory framework at stake and the rules related to general authorization apply to all electronic communications and networks, whether public or private. This does not mean that the same conditions are applied to both categories. Indeed, in the case of networks and services not provided to the public it

[11] See nevertheless the comments made hereunder regarding rights of use for radio frequencies.

[12] Recommendation 2003/203 of 20 March 2003 on the harmonization of the provision of public R-LAN access to public electronic communications networks and services in the Community, *OJEU*, L 078 of 25 March 2003. A recommendation is not formally binding for the Member States (see art 249 EC Treaty). It has however a certain legal consequences. In the case of this Recommendation based on article 19 of the Framework Directive the Member States have in particular to ensure that national regulatory authorities take the utmost account of it in carrying out their tasks. And where a national regulatory authority chooses not to follow a recommendation, it has to inform the Commission giving the reasoning for its position.

is appropriate to impose fewer and lighter conditions than are justified for electronic communications networks and services provided to the public.[13] A general overview of the regulation makes clear that the number of conditions applicable to private activities is limited.[14] Only few conditions can be attached to a general authorization to provide private services[15]: the payment of an eventual administrative tax; the obligation to respect the environment, or town and country planning rules; and the obligation to ensure safety, security and continuity of the network.

In this context we note that Belgium made use of the possibility to exempt some electronic communications activities from prior notification and therefore from most of the obligations linked to this notification. This is first the case with the operation of networks that don't cross the public domain.[16]

It should furthermore be emphasized that specific obligations may be imposed on providers of electronic communications services and networks e.g. with regard to universal service or with regard to the provision of access (including interconnection) with one own resources. The latter obligations nevertheless only apply to providers of public electronic communications networks.

As a consequence it appears that the qualification of a network (and of the service provided through this network) as public or not is of crucial importance.

In accordance with the Framework Directive, public communications network means an

> '*electronic communications network used wholly or mainly for the provision of publicly available electronic communications services*'.

The term of public is not explicitly defined in the regulatory framework but the European Commission gave in 1995 some guidance on this concept.[17] According to the Commission, 'for the public' must be understood in its common sense meaning of 'available to all members of the public on the same basis'. Working than on an *a contrario* reasoning she rather defined what is not public. In this approach are for examples not for the public the corporate networks (connecting a company and its subsidiaries or its branches) and the closed user groups (CUGs).[18] A CUG is a group

---

[13] Authorisation Directive, recital 16.

[14] P. NIHOUL, P. RODFORD, EU Electronic Communications Law - Competition and Regulation in the European Telecommunications Market, *OUP*, 2004, p. 115, 2.136.

[15] See Authorisation Directive, Annex, Letter A, points 2, 5, 7, 11, 12, 13, 15 and 16.

[16] Law of 13 June 2005 on electronic communications, art. 9, §5.

[17] See Communication by the Commission to the European Parliament and the Council on the status and implementation of Directive 90/388/EEC on competition in the markets for telecommunications services, *OJ*, C 275, 20 October 1995, p. 5. The idea than developed may still considered useful today.

[18] Ibid. at 8. For further explanations on these networks in particular (in the context of voice telephony), see P. LAROUCHE, *Competition Law and Regulation in European Telecommunications*, Hart Publishing, 2000, 10-14 and 24-26.

formed by members who have an economic relationship or a common interest which is pre-existing, extraneous to their actual telecommunication needs. The public nature of the service does however not depend on which information the user will have access to: Internet, local network.

We have to keep in mind that this qualification (public or not) has to be clearly distinguished to another one: the existence of remuneration.[19] This criterion is essential for the qualification of electronic communications service and thus the application of the whole regulatory framework which only covers economic activities as a secondary legislation of the EC Treaty. It should be noted that these services do not necessarily have to be paid for by the person for whom they are performed.[20] The essential characteristic of remuneration 'lies in the fact that it constitutes consideration for the service in question, and is normally agreed upon between the provider and the recipient of the service'.[21] Thereby in the case of an exchange relationship (in which the partners would mutually give access to each other's network), one could be considered that access is given against payments which compensate each other.

As a preliminary conclusion to the analysis made above, it appears that the exact qualification of the network and the precise legal position of the person who would open his WiFi access points to outside users with direct access to internet and to the operator of the backbone network will mostly depend on the concrete implementation of the WiFi roaming: would the service be provided against payment, would the access be open to anyone?

Consequently it is our impression that provided that the service is offered for remuneration (what is *a priori* not decided), this direct access scenario could be considered as a 'public network scenario': The group of different persons who would open up their respective networks seem not to be subsidiary to a single corporation activity neither to a CGU. The users which could have access to the WiFi network are not limited in advance to a certain category of beneficiaries. In our understanding a service could be considered as provided to anyone even if all these persons are asked to fill in a prior registration. This registration could in fact be open to everyone interested in this service (and who agree with the terms of use thereof) and would as such not limit the circle of persons admitted to the service.

Each WiFi network could individually be used for the provision of publicly available electronic communications services. But to conclude that these networks are also to be qualified as public, we have first to determine their main use: private or public.

---

[19] See the definition of the electronic communications service hereabove.

[20] See K. LENAERTS and PIET VAN NUFFEL, *Constitutional Law of the European Union (2nd ed.)*, Thomson, Sweet & Maxwell, London, 2005, 227.

[21] European Court of Justice, Case 283/86 *Humbel*, 27 September 1988, para. 17.

Use of radio-frequencies In addition to the general authorization, the European regulatory framework allows Member States to make the use of radio frequencies subject to the grant individual rights of use. The allocation of this kind of resources needs to be strictly managed because of the need to ensure the efficient use of such scarce resource and of the possible existence of technical problems like harmful interferences.

Nevertheless in order to not increase the administrative burden upon potential network operators such individual rights of use may only be required when necessary. Member States are thus required, where possible, and in particular where the risk of harmful interference is negligible, not to make the use of radio frequencies subject to the grant of individual rights of use. Such considerations have led the European Commission to recommend that the use of available 2.4 and 5 Ghz bands[22] should not be subject to the grant of individual rights for the operation of R-LAN systems[23]. The conditions for usage of such radio frequencies will in such case be included in the general authorization. This license-free use is a clear advantage of WiFi networks that participates in the success of this wireless communication standard.

3.3.5 *Data protection issues*

Processing personal data The issues to be tackled regarding data protection are mainly to identify whether one or another party is actually *processing personal data* during the 'direct access' process. Such processing needs indeed to be performed in accordance with the national rules transposing the general Data Protection Directive 95/46.[24]

The analysis of the first scenario allows us to conclude that - what the guest network concerns - some *personal data* are being *processed*[25] during the

[22] R-LAN may use all or part of either the 2400,0 - 2483,5 MHz or the 5150-5350 MHz or 5470-5725 MHz bands. The Commission decided to make these two last frequency bands available in all Member States for wireless access systems (see Commission Decision 2005/513/EC of 11 July 2005 n the harmonized use of radio spectrum in the 5 GHz frequency band for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs), *OJ*, L 238 of 15 September 2005, as amended by Commission Decision 2007/90/EC of 12 February 2007, *OJ*, L 41 of 13 February 2007, p. 10). This decision is implemented in Belgian national law by Ministerial Decree of 22 December 2004 amending Ministerial Decree of 19 October 1979 relating to private radio-communications, annex 3 (interface radio B3), *M.B.*, 7 January 2005.

[23] See the above mentioned R-LAN recommendation, point 1 and recital 9. Belgium followed this recommendation by adopting the Royal Decree of 13 February 2003 amending the Royal Decree of 15 October 1979 relating to private radio-communications, *M.B.*, 14 April 2003. This Decree exempts the use of these frequencies from any right of use. Earlier mentioned Ministerial Decree of 22 December 2004 (see previous footnote) in his annex 3 furthermore submits this to limited general conditions (maximum effective isotropic power, inside use only for the 5470-5725MHz band etc.).

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281, 23.11.1995, p. 31-50.

[25] 'Processing of personal data' *shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*; Article 1 of Directive 95/46/EC.

admission phase.[26] *Personal data* can indeed be defined as being *any information relating to an identified or identifiable natural person ('data subject')*[27]. An identifiable person is *one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

On the basis of these definitions, one can understand that during the admission phase personal data is exchanged between N_j and $M_{i,k}$. Even if this information is not directly the name of the user of $M_{i,k}$, it however allows the identification of this person quite easily: the information exchanged, even with cryptography, contains enough elements to identify precisely a device $M_{i,k}$ which can be linked to its user by N_j.[28]

In this direct access scenario, personal data is also exchanged at the time $M_{i,k}$ is accessing the Internet. At least traffic data is indeed processed by N_j as the messages of $M_{i,k}$ to the Internet and every response need to be forwarded by N_j accordingly.

As a conclusion, one can identify two personal data processing operations that will be identified by using their purpose: the *admission processing* and - what we will call - the '*web surfing*' *processing*.

Both these processing operations shall have to be performed according to the obligations of the Data Protection Directive 95/46. This mainly includes the obligation to specify the purpose of the processing (as just has been done). This aim has to be legitimate and the data may not be further processed in a way incompatible with those purposes. The person responsible for the processing (the so-called 'controller' - N_j in this case) shall have to verify whether the processing is legitimate, deliver some information to the data subject (the user of $M_{i,k}$), notify the processing to the National Data Protection Authority, comply with obligations relating to the quality of the processed data and, comply with security and confidentiality obligations.

Data retention Another legal issue is to precisely determine what are the obligations of N_j as regards the retention of traffic data. Indeed, one should notice that a European Directive on data retention has been adopted on 15 March 2006.[29] This Directive provides that Member States have to adopt measures to ensure that some data (specified in Article 5 of the Directive) are retained when they are *generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications*

[26] Please notice that personal data is of course processed during the registration phase. As this processing is however not different from the processing of personal data performed by the home network for the management of the access to the Internet and/or the Intranet of the home network by $M_{i,k}$ when working intra muros, we did not analyse this question in the present paper.

[27] Article 1 of Directive 95/46/EC

[28] Please notice that the link does not have necessarily to be made by N_j.

[29] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

services concerned.[30] The data at stake is traffic and location data on both legal entities and natural persons and the related data necessary to identify the subscriber or registered user.[31] The purpose of such retention has however been restricted to the use of such data *for the purpose of the investigation, detection and prosecution of serious crime.*[32] The data may be provided only to the competent national authorities in specific cases and in accordance to the law.

Therefore, in this direct access scenario, we can observe that the main question is to determine whether N_j can be considered as being a *provider of* publicly *available electronic communications services* and would hence be obliged to retain some data within a period of retention that shall be not less than six months and not more than two years from the date of the communication.[33]

According to the European Directive, the data to be retained will then be data a) necessary to trace and identify the source of a communication; b) data necessary to identify the destination of a communication; c) data necessary to identify the date, time and duration of a communication; d) data necessary to identify the type of communication; e) data necessary to identify users' communication equipment or what purports to be their equipment; f) data necessary to identify the location of mobile communication equipment.[34] The Directive precisely determines which data should be retained concerning Internet access, Internet e-mail and Internet telephony.

One shall notice that in Belgium, the European Directive has not been transposed yet. The Belgian law has however tackled the issue of data retention providing for a general rule in the Law of 13 June 2005 on electronic communications. This rule, applicable only to the so-called 'operators', provides that some traffic and users' identification data must be retained *for the prosecution and suppression of penal offences in the framework of the search for […] the identity of people having maliciously used an electronic network or an electronic communication service.*[35] The data - that has to be specified in a Royal Decree executing the law - may be retained for a period of minimum 12 months and maximum 36 months. The Royal Decree however does not exist.

The Belgian law thereby foresees in certain circumstances that 'non operators' could also have the obligation to register and keep traffic and user's identification data for *the prosecution and suppression of penal offences […].*[36] The law is however not specifying in this case a minimum and

[30] Article 3 of Directive 2006/24/EC

[31] The Directive is explicitly excluding the content of electronic communications, including information consulted using an electronic communications network. (article 1)

[32] Article 1 of Directive 2006/24/EC

[33] Article 6 of Directive 2006/24/EC

[34] Article 5 of Directive 2006/24/EC

[35] Article 126 of the Law of 13 June 2005 on electronic communications.

[36] Article 9 §7 of the Law of 13 June 2005.

maximum period of retention. Everything should be fixed by Royal Decree - Royal Decree that has not been adopted yet.

As all Royal Decrees are missing, one shall notice that excepting the fact that some data must be retained by operators, it is difficult to have more certainty and more precise knowledge about the kind of data to be retained and for which period of time. Reference should then best be made to the data described in the Data retention Directive 2006/24 (see above).

3.4 *Security aspects*

In this section we describe the main security concerns for the WiFi roaming scenario with the direct access to the Internet provided by the guest network N_j to a mobile device $M_{i,k}$. We classify security goals from the perspective of the involved communication participants.

3.4.1 *Device-oriented security goals*

Mobile device $M_{i,k}$ is interested in obtaining own connection to the Internet. Therefore, it is less concerned about the authenticity of the guest network N_j as long as it can use the provided roaming service in order to execute remote applications. One of the problems that arises in this context is that if N_j is malicious then it can try to eavesdrop the subsequent communication of $M_{i,k}$. Eavesdropping is a passive attack which is possible due to the ability of N_j to observe traffic within its infrastructure. This problem is especially appealing if the mobile device uses the established connection to transmit some valuable sensitive information (e.g. login credentials to access some application). Obviously, this is a threat against the confidentiality of the established communication channel. However, the same threat applies after the information leaves the infrastructure of N_j towards the specified destination on the Internet. Therefore, achieving confidentiality in case of the direct access to the Internet should not be seen as a requirement of the deployed WiFi roaming solution but rather as the requirement of the application which uses the established communication channel.

Another threat for $M_{i,k}$ arises from possible active attacks performed by N_j such as traffic redirection resulting from the modification of the server's address resolution or packets exchanged with $M_{i,k}$ aiming to spoof some destination address on the Internet. For example, if the user behind the mobile device $M_{i,k}$ uses the established connection to access an e-mail account on some server on the Internet the guest network N_j may try to spoof the destination address of that server in order to obtain login information of the user and misuse it later for the distribution of spam. Therefore, if a mobile device accesses some server on the Internet it should be able to verify that the corresponding destination address is authentic and

that the server is not spoofed by N_j. Note that spoofing (and phishing) attacks on the Internet are general security threats that are independent of the actual WiFi roaming service. Therefore, similar to the requirement on confidentiality, the corresponding protection against spoofing attacks (through the deployment of authentication mechanisms between the mobile devices and Internet servers) are not integer to a concrete WiFi roaming security solution.

However, we stress that the responsibility for the recognition of potential spoofing and impersonation attacks to $M_{i,k}$ (or to the user who owns this device) should be considered by the application running on top of the established connection. The application could deploy classical authentication techniques such as TLS-secured communication in order to achieve the requirements on authentication and confidentiality, i.e. to establish a secure end-to-end communication channel. Unfortunately, the majority of servers on the Internet today do not realize them in a sufficient form so that the number of successful impersonation and eavesdropping attacks has increased over the past years.

A more severe damage that can be caused by a malicious guest network N_j is that it may try to impersonate $M_{i,k}$ towards some server on the Internet and perform illegal activities on behalf of $M_{i,k}$ so that the owner of the mobile device can be blamed for having performed these activities. It is important to mention here that the issue whether $M_{i,k}$ can be blamed or not should be understood in the context of the legal liability. In fact it depends on the type of the evidence which should be provided in order to blame $M_{i,k}$ for some illegal activities. Several types of evidence can be used in practice. First and probably the most secure one is to deploy certain cryptographic authentication mechanisms such as digital signatures. In this case the evidence can be given in form of a digital signature generated by a mobile device upon the establishment of the connection on some information specific to that connection. This information may include the source and the destination address from the connection request in addition to the time stamps that indicate the time when the connection has been established. Obviously, a successful impersonation attack of N_j against $M_{i,k}$ and subsequent accusations against $M_{i,k}$ would depend much on the ability of the guest network to forge the corresponding digital signature of the device. Another solution, which is less secure, but enjoys popularity in the GSM roaming, is to log details about the established connections without using cryptography and to use the data from the log files for the identification of devices (and their owners) in the case of misuse. Obviously, this solution does not prevent malicious N_j from successfully modifying the logged data.

Another related threat arises in case that some contractual pre-agreement concerning the WiFi roaming service between N_j and N_i exists and the admission phase is interactive in the sense that N_i has to confirm that

$M_{i,k}$ is one of its hosts. Then, N_j may also try to impersonate $M_{i,k}$ towards N_i, thus making the home network believe that one of its hosts requested the roaming service from N_j when in fact no such request has been done. This can be seen as a security risk, especially, if the pre-agreement foresees payments for using the WiFi roaming service as in this case N_j may try to charge N_i for the unprovided service. In general both described attack scenarios can be classified as impersonation attacks against the mobile device for the only difference that in the latter case $M_{i,k}$ is impersonated towards its home network N_i and not just to some server on the Internet. Obviously, a secure WiFi roaming solution upon the execution of its admission phase should prevent attacks that impersonate some mobile device $M_{i,k}$ towards its home network N_i.

3.4.2 *Guest Network-oriented security goals*

One of the main goals for the guest network N_j upon providing the WiFi roaming service to $M_{i,k}$ is to prevent possible liability blames for the illegal activities on the Internet that have been performed by $M_{i,k}$. In order to achieve this protection N_j should obtain some proof during the admission phase that would enable N_j to shift the responsibility for any misuse performed by $M_{i,k}$ to its owner. Note that the form of this proof depends on the legal framework which applies to the WiFi roaming service and can be realized via cryptographic authentication mechanisms such as digital signatures or through the corresponding logging of the information related to the established connection between $M_{i,k}$ and the destinations on the Internet. In some sense, this goal can be seen as a counter-part of the device oriented goal on prevention of impersonation attacks against $M_{i,k}$.

Another important security risk for the guest network N_j is when a malicious device $M_{i,k}$ wishes to harm the infrastructure of N_j. This includes possible infiltrations with malware as well as the risk of the Denial-of-Service (DoS) attacks. The infiltration with malware is rather independent of the actual WiFi roaming solution and can be prevented using standard access filtering techniques. As for the DoS attacks we distinguish between two types: attacks against the general infrastructure of N_j and attacks against the infrastructure which is responsible for the WiFi roaming service, e.g. the access points $AP_{j,q}$. Note that in case of the direct access malicious $M_{i,k}$ can address its messages also to any server which belongs to the infrastructure of N_j so that possible DoS attacks against these servers should be prevented through the additional filtering mechanisms. Obviously, this protection cannot be performed within the actual WiFi roaming admission protocol. On the other hand, DoS attacks against the WiFi roaming infrastructure such as attacks that aim to crash some access point $AP_{j,q}$ should be prevented by the deployed WiFi roaming admission protocol.

3.4.3 *Home Network-oriented security goals*

In case of WiFi roaming with direct access to the Internet the home network N_i becomes active only if some WiFi roaming pre-agreement exists which includes N_j (and also N_i if the admission phase requires additional interaction between N_j and N_i). The main purpose of this interaction could be the wish of N_j to obtain confirmation from N_i that $M_{i,k}$ belongs to N_i and is eligible to use the provided WiFi roaming service. In this sense, the main threat for the home network N_i arises from possible impersonation attacks during such admission phase. However, these attacks are already considered within the specified device oriented security goal concerning the impersonation of $M_{i,k}$. If there is no pre-agreement between N_j and N_i or if the admission phase does not require interaction with N_i then no active participation of N_i is necessary. Therefore, there are no further security threats which are specific to N_i. Note that this is one of the main differences compared to the security concerns of N_i in case of WiFi roaming with tunnel access to the Internet.

3.5 *Practical realization*

This part describes mechanisms that can be used to realize wireless roaming with direct access. The whole solution can be divided into three building blocks. The first block deals with link-layer authorization and the security between the mobile node and the access point. The second block concerns the authentication of the mobile device and its home network. And finally, the third block is responsible for the full Internet access for the mobile device.

3.5.1 *Link-layer authorization and security*

For authentication and authorization at link layer, a commonly used solution is the IEEE standard 802.1X[37]. It prevents the mobile to send any data packet as soon as it has not been authorized. Authorization is based on authentication and local policy. In our direct access case, we typically accept any authenticated mobile from an authenticated partner network. WPA (Wi-Fi Protected Access[38]) should be used in conjunction with 802.1X so that all the communication between $M_{i,k}$ and $AP_{j,q}$ is encrypted.

3.5.2 *Authentication*

In our situation, the authentication has to be performed with the contribution of a third party, using a protocol such as RADIUS[39]. Since we have to authenticate the home network as well as the mobile identity, the

[37] *802.1x-2004 IEEE standard for local and metropolitan area networks – Port-Based Network Access Control*, IEEE, 2004.

[38] *802.11i-2004 IEEE Standard. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements.* IEEE, 2004.

[39] C. RIGNEY, S. WILLENS, A. RUBENS, and W. SIMPSON, 'Remote Authentication Dial In User Service (RADIUS)', *RFC 2138*, IETF, June 2000.

authentication can be either performed by two different operations or by a single one using a RADIUS server hierarchy. Such kind of authentication is usually mutual and use protocols such as EAP-TLS.[40]

3.5.3 *Internet access for the mobile node*

In the direct case, the mobile node, once authenticated, receives an IP address of the guest network via DHCP[41&42] or ND.[43] Then, the full Internet access of the mobile node is simply provided by forwarding its packets to the Internet. In order to avoid $M_{i,k}$ accessing the guest network service with full access rights, appropriate firewall rules should be applied.

3.5.4 *Technical issues*

In addition to the legal issues of the direct access solution, some technical risks also appear. The IP address used by the mobile node to connect to another host of the Internet is an IP address belonging to the guest network. The visiting host is thus associated to its guest network. For instance, if the guest network has an access to a digital library based on its IP address, the mobile will also have access. Even if the visitor is authenticated, the action he performs on the Internet may have important consequences for the guest network. If $M_{i,k}$ sends spam through the Internet, N_j might be considered as a spam-sender network, that is put into the blacklist databases and possibly prevented from sending any e-mail.

3.6 *Existing solutions*

There exist several initiatives that suggest solutions for WiFi roaming with direct Internet access. These solutions can be classified in two main categories: Roaming with local authentication (step 2 in Fig. 1 is void in this case) and roaming with delegated authentication. We will not consider a connection to open WiFi networks as a roaming situation.

3.6.1 *Roaming with 'local authentication'*

Local authentication is the most spread and simplest way to implement WiFi roaming, for instance this type of authentication is frequently used in WiFi networks offered by the hotels as well as for other public hotspots, e.g. in the airports. Local authentication can be either offline (e.g. with username/password as in many hotels) or online (e.g. using credit cards or similar payment methods).

---

[40] B. ABOBA and D. SIMON, 'PPP EAP TLS Authentication Protocol', *RFC 2716*, IETF, Oct. 1999.

[41] R. DROMS, 'Dynamic Host Configuration Protocol' *RFC 2131*, IETF, Mar. 1997.

[42] R. DROMS, J. BOUND, B. VOLZ, T. LEMON, C. PERKINS, and M. CARNEY, 'Dynamic Host Configuration Protocol for IPv6 (DHCPv6)', *RFC 3315*, IETF, July 2003.

[43] T. NARTEN, E. NORDMARK, and W. SIMPSON, 'Neighbor discovery for IP Version 6 (IPv6)', *RFC 2461*, IETF, Dec. 1998.

3.6.2 *Roaming with 'delegated authentication'*

There exist several solutions which deploy the concept of delegated authentication. For instance, Fon[2] runs on a commercial basis selling own WiFi routers that mediate the authentication of mobile devices wishing to obtain connectivity from a WiFi network to a FON server. FON routers split the WiFi signal creating a secure private channel to broadband internet and a separate channel to be shared with the other users. However, Fon has several security threats[44] - in particular the deployed address filter technique allows impersonation attacks by spoofing the corresponding addresses.

Wisher[45], another commercial WiFi roaming provider, requires guest networks to distribute WEP/WPA keys to authorized guests. Obviously, this is an even riskier approach than Fon since it requires strong trust relationship that guests do not redistribute the obtained keys.

There are several solutions developed for the WiFi roaming in national research and education networks in Europe by the TERENA Task Force on Mobility.[46] The most promising of the proposed solutions is eduroam[3] based on 802.1X authentication and RADIUS-server hierarchy. It deploys the federated approach where networks become members of a federation through some initial (possibly off-line) contractual agreement. Although member networks share some level of trust, they retain their own administrative control. In eduroam the initial account of a mobile device is created at its home network, and whenever this device wishes to connect to another network its credentials are routed to the responsible RADIUS-server of the home network which replies with the authentication result. Unfortunately, this service is only offered in research and education networks.

4 WiFi roaming with *tunnel access*

4.1 *Overview*

The possible steps of a WiFi roaming process with the tunnel access to the Internet are depicted in Fig. 2. The mobile device $M_{i,k}$ approaches the guest network N_j and connects to one of its access points ($AP_{j,q}$). Then, $M_{i,k}$ requests that N_j creates a tunnel to its own home network, N_i. This request (step 1), has at least to contain the information about the home network, e.g. its identity.

[44] F. BJÖRCK, 'Fon security scenarios', http://www.bjorck.com/fon-security-scenarios.htm, January 2007.

[45] Wisher, http://www.wisher.com

[46] TERENA TF on Mobility, http://www.terena.org/activities/tf-mobility/

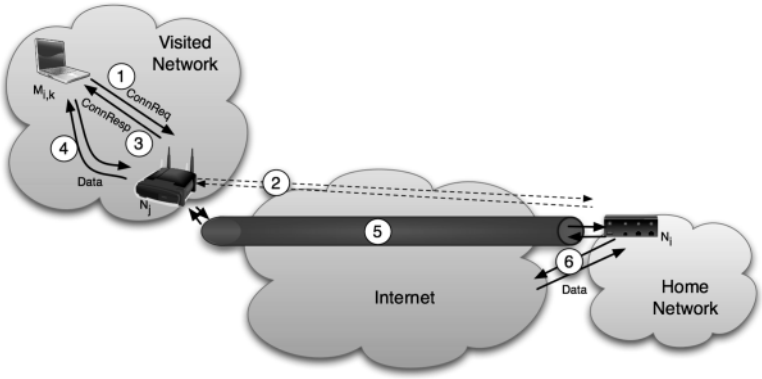

Figure 2. WiFi Roaming with Tunnel Access

The authentication with N_j is similar to the one in the direct case. Moreover, N_i has to authenticate and authorize $M_{i,k}$ to use a tunnel to access the Internet through its network. If the request is accepted, we can consider that a tunnel is opened between N_j and N_i for $M_{i,k}$.

We stress that the security protocols executed between AA, N_j, N_i, and $M_{i,k}$ do not necessarily consist of a single message exchange. They may contain more complex exchanges with intermediate local computations. They may also be useless in some cases where some information is implicitly known (using cache for instance). Through the opened tunnel, the mobile device $M_{i,k}$ can connect to the whole Internet. The data packets sent from $M_{i,k}$ (step 4) are tunneled to its home network N_i (step 5), and then forwarded to the destination server on the Internet (step 6). For any such server, $M_{i,k}$'s packets are delivered by N_i and the reverse traffic to $M_{i,k}$ is sent first to N_i and then tunneled to the device via N_j.

4.2 Trust relationship between participants

The actual realization of the previously introduced abstract WiFi roaming protocol with tunnel access to the Internet may also depend on the assumed trust relationship between $M_{i,k}$, N_i, and N_j. In this setting the notion of trust can be seen as a factor used by the guest network N_j in its decision on whether to grant $M_{i,k}$ the tunnel access to the claimed home network N_i or not. Similar to the WiFi roaming case with direct Internet access the establishment of some sufficient trust relationship between $M_{i,k}$ and N_j is necessary for the granted tunnel connection. This sufficient trust relationship that can be substantiated prior to the roaming process through adequate legally binding documents (in a manner that is still to be defined, according to the decision to create a new legal entity or not) and established during the admission phase by some authentication

mechanisms which should provide N_j with guarantees with respect to the roaming service.

4.2.1 *Trust relationship between $M_{i,k}$ and N_i*

As in the WiFi roaming case with direct Internet access we assume that some pre-established trust relationship between the mobile device $M_{i,k}$ and its home network N_i exists as a result of the registration phase. Therefore, it is likely that N_i will always confirm that $M_{i,k}$ is one of its hosted devices if asked by N_j, unless N_i revokes $M_{i,k}$. Besides that, we assume that N_i will grant the Internet connection to $M_{i,k}$ if requested so by the device. Obviously, the authentication of $M_{i,k}$ towards N_i becomes an important issue.

4.2.2 *Trust relationship between N_j and N_i*

Similar to WiFi roaming with direct Internet access we distinguish between two distinct cases.

The first case assumes that N_j and N_i are untrusted in that they do not share any pre-agreements concerning the roaming service. In particular, they cannot identify each other as legitimate roaming partners, neither directly nor indirectly through some third party acting as the authentication authority *AA*. In this case the guest network N_j has to decide whether to provide a tunnel access between $M_{i,k}$ and some unknown network N_i, even if N_i is willing to accept the tunnel upon the identification of $M_{i,k}$ as its legitimate host.

The second case assumes that N_j and N_i have some pre-established trust relationship in form of either direct or indirect (through an authentication authority *AA*) pre-agreements for the roaming service. This allows N_j to identify N_i as a legitimate partner for roaming and facilitate the decision of N_j concerning the establishment of the tunnel between $M_{i,k}$ and N_i.

4.2.3 *Trust relationship between $M_{i,k}$ and N_j*

The initial assumption at the beginning of the admission phase is that the approaching device $M_{i,k}$ is untrusted by the guest network N_j. While executing the admission phase N_j should be able to decide whether a sufficient trust relationship to $M_{i,k}$ can be established and the tunnel access to N_i granted.

This depends on the trust relationship between N_j and N_i. If the corresponding trust relationship is missing, then N_j can treat N_i as an unknown network which cannot be identified as a legitimate roaming partner. This makes the case comparable to that for the direct Internet access except that N_j has to decide not about granting the Internet connection but about granting the tunnel to reach N_i. Note, however, that since N_i is unknown it can also be any destination of the Internet. This may cause additional legal implications.

Otherwise, if N_j and N_i are trusted and can identify each other as a legitimate roaming partner then it is also possible for N_j to establish the necessary trust relationship with $M_{i,k}$ for granting it the tunnel access to its home network N_i. Obviously, N_j needs to identify $M_{i,k}$ as a valid host of N_i. Note that in this case $M_{i,k}$ receives just the tunnel connection to N_j and the decision whether $M_{i,k}$ will also be given the actual access to the Internet is carried out by N_i without any necessary involvement of N_j.

4.3 *Legal aspects*

4.3.1 *Liability for illegal content*

The reasoning applied here above with respect to the direct Internet access scenario is valid in this case. Undeniably, the role of both networks as technical intermediaries has not changed: the only difference is that the provider granting access to the Internet is no longer the guest network N_j but the home network N_i. Both networks remain 'information society providers' according to article 12 of the e-commerce Directive and can therefore benefit from the exemption of liability for the illegal content that would be transmitted through the services that they provide (see Section).

4.3.2 *Contractual issues*

Trust and legal relationship between the networks N_i and N_j As to the trust and legal relationship between N_i and N_j, the observations made for the direct Internet access case in Section are still valid in this scenario. Indeed, the need for a legally binding document (by mean of a mutual agreement of via a third party *AA*) will be valuable in order to put down all requirements that have to be met by the networks involved in the roaming project.

However, one should pay attention to the fact that the tunnel opened by N_j via the Internet to the home network N_i can be used as a gate by unauthorized intruders. Therefore, the binding document to be accepted by both networks should specify precisely under which conditions the tunnel can be opened and what will be the responsibilities of each network concerning unauthorized access.

Legal relationship between $M_{i,k}$ and networks N_i and N_j The reasoning held above can apply in this scenario since $M_{i,k}$ will still have to comply with the potential document stating his obligations regarding the use of the Internet and the access to the network.

The only difference is that $M_{i,k}$ shall not directly access the whole Internet through N_j's network but through N_i's network. Therefore, $M_{i,k}$ will still have to apply the already existing N_i's Internet use policy (if any).

Specific contractual issues As said here above, some Internet providers prohibit the resale or public distribution of the Internet connection provided with other people than the users having subscribed to the Internet access.

In this specific scenario, the guest network N_j is not offering a direct and unlimited Internet access through its network: N_j only provides $M_{i,k}$ with a tunnel - via the Internet - so that $M_{i,k}$ can connect to its home network N_i and eventually access the Internet via N_i's Internet provider.

Although N_j does not offer a direct Internet connection to $M_{i,k}$, the creation of a tunnel implies the use of the Internet connection provided to N_j by its Internet provider. As a consequence, this could still be considered as a breach of N_j's contractual obligation not to share its Internet access with third parties. However, attention should be paid to the exact wording of the clause prohibiting N_j to share its Internet access (if any) in order to make sure that such use (the mere creation of a tunnel) is also forbidden by the terms and conditions of N_j's Internet provider.

4.3.3 *Telecommunication issues*

Our previous analysis of electronic communications issues in Section will remain valuable in this scenario of roaming with tunnel access.

The nature of the service or network (public or private for example) and, hence, the precise legal position of the person who would like to open his WiFi access points to outside users in order to create a tunnel access to N_i will mostly depend on the concrete implementation of the WiFi roaming solution on the market: would the service be provided against payment, would the access be open to anyone, etc.? The fact that the only available communication will come through this tunnel is not relevant.

4.3.4 *Data protection issues*

Processing personal data In the WiFi scenario with tunnel access, we can mainly identify two processing operations: one for the admission of $M_{i,k}$ and one for the need of creating the tunnel and managing the exchange of messages between N_j and N_i when $M_{i,k}$ is accessing the Internet or the network of N_i through the tunnel.[47]

These processing operations of personal data need to be performed in accordance with the national rules transposing the general Data Protection Directive 95/46, as more extensively explained in Section as regards the WiFi roaming scenario with direct access.

However, one important point that has to be underscored at this stage is that the guest network N_j would - in this scenario - probably be qualified as being a *processor* and not a *controller* of the personal data processing. If it can be argued that the person who determines the purposes and means of the processing is not the guest network N_j, but another (legal) person, that other person will be the controller of the processing. That person

[47] Both are however linked in a manner that one could argue that only one processing is at stake here. The same reasoning could besides be held for the processing operations described in Section.

shall have the entire responsibility of complying with the data protection rules. The guest network N_j, being only a *processor* shall have to follow the instructions of the controller (these obligations and the liability issues shall have to be laid down in a written contract): it will process the personal data *on behalf* of another person. In our opinion, the tunnel scenario allows the possibility for the legal entity ALAWN or *AA* (if any) of being a *controller*, while the participating networks will follow the way ALAWN or *AA* imposes the data to be processed (e.g. the way the admission phase should be performed, the tunnel created): they will be processors.

Data retention As for the WiFi roaming with direct access, some data retention obligations could be imposed on N_j if it can be qualified as a *provider of publicly available electronic communications services*. On the contrary, the home network N_i, as it is only accepting connections of members of its own network would not be such kind of provider and would consequently not have a data retention obligation. Nonetheless, as far as data retention is concerned, as already explained in Section , there are currently no precise rules to apply in Belgium and reference should be made to the European Directive on the matter.[48]

4.4 *Security aspects*

This section focuses on the main security threats in case of WiFi roaming where the guest network N_j establishes the communication tunnel between the mobile device $M_{i,k}$ and its home network N_i. Similar to the WiFi roaming case with direct access we describe security goals from the perspective of the participating mobile devices and networks.

4.4.1 *Device-oriented security goals*

The result of the admission phase in this WiFi roaming scenario is the establishment of the tunnel between $M_{i,k}$ and N_i. Through this tunnel $M_{i,k}$ can obtain Internet connection granted by N_i. Again, we first address the confidentiality of the transmitted information which can be seen as an optional security goal in case the established tunnel connection is used for the transmission of some sensitive data. Unlike the case with direct access the establishment of the tunnel is an explicit action of the WiFi roaming admission protocol. Therefore, it should be possible to ensure an end-to-end secure tunnel between $M_{i,k}$ and its home network N_i, thus, preventing N_j from eavesdropping the communication which is forwarded from the tunnel.

Further we address the problem of impersonation. A malicious guest network N_j may try to convince $M_{i,k}$ that the tunnel is established with the home network N_i whereas in reality the tunnel ends at some point which

[48] Directive 2006/24/EC, *op.cit.*

is not N_i, i.e. by spoofing the address of N_i. Therefore, we require that a secure WiFi roaming solution for the tunnel access should allow $M_{i,k}$ to authenticate the network to which the tunnel is established as its own home network N_i. Note that unlike the case of WiFi roaming with direct access to the Internet there is no need to consider scenarios where malicious N_j tries to spoof other destinations on the Internet since $M_{i,k}$ obtains its Internet connection from its home network N_i which is assumed to be trusted. Still the problem remains when such attacks are performed by some outsider adversary which manipulates the traffic exchanged between $M_{i,k}$ and some destination on the Internet as it travels between N_i and the destination. Again, this is the task of the application executed on top of the established communication channel.

In addition to that we consider potential impersonation attacks by the guest network N_j which acts pretending to be some valid host of N_i. The risk here is that N_j may obtain the Internet connection, perform illegal activities, and later shift the liability claims for these activities on to $M_{i,k}$. A similar threat comes from modifications of the tunnel traffic and from the injection of messages into the tunnel in the name of $M_{i,k}$. Note that these problems may occur either during the admission phase if the latter requires interaction with N_i or during the actual communication phase, i.e., after the establishment of the tunnel between $M_{i,k}$ and N_i. Therefore, we require that a WiFi roaming solution with tunnel access should prevent the malicious guest network N_j from being able to impersonate $M_{i,k}$ towards N_i.

4.4.2 *Guest Network-oriented security goals*

Obviously, the guest network N_j is interested in not to be blamed for the illegal activities on the Internet performed by any mobile device $M_{i,k}$ which obtains access to the Internet from the tunnel established by N_j. Therefore, it is important that N_j is able to authenticate each mobile device as a valid host of some home network N_i prior to the establishment of the tunnel. Moreover, from the admission protocol N_j should be able to obtain some proof that the tunnel connection has been established towards N_i in order to present this proof in case of accusations. This includes the necessity of authenticating the home network N_i to which the tunnel is established. Again, the form of this proof depends on the legal framework which applies to this WiFi roaming scenario. It can be realized by cryptographic authentication techniques such as digital signatures or by logging the connection details. Additionally, if some pre-agreement between the networks exists which regulates payment responsibilities among the roaming participants; this proof could also be used by N_j to claim charges for the provided roaming service.

Further concerns of the guest network N_j include potential damages to its infrastructure caused by some malicious device $M_{i,k}$. Similar to the WiFi

roaming case with direct Internet access we consider protection against possible infiltrations of the guest network's infrastructure with malware out of scope of the secure WiFi roaming solution for the tunnel access. However, we require that N_j should be protected against possible Denial-of-Service (DoS) attacks that may result from the use of this solution. There is one significant difference to the scenario with direct access. Namely, the whole traffic from $M_{i,k}$ will be forwarded over the established tunnel to N_i. This eliminates certain risks for the infrastructure of N_j and lowers the risk of DoS attacks against it. Nevertheless, the risk of DoS attacks against the WiFi roaming service itself remains and has to be handled by the deployed WiFi roaming solution.

4.4.3 *Home Network-oriented security goals*

In contrast to WiFi roaming case with direct access, the home network N_i in the case with tunnel access is always active, i.e., it is seen as the endpoint of the tunnel and has, therefore, to accept or decline its establishment. This imposes several threats against N_i. First, N_i would usually accept the tunnel if it is assured that the mobile device which requests the tunnel is one of its legitimate hosts. Hence, it is important for N_i to be able to authenticate the validity of $M_{i,k}$. This, should be done not only prior to accepting the tunnel but also during the actual communication as a malicious guest network N_j may try to inject messages into the established tunnel.

In case that some WiFi roaming pre-agreement between N_j and N_i exists, possibly through some third party such as the authentication authority *AA*, the home network N_i should be able to authenticate N_j prior to accepting the tunnel connection. This authentication mechanism may also involve the authentication authority *AA* in case that the pre-agreement between N_j and N_i is indirect. If the pre-agreement also specifies the payment responsibilities of the involved roaming participants then N_i should be able to obtain some proof that would be sufficient for N_i to protect itself against illegitimate financial claims from N_j. The form of this proof should be specified within the legal framework which applies to this WiFi roaming scenario. The proof can be realized via cryptographic authentication techniques or by logging the communication details.

4.5 *Practical realization*

In the tunnel mode, the first building block of the technical realization is similar to the one used in the case of a direct access (cf. Section 3.5.1), that is the link layer authorization and authentication of the mobile device can be solved in the same way. The following items discuss the different facets of the tunnel establishment and the Internet connectivity for the case with the tunnel access.

4.5.1 *Owner of the mobile node IP address*

The mobile node can obtain an IP address belonging to either the guest network N_j or its home network N_i. Since the whole data is tunneled to N_i, the use of an address from the space of addresses maintained by N_j requires address translation. On the other hand, using an address of N_i may involve the need for specific mechanisms to discover which address to allocate and how to distribute it.

4.5.2 *Tunneling between N_j and N_i*

Tunneling can be performed using a simple IP-over-IP tunnel, i.e., by adding another IP header with the IP address of N_i as the destination address. This solution imposes additional constraints on N_j, as the guest network has to be aware of $M_{i,k}$ at the IP level and allocate, therefore, addresses according to the policy of the home network N_i.

Another solution, called L2TP[49], uses layer-2 tunnels to transmit data between two end-points over the Internet. The L2TP tunnel can be used by N_j to address $M_{i,k}$ at the data-link layer (e.g. using IEEE 802.1X[35]), which in turn is considered by the tunnel end-point in N_i as part of its physical link. Additionally, L2TP permits to proxy EAP authentication session between the mobile and its home network.

4.5.3 *IP address allocation policy*

If the IP address of the mobile device should belong to the space of its home network, a way to pick and distribute this address has to be decided. Several request-response rounds have to be avoided as much as possible since they impose significant delays during the connection phase.

A first solution could be to allocate statically and *a priori* a different IP address to any mobile that registers with N_i. This solution does not need any communication between the mobile node and its home network when it connects to a guest network. However, this solution does not permit the mobile device changing its address on its own and can be used to track $M_{i,k}$ if its address never changes. The IP address could also be attributed by a N_i server once $M_{i,k}$ is authenticated in the same way as DHCP does[40&41]. This address could be included in the connection acceptance message.

Third, an entire /64 IPv6 prefix could be allocated (statically or not) to each mobile node. This solution should work great but is nevertheless an important address wasting.

---

[49] W. TOWNSLEY, A. VALENCIA, A. RUBENS, G. PALL, G. ZORN, and B. PALTER, 'Layer Two Tunneling Protocol "L2TP"', *RFC 2661*, IETF, Aug. 1999.

Finally, IPv6 router advertisements[43] (or secure ones[50]) can be used in the same way as if all the mobile nodes were on the same link. It permits $M_{i,k}$ to freely choose its own addresses. Note that some configuration has to be performed on the LAN in order to avoid that unneeded multicast messages.

4.6 *Existing solutions*

The only recently proposed approach addressing the citywide WiFi roaming[1] does not rely on a pre-established federation of networks. The guest network N_j accepts just any device without authenticating it and grants it a tunneled access to its home network N_i using VPN and NAT traversal techniques with the assistance of the STUN server that resolves current IP bindings. Thus, the guest network acts purely as a mediator of the communication mitigating the authentication task to the home network, which itself can be malicious. The authors propose to cut-off the connection if the home network does not respond within a certain time interval. This approach bears various legal risks resulting from the misuse of the granted connection since the guest network does not receive any information which would be useful to protect it from the legal claims that may arise later. We stress that in WiFi roaming some mechanism allowing the guest network to authenticate mobile devices and to prove to the third parties in the case of dispute that the home network was accessed by that device is indispensable from the legal point of view. Nevertheless, the tunneling approach if refined by the necessary authentication mechanisms and some contractual agreement between the networks seems to be the most suitable form of WiFi roaming from the security point of view since the connection is granted to one particular address (that is of N_i) and not to the whole Internet.

5 Discussion and conclusion

In this section we briefly discuss and compare both presented approaches for WiFi roaming in terms of their mentioned legal and security aspects.

5.1 *Discussion on legal aspects*

From a legal view point, one can see that the legal consequences of a choice between a WiFi roaming with a tunnel access and a WiFi roaming with a direct access are rather small. Consequently, it is still difficult – at this stage of the study – to plead in favor of one solution.

[50] J. Arkko, J. Kempf, B. Zill and P. Nikander, 'SEcure Neighbor Discovery (SEND)', *RFC* 3971, IETF, March 2005.

As to the *contractual issues* raised in this paper, one can conclude that the need of a legally binding document would be valuable to lay down all requirements to be met by the networks involved in the roaming project.

Regarding the *liability issues* raised by WiFi roaming, they should remain almost identical in both scenarios. However, the 'duty of care' of the participating networks will be different depending upon the respective responsibilities of each actor.

The main question raised as to *telecommunication law* will still be to determine whether or not the networks at stake shall be considered as private or public, since both have specific legal regimes.

Concerning *data protection*, it is clear that both scenarios will lead to the co-existence of two processing operations. However, in the first scenario, the guest network shall probably be considered as the controller, whereas a third legal entity (e.g. *AA*) shall most likely be assumed to be the processor. The question is of importance since the controller will bear the entire responsibility of complying with the data protection rules.

With respect to *data retention*, some obligations could be imposed on the networks involved if they can be qualified as providers of publicly available electronic communications service. However, the lack of precise rules in Belgium concerning the implementation of European law prevents to identify clearly which providers and which data will be concerned by data retention obligations.

5.2 *Discussion on security aspects*

From the security point of view, the main difference between both WiFi roaming approaches is the requirement on the authentication of the home network N_i towards its device $M_{i,k}$. In the case of a direct access no such authentication is needed as the connection is established by the guest network N_j directly to the destination on the Internet. However, this imposes several security risks for the mobile device $M_{i,k}$ which can be prevented by the tunnel approach. The main risk results from possible impersonation attacks of a malicious guest network N_j which may try to spoof the destination address on the Internet. This threat is no more valid in the case of the tunnel access as the only destination to which N_j establishes the connection is the home network N_i.

Furthermore, the authentication of N_i towards $M_{i,k}$ allows for the deployment of encryption mechanisms to ensure protection of the communication between $M_{i,k}$ and N_i such that N_j can be kept out of reach of any sensitive information. Obviously, it requires less effort to deploy such mechanisms between $M_{i,k}$ and N_i than between $M_{i,k}$ and any potential destination on the Internet that would be necessary in the case of the direct access.

Another advantage of the WiFi roaming solution based on a tunnel access is the lower risk of damages to the infrastructure of the guest

network N_j since the whole traffic from the mobile device $M_{i,k}$ is forwarded directly to N_i. This prevents unauthorized connections between alien mobile devices and servers located within the guest network.

On the other hand, the requirement that the mobile device $M_{i,k}$ authenticates itself to the guest network N_j as one of the valid hosts of its home network is similar in both approaches. However, also in this case the tunnel approach provides better flexibility as through the necessary interaction with N_i the corresponding authentication of $M_{i,k}$ can be performed by the home network 'on the fly'.

5.3 *Conclusion*

Although from the legal point of view the WiFi roaming service based on the tunnel access does not seem to offer clear advantages compared to the case with the direct access, we observe that from the security point of view the tunnel-based solution is clearly preferable. Nevertheless, the additional involvement of the home network N_i into the communication and the overhead for the usage of tunnels may result in some efficiency lacks of the tunnel-based solution compared to the scenario with the direct access. Therefore, it is important to address efficiency concerns within the design of practical WiFi roaming solutions.