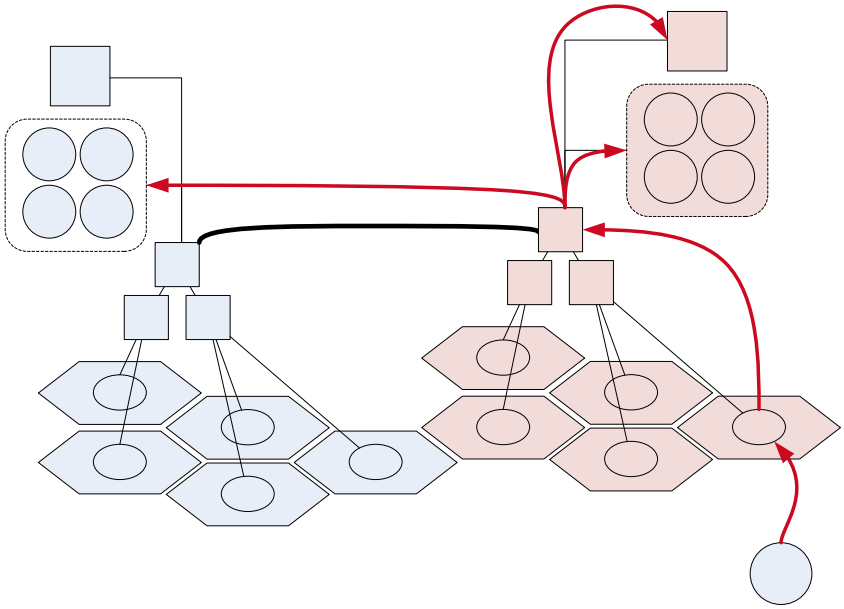


National Roaming for Resilience

National roaming for mitigating mobile network outages

November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Rossella Mattioli, Dr. Marnix Dekker

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

This work has been carried out in collaboration with EY Luxembourg, in particular: Brice Lecoustey, Alexandre Minarelli, George Tountas and Céline Frédéric.

We have received valuable input and feedback from a range of experts from Electronic Communications providers and regulators. In particular we would like to thank the contributions from Marieke Fijnvandraat and Staffan Lindmark.

We have also received valuable reviews from the industry experts in the ENISA Electronic Communications Reference Group.

Finally we thank the experts at National Regulatory Authorities across EU and EFTA countries who work with us as members of the Article 13a Expert Group, in providing us useful feedback during discussions, interviews and reviews of drafts of this document.

Legal notice

Executive summary

Mobile communications are an integral part of everyday life. In less than 30 years they have surpassed the traditional fixed line telephony. Every day millions of European citizens rely on mobile telephony for work, social life, but also to contact emergency services. Hence outages of a mobile network can have a severe impact on the economy and on society.

Mobile network outages are common. In 2012, EU Member States reported 79 significant incidents of electronic communications to ENISA and the European Commission. Most of these incidents had an impact on mobile telephony and mobile Internet.

The goal of this report is to help National Regulatory Authority (NRAs) understand if and how roaming at national level could be used to improve resilience of mobile communication networks and services in case of large outages and start the discussion with the market players around this topic.

In some countries, national roaming is imposed by the NRAs with the objective to promote and stimulate competition by facilitating the entrance of new actors in the market. Sometimes national roaming is implemented on a voluntary basis between operators without intervention or request from the NRA for commercial purposes but as it will become clear in this report it can also be used to mitigate outages.

ENISA is aware that each Member State has a different regulatory approach and telecommunications market. For these reasons this report, after investigating the technical and organizational aspects, presents a portfolio of solutions that can be applied based on the different markets and regulations:

- **No roaming**
- **Ad-hoc activation of roaming with manual selection**
- **Automatic roaming for a fixed set of SIM cards**
- **Ad-hoc activation of roaming with automatic selection**
- **Roaming permanently activated by the customer**

Member States are invited to use this as a starting point for the discussion of national roaming as a resilience solution with the mobile telecom operators in order to develop schemes to mitigate large outages following the resulting recommendations:

Discuss portfolio of solutions offered *- In this way they can use these options as a base to tailor their own solution taking into consideration their own legal constrains and needs and agreements among operators.*

Promote National Roaming awareness *– Each Member State should work with interested parties such as mobile operators on National roaming solutions awareness in case of outages.*

Identify clear thresholds in case of activation *- In case one of the above solutions is selected, ENISA invites the competent authority to define clear thresholds both in users affected and time limit in order to facilitate the emergency response.*

Prioritize voice and SMS *- Another important recommendation includes services prioritization. In case of activation of national roaming as a resilience solution not all types of traffic should be transferred at one time on the other operator in order to avoid congestion.*

Favour open Wi-Fi as alternative solution for data connectivity *– Data connectivity should be transferred to available wireless networks.*

Establish a M2M inventory *- Considering the current trend and growth of M2M technologies regarding smart cities and public utilities, it is auspicated that every Member State starts to develop with providers an inventory of all these SIMs per service and provider in order to assess the possible impact and define a comprehensive continuity plan in case of outage.*

Be prepared for an eventual mobile network outage *- Member States should consider*

- *a comprehensive national risk assessment framework that takes into account not only single provider's business continuity plans but*
- *envisions also cascading effects on the population and critical services as government and public transport for example.*

Identify key people within CI services *- Key people and key services should be identified and emergency preparedness plan should be defined accordingly.*

Mobile communication networks and services have become an integral part of everyday life. People are now more and more reliant on their mobile phone and expect to be connected anywhere at any time. Neelie Kroes, the European Commissioner for the Digital Agenda remarked: "Telecom touches everything and users are developing massive expectations of it. Markets must function, devices must function, networks must function and investment needs to happen."

For these reasons ENISA investigated national roaming as a solution for mitigating outages in order to foster security and resilience of European communications networks and ensure that European citizens can communicate also in case of major outages.

Table of Contents

1 Introduction

Mobile communications are an integral part of everyday life. In less than 30 years they have surpassed the traditional fixed line telephony. Every day millions of European citizens rely on mobile telephony for work, social life, but also to contact emergency services. Hence outages of a mobile network can have a severe impact on the economy and on society.

For example, last year there was a large mobile network outage in the Netherlands. The network of one provider failed, causing outages in a vital economic area in the Netherlands. Millions of customers were affected, for several days, and even public transport in a particular metropolitan area was afflicted. It must be noticed that in this particular incident only the network of one provider was affected. Subsequently, the Dutch government started a discussion with providers about possibilities of using roaming to mitigate outages of mobile networks. Recently these discussions resulted in a national roaming agreement specifically for significant mobile network outages. Researches are on-going about possible extensions of this agreement.

ENISA has been working for several years with regulators in EU Member States to address security and resilience of electronic communication networks. In particular, ENISA has been supporting regulators in the implementation of Article 13a of the 2009 reform of the EU's legislative framework for electronic communications[1]. The goal is providing advice and fostering exchange of best practices about improving the security and resilience of electronic communication networks in the EU. In this document the reader will find an overview of different ways national roaming could be used to address mobile outages.

Article 13a of the EU directive on a common regulatory framework for electronic communications networks and services

As part of the 2009 reform of the EU's legislative framework for electronic communications, a new article in the Framework directive was added: Article 13a asks EU Member States to ensure security and resilience of electronic communication services and networks. ENISA has been supporting the EU Member States in implementing Article 13a. For example, ENISA set up an expert group of experts from NRAs (national regulatory authorities) which meets several times per year to discuss the implementation of Article 13a, past incidents, common issues and best practices. ENISA also collects reports about significant incidents from NRAs across the EU and aggregates these reports to provide a single EU perspective. Based on reports about past incidents and discussions with NRAs, ENISA chooses topics for further investigation or research. This year, for example, ENISA is investigating two topics in more detail:

- Dependencies of electronic communications on power supply; this will be addressed in a separate report.
- National roaming to mitigate mobile network outages; results of our research are reported in this document.

More information about ENISA's work on Article 13a, and the Article 13a Expert Group can be found at: http://resilience.enisa.europa.eu/article-13.

[1] European Parliament and Council (2009), DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services

Trends in latest incidents

Mobile network outages are common. In this section we present some of the data NRAs reported to ENISA and the European Commission (EC) for 2012, in the context of the Article 13a: EU Member States reported 79 significant incidents of electronic communications to ENISA and the European Commission. Most of these incidents had an impact on mobile telephony and mobile Internet (see Figure 4).

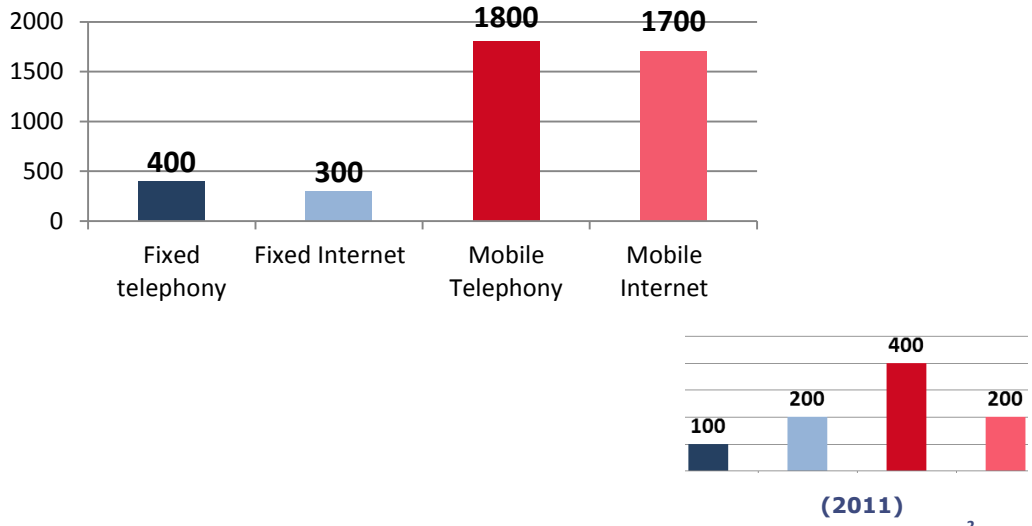


Figure 1: Average number of users affected per incident per service (1000s).[2]

For incidents in all four services, hardware failure was the most common cause. For mobile telephony and mobile internet the second most common cause was a software bug.

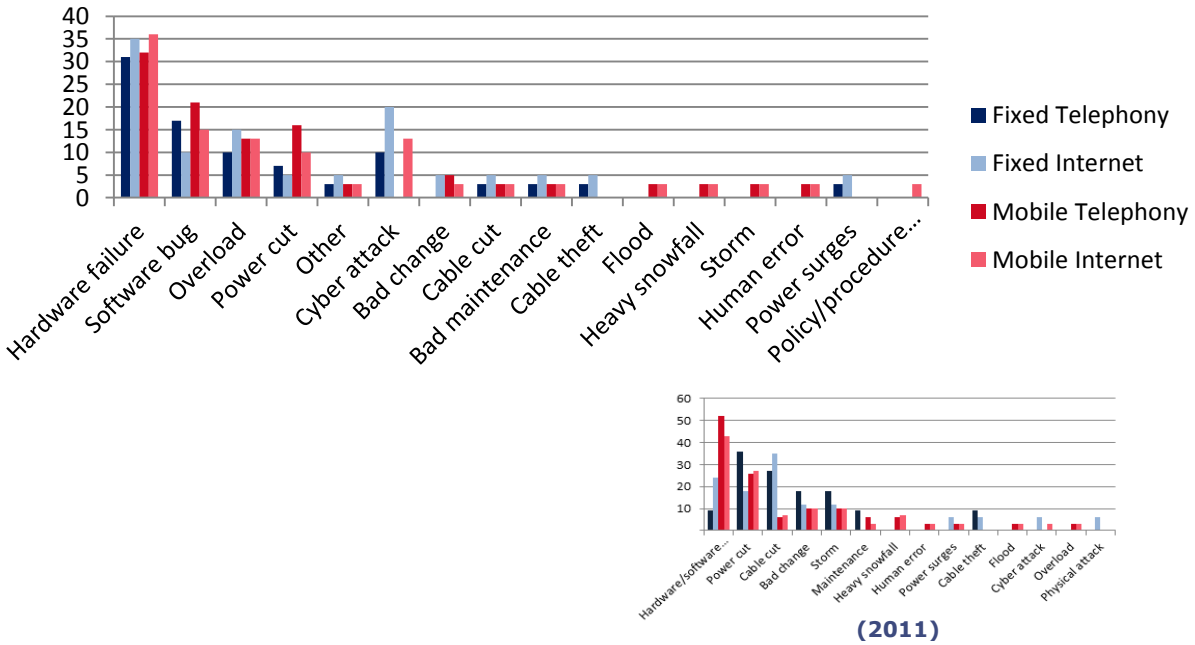


Figure 2: Incidents in 2012 and 2011 per root cause per service (percentages)

[2] ENISA (2012), Annual Incident Reports 2012: Analysis of the Article 13a incident reports of 2012

Target audience

This report is aimed for experts in NRAs and ministries in EU Member States who work on security and resilience of electronic communication networks and services.

They can use this report to start the discussion around the topic with industry experts involved in security, resilience, and/or business continuity, especially belonging to Telecommunications Provider. This report can be also used by civil protection, crisis management agency and critical industries to get an idea of how to improve resilience of mobile communications for critical functions and critical services who rely on mobile networks to function properly.

Goal & Scope

The goal of this report is to help NRAs understand if and how national roaming could be used to improve resilience of mobile communication networks and services in their country and start the discussion with the market players around this topic.

In this report are analysed only the core electronic communication services: mobile telephony and mobile Internet access. Other types of mobile services or value added services are not considered.
It must be underlined that this report considers mobile phones but also mobile devices in general, including mobile communications between machines (MTM). Moreover it should be also remarked here that the focus is on national roaming from a resilience perspective, i.e. how national roaming can be used to mitigate outages. Although they are mentioned at times, other types of motivations for national roaming (for example, competition, innovation, cost-reduction, et cetera) are not deepened.

Structure of this document

This document is structured as follows:

- general background on electronic mobile communication in Europe and its technical working;
- introduction of national roaming and overview of existing national roaming agreements;
- overview of challenges and limitations surrounding national roaming;
- portfolio of a number of viable approaches that NRAs could evaluate to mitigate mobile network outages using national roaming;
- summary and recommendations.

2 The role of mobile communications in everyday life

Mobile communication networks and services have become an integral part of everyday life. People are now more and more reliant on their mobile phone and expect to be connected anywhere at any time. Neelie Kroes, the European Commissioner for the Digital Agenda remarked: "Telecom touches everything and users are developing massive expectations of it. Markets must function, devices must function, networks must function and investment needs to happen."

A good example of the possible impact of a mobile communication network outage is the previously mentioned outage in the Netherlands[3]. In 2012, the infrastructure of a large electronic communication operator was disrupted by a fire in a building adjacent to a site of the provider. The consequences of the fire on the site of the provider affected about 5 million subscribers in the western part of the country, impacting critical metropolitan areas like Rotterdam (a major port and a major industrial area) and the Hague (the seat of the Dutch government). The outage affected both 2G and 3G communications, and had an impact on phone calls, messaging, Machine-to-Machine communications and mobile Internet. It is important to note that due to the outage tram connection between Utrecht - Nieuwegein were out of order too because of their reliance on M2M 2G for communication with control centres. This incident highlights the dependency of economy and society on mobile communication networks and services and how the outage of a mobile provider could have cascading consequences on other critical services and therefore everyday life of large part of the population.

2.1 Penetration and adoption of mobile communications

Penetration of mobile electronic communications is high in all EU countries and the number of mobile SIM cards in use has exceeded 100% of the population in all EU Member States (see Figure 1). Mobile connections are expected to continue growing in the coming years, while at the same time fixed line connections are expected to decrease in most EU countries (see Figure 2).

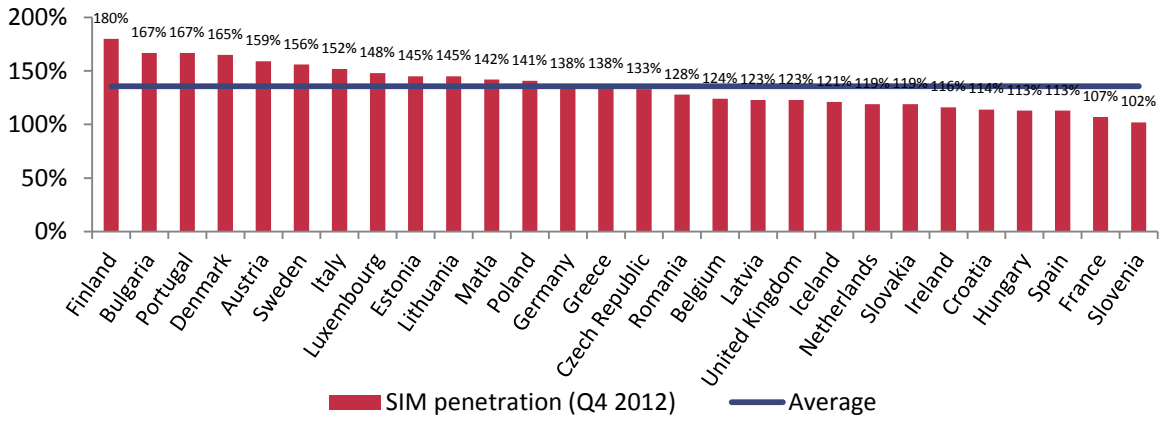


Figure 3: SIM penetration in EU (Q4 2012)[4]

[3]Reuters (2012), Vodafone Dutch service disrupted by fire, Reuters, http://www.reuters.com http://www.reuters.com viewed on 01/07/2013
[4]Data based on GSMA Intelligence (2013), Data Dashboard, https://gsmaintelligence.com/data/ viewed on 01/07/2013

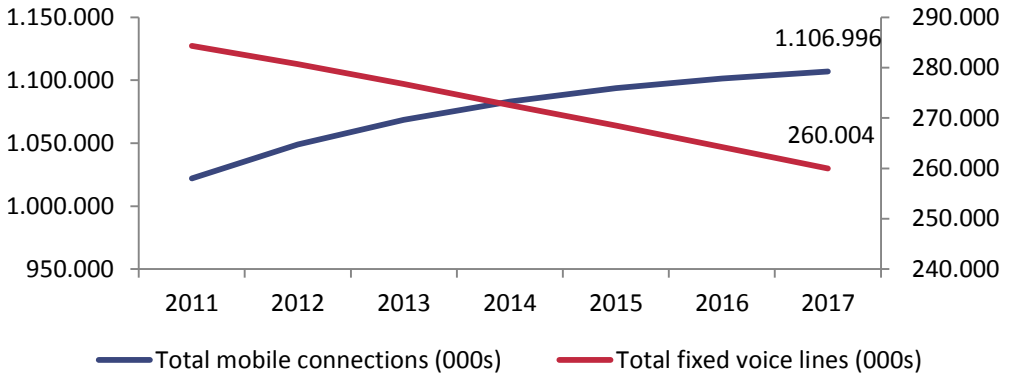


Figure 4: Mobile connections and fixed lines in Europe (000s)[5].

According to surveys, mobiles phone users want to check their phones about every 6 minutes and some check it up to 150 times per day[6]. With the adoption of smartphones, use of mobile communications will continue to increase as smartphones offer many new attractive features and services for users. In 2017, smartphones are expected to account for about 90% of all mobile phones (see figure 3).

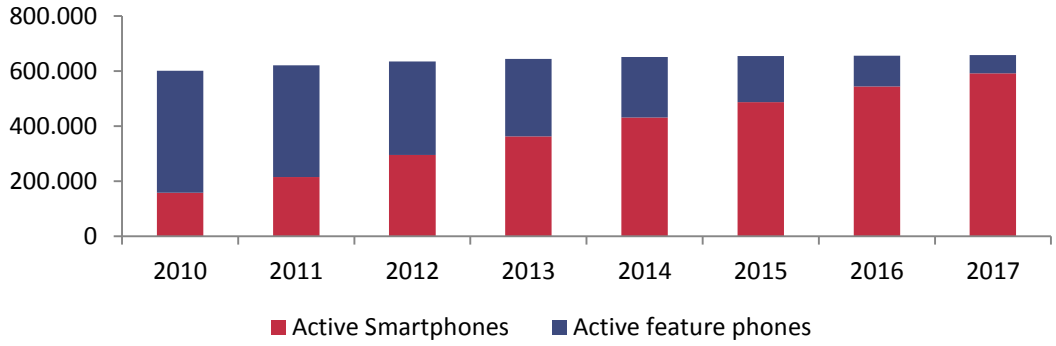


Figure 5: Types of mobile phones in Europe[7]

2.2 Machine to Machine

Besides consumer usage, electronic communications are also used in Machine-to-Machine (M2M) communications, where two systems exchange data without human intervention. Mobile Machine-to-Machine communications can rely on 2G/2.5G/3G/3.5G/4G networks. They are used in public utilities, automotive, consumer electronics, healthcare, security, smart metering (electricity meters), RMAC (remote monitoring automation and control) telemetry applications, "track and trace," with mobile connectivity not integrated directly into a car, POS/payment and ATMs. Considering that this technology represents one of the core components of the development of smart city they are one critical point of failure. Depending 2G/2.5G/3G/3.5G/4G the outage of a mobile provider could have cascading consequences on other critical services and therefore everyday life of large part of the population.

[5]Based on Ovum (2012), Mobile Regional and Country Forecast: 2012–17, Telco Strategy
[6] Spencer B, (2013), Mobile users can't leave their phone alone for six minutes and check it up to 150 times a day, Daily Mail http://www.dailymail.co.ukhttp://www.dailymail.co.uk viewed on 02/07/13
[7] Based on Ovum (2013), Mobile Phone and Smartphone Forecast 2013–2017, Devices and platform

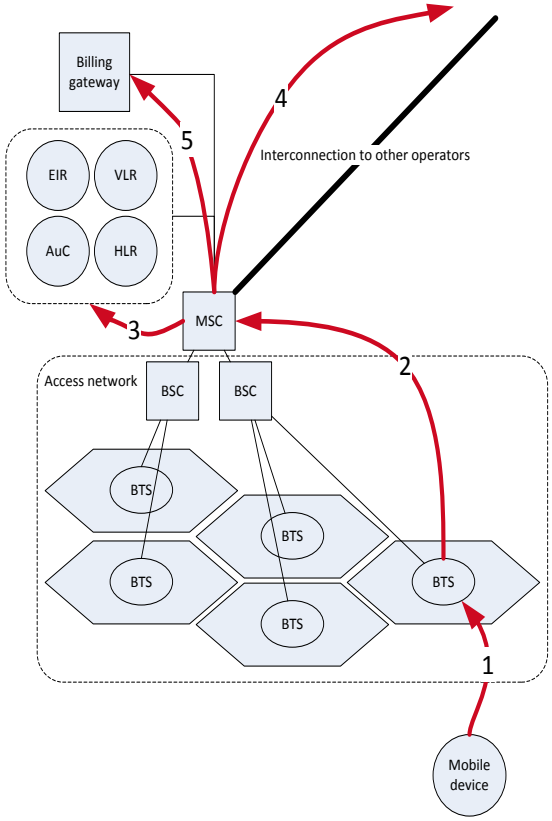
2.3 Mobile network access at the home operator

Mobile communications permeate our reality and in order to start discussing organizational and technical challenges there follows an overview of the components in a mobile network. It is shown how normally a customer connects to his/her operator, and how a telephone call is set up[8].

Note that this is an abstract and generalized picture. Network architectures and communication technology is constantly changing and differs from one provider to the other. We briefly describe the steps, introducing the main components of the mobile network.

Suppose a subscriber turns on his/her mobile device and wants to make a telephone call:

1. The mobile device (of the subscriber) finds a mobile base station (BTS) in reach and requests the base station to connect. The device sends the International Mobile Subscriber Identity (IMSI) of his/her Subscriber Identity Module (SIM) card to the base station. In addition, the device requests for a location registration in order to use mobile services.
2. The base station (BTS) forwards the request to a base station controller (BSC), and finally to the mobile switching centres (MSC).
3. The MSC authenticates the device with the IMSI of the SIM, and checks if the user can connect and what services are available to the user, by checking if IMSI is in the HLR (Home Location Register). This is called the IMSI attach procedure. In a next step the MSC checks the kind of services available to the user (the credit, etc.). If all is well, the location registration request is accepted.



In this example the mobile device was connecting to a base station of its own operator, also called home-operator.

Figure 6: Connecting to the (home) network

Dealing with networks of multiple operators in automatic or manual modes

In practice in most EU countries, most areas are covered by the base stations of several operators. It may even be the case that (temporarily) the mobile device is out of range of the home network, and only in range of other networks. In this case, the device tries to select a more suitable network and to request for a location registration on the visited network.

There are two modes for network selection: automatic and manual. In both cases, the device relies on information directly stored in the SIM card:

[8] GSMA (2012),Mobile Infrastructure Sharing

- Home network and equivalent list including the home operator code (Mobile Country Code followed the Mobile Network Code) derived from the IMSI or equivalent home operator networks' codes if present, in priority order.
- Operator controlled networks list including the codes for networks preferred by the operator in priority order. The different access technologies for each network are also reported.
- User controlled networks list including the code for networks preferred by the user in priority order. The different access technologies for each network are also reported[9].
- Forbidden networks list including the codes of networks with access denied to the device with a reject message.
- Equivalent networks list including list of equivalent networks codes as downloaded by the actual registered network. This list is replaced for each new location registration procedure. These networks are equivalent to the current network in the networks selection[10] .

In automatic mode, the mobile device scans the spectrum and finds all available networks. The device then chooses a network in priority order based on the following list:

1. Home network or equivalents list in priority order (e.g. operator with a permanent national roaming agreement with a tier)
2. User controlled networks list in priority order
3. Operator controlled networks list in priority order
4. Other network with received high quality signal in random order
5. Other networks in order of decreasing signal quality

This means that it requests first to the home network or equivalent as described in the first list. If none of them are found, the device selects a network in the next list, et cetera. Once a network is selected, the device sends a location registration request in order to register to this network and access mobile services.

In manual mode, the device researches and displays all available networks including the networks present in the forbidden networks list (in opposition to the automatic mode). The networks are presented to the user in the same priority order as do the automatic mode. Then, the user selects arbitrary a network from the networks list. Once the user has made a manual selection, the mobile device sends a location registration request to the network in order to access mobile services from this selected network[11].

The base station forwards the request to the MSC. In case of visited network, the MSC would not find the IMSI of the visited user in its HLR but can identify the code of the home network thanks to the IMSI so it can contact the HLR of the home operator. In case there is no roaming agreement between both operators, the home network answers that the device should never be allowed to connect to the visited network and the BTS of the visited network sends a reject message in response to the location registration request (see section 2.3.2). Mobile services are denied and the mobile device does not connect to the base stations of that operator anymore. The situation is depicted in Figure 7. In case a roaming agreement has been set up, the device follows the process as described in the section 2.4.

[9] 3GPP Organisational Partners (2013), 3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application (release 12)
[10] 3GPP Organisational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)
[11] 3GPP Organisational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)

Reject messages

There are many different types of reject messages sent in reply to a denied location registration request[12], but they can be summarized in two main categories: hard reject and soft reject. In both cases, when a mobile device is not allowed to have access to a visited network, because roaming agreements between the visited and the home operators are not activated, the visited operator would send back an appropriate Reject Cause Value to let the device continue searching for other networks.

If the network sends a "hard reject" message (Reject Cause Value = network not allowed), then the device is not allowed to roam in the visited operator network and is informed that the network is forbidden. The device then automatically adds the network to a list of "forbidden networks for roaming" stored in the SIM card. This list is kept even when the device is switched off or when the SIM card is removed. The device will not be able to connect to this network in automatic mode anymore. Nevertheless, it could access it in manual mode if the location registration request becomes successful. Indeed, during manual search, the device shows all the available networks to the user, even the ones already included in the "forbidden Networks list"[13]. The user can select again the same foreign network (which previously sent a hard reject message), and then a new location registration request is sent and can potentially become positive (for example, in case of ad hoc roaming activation). This of course means that users of an operator experiencing an outage will not be able to automatically connect to any visited networks even if national roaming is configured and authorized, unless they initiate a manual network search on the device.

On the other hand, in case of light error message ("soft reject") (i.e. not forbidden), the device continues receiving signals from the foreign networks even if it cannot connect to it. The negative side of this configuration is a certain level of pollution of signals between antennas and mobile devices. However, it does not impact quality of service for users or mobile devices' battery longevity. In this case only, the device can automatically switch networks at any time if the message becomes positive. This of course means that, if the home operator experiences a network breakdown and the visited operator authorizes national roaming for these affected subscribers, devices will automatically switch to and access the visited network.

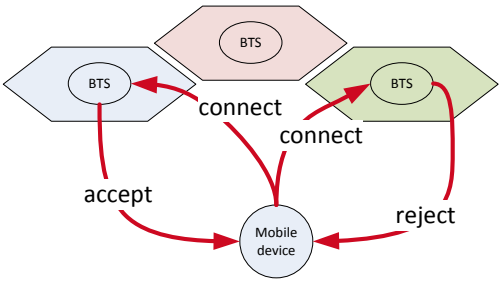


Figure 7: Coverage by multiple networks

[12] 3GPP Organisational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)
[13] 3GPP Organisational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)

2.4 Roaming

Roaming is defined as the use of mobile services from another operator, which is not the home operator. The most well-known form of roaming is international roaming, which allows users to use their mobile devices when abroad. National roaming is roaming on networks of operators within the same country.

This happens in case the user cannot reach a base station of its home-operator, but connects to the base station of another network (roaming), because for example:

- the mobile device is being used abroad
- in that area the home operator is not covered by base stations.

We call the network that is not a home network and to which the mobile device tries to connect to a "visited network".

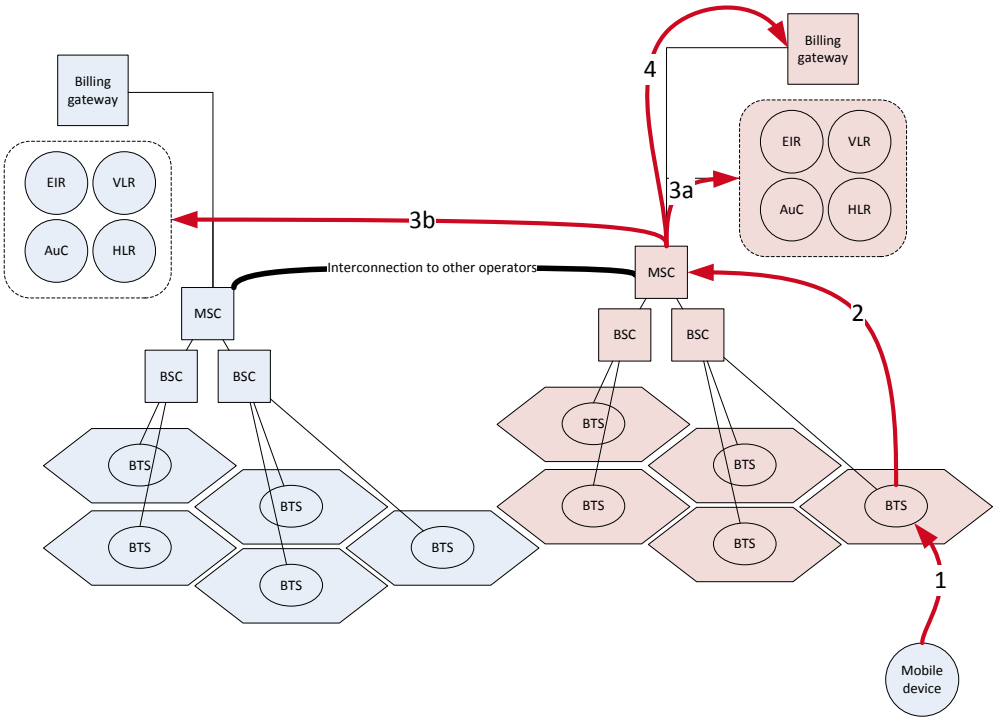


Figure 8: Mobile device roaming in another network

Roaming works basically as follows:

1. The mobile device (of the subscriber – in blue) finds a mobile base station (BTS) of another operator in reach (the pink components) and requests one of these base stations to connect. The device sends the IMSI of its SIM to the base station to register. On the device, the selection of an operator's network could be either in manual or automatic mode. As described in the section 2.3.1, mobile device selects a network based on different lists classified in priority order. In addition, the device requests for a location registration in order to use mobile services.
2. Like before, the base station (BTS) forwards the request to a base station controller (BCS), and finally to the mobile switching centre (MSC) of the visited network.

3. The steps are different from this point on:
    a. The MSC of the visited operator tries to find the IMSI (of the SIM of the mobile device) in its network's HLR. The MSC however does not find it as that IMSI was allocated by a competitor (the home operator).
    b. The MSC uses the IMSI to identify the home network of the SIM (the blue components) thanks to the Mobile Country Code followed by the Mobile Network Code. If a roaming agreement exists between the providers, the MSC contacts the home network's HLR, authenticates the mobile device and retrieves the relevant parts of the profile of the subscriber. This data (about the visiting subscriber) is stored in the VLR (Visiting Location Register) of the visited network. The VLR keeps a temporary profile of the subscriber, for the purpose of roaming. This is done even before the subscriber starts to consume any services (idle mode)[14].

A mobile device registered on a visited network periodically and automatically attempts to connect to its home operator network or any other high priority networks (as described in the section 2.3.1) if on automatic mode. A period is configured in the SIM card to scan the available networks in a specific location. The default period used is usually 60 minutes but can be configured from 6 minutes to 8 hours in 6 minute steps in the SIM. If any higher priority networks are found, the mobile device stays on the visited network[15].

Often, the visited operator charges more than what the home network operator would have charged. These extra costs are called 'roaming costs'. Consumer organizations, governments in the EU and the EC have repeatedly taken legislative steps to reduce roaming costs[16] (for example, by posing hard limits to the price of calls, data, and messages across the EU).

To avoid expensive bills due to inconsiderate consumption of mobile services on a foreign network, users have the possibility to set up a "do not roam" button, especially for mobile data consumption. With that set up directly configured in the mobile device, the users cannot consume data when they are roaming on another network.

[14] European Parliament (2006), Technical Issues on Roaming: Transparency, Technical Aspects and Data – Overview related to the proposed regulation on Roaming
[15] 3GPP Organisational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)
[16] European Parliament and Council (2012), Regulation (Eu) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union.

3 Existing national roaming schemes

International roaming is perhaps the most well-known type of roaming, but also national roaming is quite common. In this section we give a brief overview of existing national roaming schemes. The overview is the result of the desktop research and interviews with all the different stakeholders.

3.1 Types of roaming schemes

We summarize hereunder the different types of national roaming schemes, used in the EU, and outside the EU.

MVNO - Mobile Virtual Network Operator	A MVNO is a virtual operator which does not own a mobile access network. The MVNO has an agreement with another operator, to allow its customers to access the mobile network and consume mobile services[17].
New entrants	This national roaming scheme aims to facilitate new entrants in the market – with the goal to improve competition. The new entrant makes a national roaming agreement to have an immediate full geographic coverage without high initial investments[18]. Such agreements are usually temporary. A common situation is to allow new 3G licensees to temporary use the 2G network of existing operators during the time it is rolling out its own infrastructure[19]. Note that Article 12 1(g) of the Access Directive (2002/19/EC) provides a legal framework for imposing national roaming obligations to operators with a significant market power in order to improve and stimulate competition in the market. France represents an example of this scheme.
Coverage of rural areas	In this scheme a provider extends its coverage to scarcely populated (rural) areas using a national roaming agreement. This national roaming scheme aims to facilitate smaller operators who may not be able to sustain the costs of covering a large territory with a low density of population[20]. Note that Article 4 of the directive No 128/1999/EC provides a legal framework for this: "Member States may, where necessary, take action, in accordance with Community law, to ensure the coverage of less-populated areas"[21].

[17] Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest, p.3
[18] Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest, p.2
[19] GSMA (2012), Mobile Infrastructure Sharing, p.15
[20] Nepal Telecommunications Authority (2011), Consultation paper on National Roaming, Kathmandu
[21] European Parliament and Council (1998), DECISION No 128/1999/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 1998 on the coordinated introduction of a third-generation mobile and wireless communications system (UMTS) in the Community

	Australia gives a good example of this type of agreement.
Regional licenses	In countries with regional licenses, national roaming can be used by operators to offer services in other regions. This allows smaller operators to provide a national service, without actually covering the entire country[22]. This situation is seen, for instance, in large countries like India where the market is divided in regions/states.
In flight/at sea mobile services	Some operators provide roaming services to allow customers to use mobile services in flight or at sea,[23] for instance using roaming agreements with satellite communications providers.
Emergency roaming	The roaming agreement can be used for resilience purpose, supporting the traffic of customers affected by an outage. Different schemes can be implemented and are described in more detailed in the section 5. Sweden, USA and Caribbean are good examples of different schemes of national roaming for resilience purpose.

[22] Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest, p.2
[23] Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest, p.24

3.2 National roaming in the EU

In some countries, national roaming is imposed by the NRAs with the objective to promote and stimulate competition by facilitating the entrance of new actors in the market. Sometimes national roaming is implemented on a voluntary basis between providers (as part of business agreements), without intervention or request from the NRA. We summarized the findings of the research in Figure 9 where the different implementations of national roaming are represented. Note that we did not find information or receive feedback about all EU countries, so this overview may be incomplete and it represents only if national roaming is obliged by the NRA or allowed for commercial purposes.

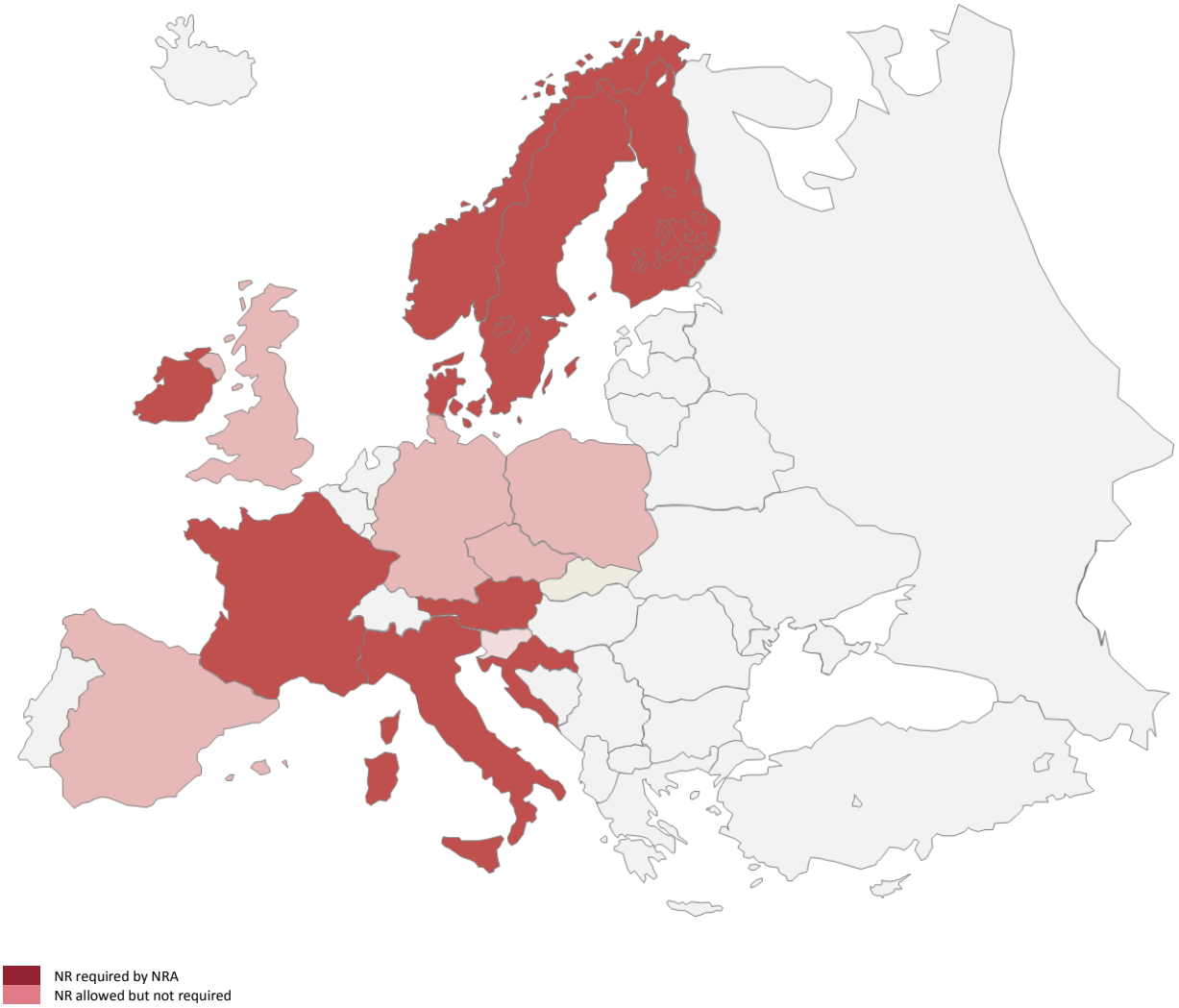


Figure 9: Existing national roaming implementations in the EU

Austria

In Austria, operators owning a 2G network are obliged to provide national roaming to operators which enter the market with a 3G license without the need for deploying also a 2G infrastructure. This type of national roaming can be used for a maximum duration of four years, and the 3G licensees have to cover at least 20% of the population. The roaming obligation only covers roaming

on 2G network to 3G operators (i.e. not 3G-to-3G for example)[24]. The goal of this scheme is to facilitate the entrance of 3G operators.

Austria (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
8,4M	13,4M	159%	3

Czech republic

In the Czech Republic, the Electronic Communications Act does not require national roaming. Also the national regulatory authority does not require national roaming to mobile operators although it is possible to provide it on a commercial basis (common agreement). A change should occur in 2014, after the completion of the auction for mobile frequencies.

Czech Republic (Q4 2012)[25]

Population	Mobile connections	SIMs penetration rate	Number of Operators
10,5M	13,8M	138%	3

Croatia

According to the Croatian Electronic Communication Act, all operators must provide access to their networks. In 2005, Tele2 (3rd operator) signed a roaming agreement with Vipnet to ensure that, upon its launch, its customers would have access to a network with national coverage which was in force until 2008 when Tele2 signed a contract with HT. All terms are commercially agreed (in both cases).

Croatia (Q4 2012)[26]

Population	Mobile connections	SIMs penetration rate	Number of Operators
4,8M	6M	116%	3

Denmark

According to the Danish law, all operators must provide access to their networks. With such scheme, the Danish NRA aims at promoting the access of new entrants and particularly MVNO in order to

[24] Ovum (2012), Country Regulation Overview – Austria
[25] GSMA Intelligence(2013), Data Dashboard https://gsmaintelligence.com/ viewed on 01/07/2013
[26] GSMA Intelligence(2013), Data Dashboard https://gsmaintelligence.com/ viewed on 01/07/2013

stimulate market competition[27]. In 2003, 3 Denmark signed a roaming agreement with TDC to ensure that, upon its launch, its customers would have access to a network with national coverage.

Denmark (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
5,6M	9,2M	165%	6

Finland

In Finland, similarly, the Telecommunications Market Act was amended in 2001 to oblige 2G licensees with significant market share to provide national roaming to 3G operators, covering a minimum of 20% of the population. Furthermore, in 2006, the act was again amended to be more general and applicable to all mobile network technologies to oblige all mobile operators with significant market power to agree on national roaming with other operators upon request[28].

Finland (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
5,4M	9,7M	180%	4

France

In France, a recent entrant (i.e. Free/Iliad) made a national roaming agreement with the incumbent operator Orange France in 2012 while building out its own infrastructure. In France, 2G national roaming is enforced by the regulator, but the 3G agreement is based on commercial arrangement between operators. To benefit from the 2G national roaming, Free had to cover a least 25% of the population with 3G technology. This temporary agreement should be terminated by 2016[29].

France (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
63,6M	67,9M	107%	4

Italy

In Italy national roaming is enforced by the NRA. New entrants have the opportunity to request national roaming agreements from existing operators for a period up to 18 months. National

[27] Ovum (2012), Country Regulation Overview - Denmark
[28] Ovum (2013), Country Regulation Overview - Finland
[29] ARCEP (2012), Avis n° 2012-1627 de l'Autorité de régulation des communications électroniques et des postes en date du 20 décembre 2012 sur la demande d'avis de l'Autorité de la concurrence relatif aux conditions de mutualisation et d'itinérance sur les réseaux mobiles

roaming must be provided on a non-discriminatory basis by operators with a significant market share, with prices based on the actual costs[30].

Italy (Q4 2012)[31]			
Population	**Mobile connections**	**SIMs penetration rate**	**Number of Operators**
61,0M	92,7M	152%	4

Ireland

In Ireland, like in Austria, national roaming is mandatory for operators of 2G networks, and must be offered to 3G operators covering 20% of the population. This agreement is in principle based on commercial negotiations. In case of non-agreement, the regulator may set the prices based on the retail price minus any avoidable costs[32]. In Ireland, two new entrants, Meteor and 3, successfully concluded national agreements with established operators in 2005[33].

Ireland (Q4 2012)			
Population	**Mobile connections**	**SIMs penetration rate**	**Number of Operators**
4,6M	5,4M	116%	4

Poland

In Poland, operators are not obliged to offer national roaming, but it is allowed by the NRA. Indeed, new entrants have had the opportunity to conclude national roaming agreements with existing operators[34]. For example, Polish telecom P4 made a national roaming agreement with Polska Telefonia Cyfrowa in 2012 to reduce gaps network coverage. This operator already concluded similar deals with other operators in the past for the same purpose[35].

Poland (Q4 2012)			
Population	**Mobile connections**	**SIMs penetration rate**	**Number of Operators**
38,3M	54,1M	141%	4

[30] Ovum (2013), Country Regulation Overview - Italy
[31] GSMA Intelligence(2013), Data Dashboard
https://gsmaintelligence.com/ viewed on 01/07/2013
[32] Ovum (2012), Country Regulation Overview - Ireland
[33] Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest, p. 11-12
[34] Ovum (2013), Country Regulation Overview - Poland
[35] Telegeography, Play looks to close national roaming deal with PTC, Telegeography
http://www.telegeography.com viewed on 01/07/2013

Sweden

First example in Europe, in Sweden, the regulator (PTS) has implemented an emergency roaming scheme since 2008. The scheme is based on voluntary agreements between the operators (i.e. Telenor, Tele2, TeliaSonera and Tree), and regards a limited number of SIM cards (4,000) to roam nationally. A detailed overview on the solution is provided in chapter 5.3.

Sweden (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
9,5M	14,8M	156%	6

Spain

In Spain several operators have entered into national roaming agreements over the past years. In 2008 Yoigo concluded a five-year agreement with Telefonica Espana as well as with Orange Spain, in order to extend its 2G and 3G coverage to areas not yet covered by its own network[36].

Spain (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
46,9M	53,2M	113%	4

The Netherlands

Following the outage of Vodafone in 2012, the Netherlands searched for a resilience solution in case of an operator outage. As a result, the three operators (Vodafone, KPN and T-Mobile) have concluded regional roaming agreements that would allow each two providers to temporary serve the third provider's customers in case of an outage. The coverage will not be necessarily national as the agreement could enter into force for a specific region of the country only. A detailed overview of the solution is provided in chapter 5.2.

Netherlands (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
16.7M	19.9M	119%	4

[36] Ovum (2012), Mobile Network Sharing Deals Analyzer: 2H11–1H12, Telco Strategy

3.3 National roaming outside the EU

Australia

National roaming is allowed in Australia to extend the coverage of an operator in the countryside. Vodafone Australia provides this service to its customers on demand[37]. The principle is that if Vodafone's customers want to use their mobile communications services in the rural areas of Victoria and Tasmania, outside the coverage of their home operator, they have the possibility to contact the customer centre to activate the national roaming service. In this case, customers roam on the network of Telstra as soon as the network of Vodafone is not available in the specified areas. The switch of networks is automatic unless the customer is already on a call. In this last scenario, the call drops and the user has to redial the number from the Telstra's network.

Australia (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
23.1M	30.6M	133%	3

India

The Indian telecommunications sector is split according to the 22 circles of India and most of the Indian operators have only local or regional licenses to operate mobile services. In this context, roaming represents a way to provide mobile services at national level (i.e. in all circles). This kind of roaming is called inter-circle roaming and is currently in the process of being regulated on prices by the Telecom Regulatory Authority of India (TRAI)[38]. Each circle acts as a separate country/region which makes the comparison with national roaming. Nevertheless, there are some cases of intra-circle roaming which can be associated to national roaming: a customer of an operator can use the network of a competitor operating in the same circle. This type of intra-circle roaming has primarily been implemented to improve operator's coverage inside circles where they do not have strong network.

India (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
1.3B	864.7M	68%	13

USA

In 2011, the Federal Communications Commission (FCC) adopted an order to ensure that customers have access to mobile Internet anywhere the service is technically available[39].

[37] Vodafone Australia, National roaming, http://www.vodafone.com.au/personal/services/coverage/nationalroaming viewed on 08/08/2013
[38] Telecom Regulatory Authority of India (2013), Consultation Paper on review of Tariff for National Roaming, New Delhi
[39] Goldman D. (2011), FCC requires national data roaming for all, CNN Money, http://money.cnn.com/2011/04/07/technology/fcc_wireless_roaming/index.htm viewed on the 08/08/2013

In this context, the FCC has required the main operators (AT&T and Verizon) to offer national roaming agreement to smaller and rural operators in order to provide national data services to all customers and compete with main providers. This completes the existing framework on national roaming for voice services. Indeed, the national authority already requested operators to conclude voice national roaming agreements for the first time in 1981. In 2007, the FCC strengthened its position arguing that mobile providers need to provide voice roaming automatically.

In addition, USA has experienced some sorts of emergency national roaming. Such agreement was introduced ad hoc in 2012 between AT&T and T-Mobile for areas heavily impacted by Hurricane Sandy in New York and New Jersey. Customers were authorized to make calls in those areas on the network which was the most operational, whichever the network was a home or a visited network. This means that the switch of network was automatic, based on the best signals. This service was not differently charged to the customers but followed the existing rate plans[40].

USA (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
317.1M	347.2M	109%	12

Caribbean

In addition to USA, Caribbean has implemented emergency roaming agreements ad-hoc. Beginning of 2013, CCT experienced an important outage, requesting the support of its competitors Digicel. During more than 7 days, Digicel hosted both prepaid and post-paid customers of CCT without any changes of tariff plans for them. They were able to make national and international calls while also using their data services. CCT customers were requested to select the Digicel network thanks to the manual mode of their device[41].

Virgin Island (Q4 2012)

Population	Mobile connections	SIMs penetration rate	Number of Operators
23,816	28,696	120%	3

[40] Berry Review (2012), AT&T & T-Mobile Enter Into Emergency Roaming Agreement for Hurricane Sandy, http://www.berryreview.com/2012/10/31/att-t-mobile-enter-into-emergency-roaming-agreement-for-hurricane-sandy/ viewed on the 09/08/2013

[41] BVI Platinum (2013), CCT Network Woes Continue; Digicel/CCT Reach New Roaming Agreement, http://www.bviplatinum.com/news.php?page=Article&articleID=1357663206 viewed on 08/08/2013

4 Limitations and challenges

We interviewed a number of experts from regulators and the telecommunications industry players, asking them about their views on and experiences with national roaming. Some of the regulators we interviewed had already some experience with national roaming in the past (e.g. Austria, Finland, and Italy). Others currently have national roaming schemes in place (e.g. France, Sweden), or have researched it in the past. We show which regulators were interviewed in the map below (cf. figure 10). In addition, we interviewed four mobile network providers who have been involved in national roaming in France, in the Netherlands and in India (where national roaming is a regional matter). In total hence we interviewed experts from 22 different organizations.

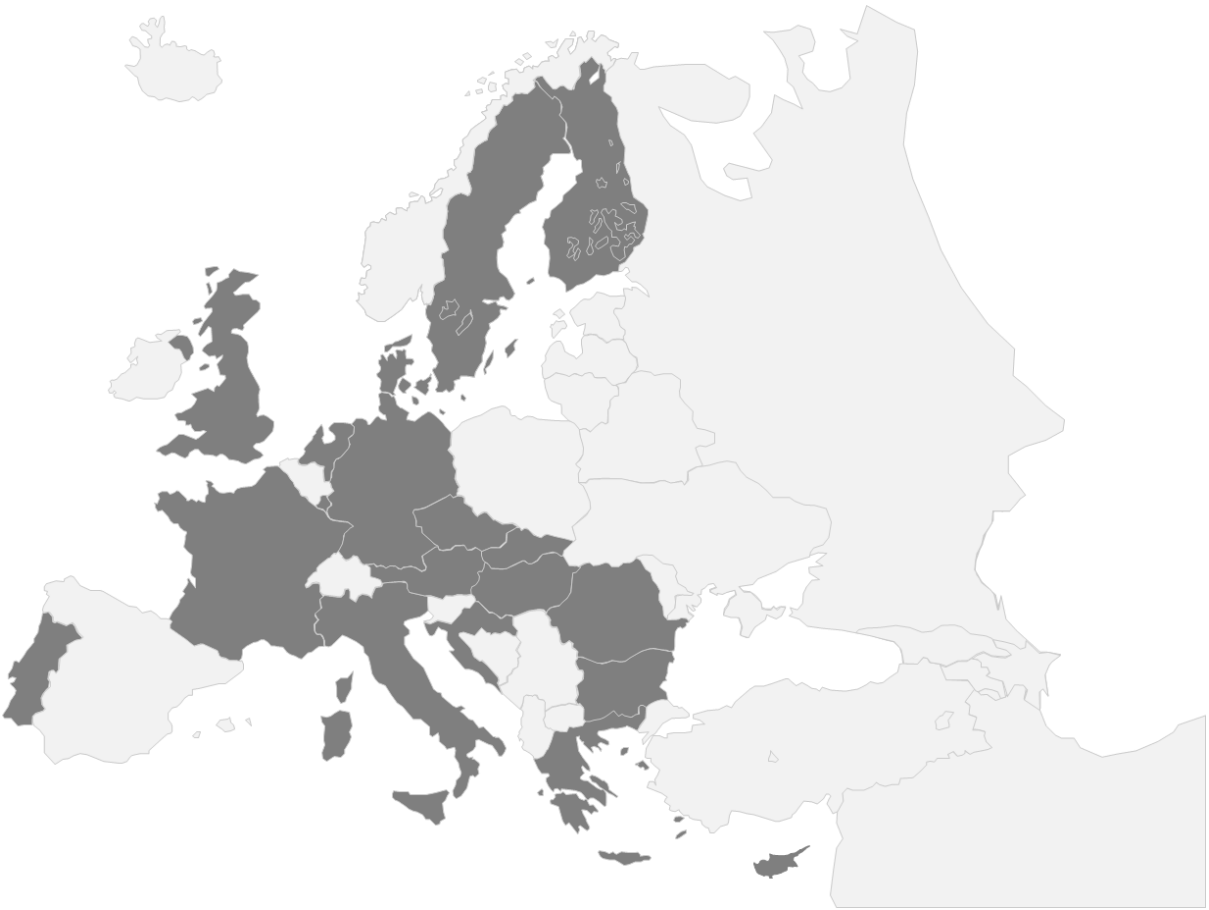


Figure 10: Interviews of regulators

In this section we summarize the issues that were raised and discussed in these interviews.

4.1 Limitations

In the course of this study a number of experts pointed us to the limitations of national roaming for resilience purpose. It is clear that a number of outages cannot be addressed with national roaming. In this section we try to underline all the major limitations that can be seen as a starting point for future areas of research.

Outages affecting all providers in the country

Outages affecting all providers at once cannot be mitigated using roaming. For example, power cuts usually affect all the providers in a geographic area at the same time. Similarly, natural disasters might affect several providers at once.

Outages affecting the home HLR

To set up a roaming call the VLR of the visited network and the HLR of the home network must communicate with each other (via the MSCs) to authenticate the SIM of the mobile device (see Section 2.4). National roaming cannot be used if the HLR of the home network is unreachable by the visited operator. This means for example that failures of the HLR (a common cause of outages) cannot be mitigated by roaming.

Similarly, the IN (Intelligent Network) of the home operator is needed to allow prepaid subscribers to make calls. In case of IN or MSC breakdown, the visiting network is not able to check the profile and balance of the visiting subscribers.

In 2012, Orange France and O2 UK mobile networks were separately affected by a core network breakdown impacting millions of customers. In both cases, the HLR generated multiple error messages creating an oversaturation of signals and leading the core network to crash. A similar case appeared in the USA as well in 2011, impacting Verizon[42].

Outages affecting shared infrastructure

There are settings where the access network is shared by several operators. For example, in certain remote areas this may be used to share and reduce high costs of covering areas with low density of subscribers. In these settings, an outage in the access network would affect several providers at once. National roaming would not work to mitigate such an outage.

Overloads

National roaming can be a solution if other network providers are up and running and able to deal with the traffic of the roaming devices. This means, as mentioned in the introduction, that in crises situations where there is a high traffic overload on all providers, roaming is not a solution. A recent example is when in 2013, operators in the centre of Boston experienced a big congestion of network during the annual marathon due to high calls volume following the panic caused by the bombs explosion[43]. The unavailability of mobile networks caused more panic, which made the work of emergency services more difficult. National roaming, however, would not be a solution for this kind of outage.

4.2 Challenges

During the interviews experts raised a number of challenges that should be addressed.

Overload of the visited network

If during an outage mobile devices are allowed to roam on other networks, this could cause an overload or a reduced quality of service for the original subscribers of the visited network. As a way to address this, providers offering roaming could configure restrictions and prioritize their own customers, in order to keep an acceptable level of quality for their subscribers.

Competition

National roaming could negatively impact competition, and remove incentives for providers to offer resilient and redundant networks. By allowing national roaming, one might create a “race to the bottom”, where no provider has an incentive to provide resilient networks anymore – because it is

[42] Fitchard, K. (JUL. 13, 2012), Why are mobile networks dropping like flies? Gigaom viewed on 01/07/2013 Why are mobile networks dropping like flies? Gigaom

easy to back up on the networks of others during an outage. Interestingly, national roaming is often used in the EU to actually improve competition (new entrant's scheme e.g.).

One way to address these concerns would be to restrict national roaming to specific circumstances, in order to deal with severe outages. Another way would be to ensure that the operator suffering the outage actually bares additional costs for using the other networks (say intra-provider roaming costs), so as to create an incentive for the operator to prevent outages in the future.

Set up costs

The implementation of national roaming could require (too) large investments by the providers. As a way to address this, operators could leverage on existing international roaming infrastructure. In other words, by technically mimicking international roaming as much as possible, the technical investments needed should be limited.

Roaming costs

It is common practice for providers to charge roaming subscribers higher fees for international roaming[44]. Also in national roaming, visited providers could be charging higher fees for the roaming service. To transfer these costs to the subscriber would seem more complicated, however, in the case of national roaming. Subscriber must be made aware there is an outage and asked to opt-in to higher costs. This does not seem very feasible to organize for large numbers of users. At the same time it would probably anger most consumers if the on top of the outage they are offered the same services they paid but now for a higher price.

Triggering roaming

National roaming is considered a kind of last-resort solutions. The Dutch regulator, for example, has agreed with operators to enable national roaming when it is expected that an outage will affect 500,000 customers affected and the network recovery time is expected to be longer than three days. This however raises another issue. How can operators know if an outage will last a long time? Providers might underestimate the time needed for recovery. During the outage in the Netherlands, for example, the provider repeatedly said it expected to restore service in a matter of hours. But in the end the incident lasted more than several days. One solution could be to use a more objective parameter for triggering roaming: for example, the duration (until now). For example, the trigger could be, if an incident lasts more than 12 hours, then national roaming should be enabled.

Voluntary or regulated

It is not clear whether the NRA has a legal mandate to oblige providers to engage in national roaming agreements for the purpose of resilience. According to article 13a, EU Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks[45].

One could argue that national roaming is a step to guarantee resilience. One could also argue that the NRA should just set high-level resilience requirements, and that it is up to the provider to

[44] This practice is often severely criticized by EU governments and the EC and stands to finish soon.
[45] European Parliament and Council (2009), DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services

determine what are appropriate steps, and whether or not national roaming agreements could be helpful in case of large outages.

5 Technical solutions for mitigating mobile network outages

In this section we provide 5 different options for NRAs, based on the input we received from experts from industry and regulators. For each option we list the pros and cons, and we discuss the main challenges.

	No national roaming	Ad-hoc activation of roaming with manual selection	Automatic roaming for a fixed set of SIM cards	Ad-hoc activation of roaming with automatic selection	Roaming permanently activated by the customer
Type of outages	←				→
Access network	- Not covered	+ Entire users base could be covered - No M2M communications	+ Only vital public functions could be covered - No M2M communications	+ Entire user base + M2M communications	+ Entire user base could be covered - Competition
Core network	- Not covered	- Not covered	- Not covered	- Not covered	- Not covered
All operators affected or shared infrastructure	- Not covered	- Not covered	- Not covered	- Not covered	- Not covered
Overloads	- Not covered	- Not covered	- Not covered	- Not covered	- Not covered

Figure 11: Current situation in Europe of implementation of National Roaming for mitigating mobile network outages

5.1 No national roaming

In this approach, national roaming is not set up as a solution to counterbalance the effects of an outage. The NRA only raises awareness with subscribers (particularly subscribers in critical sectors) about the importance of backup and failover solutions; ways to mitigate outages of their own provider, including:

- Dual or backup SIMs: subscribing to mobile communications services with more than one provider allows the customer to spread the risk across two or more providers.
- Foreign SIMs: foreign providers have roaming agreement with more than one operator in almost every country. In that sense, an international card allows the user to use more than one network.
- Other mobile communication services as Wi-Fi, satellite, radio, et cetera.

Technical set up and cost structure

This approach does not require any specific technical set up. In addition, the cost is totally supported by the customers who ensure themself in case of outage. This approach is individual and depends on each customer.

Pros, Cons and issues/challenges

The main advantage of this approach is that it does not require any investments or legal agreements. The approach is individual and depends on each customer which agrees to support their own additional costs to insure him against the negative impact of an outage.

The main disadvantage is that the above-mentioned options are usually cumbersome for consumers:

- With dual SIMs users should keep track of two telephone numbers for the important contacts.
- SIM from a foreign country would be too costly to use continuously. In addition, foreign SIM card could be able to roam on specific providers' networks with which the home operator has concluded an international roaming agreement. There is no way to prevent these specific operators to be affected. Lastly, some countries impose customers to have a billing address in the country before subscribing to mobile services so it would be difficult to acquire such a SIM card.
- Other identified communications services do not represent a complete alternative: Satellite telephony is too expensive to use continuously while Wi-Fi allows only a sedentary use of the services. Wi-Fi could be associated to fixed communications services more than a substitute to mobile services.

5.2 Ad-hoc activation of roaming with manual selection

As for the above mentioned solution, it is possible to activate national roaming, ad-hoc, leaving at the customer level the decision to use or not this service thanks to the manual network selection.

The Netherlands is a similar example of this solution.

Technical set up

This ad hoc activation of national roaming can be configured according to two different models already presented in the previous scheme. The only difference in this case is that the customer manually selects the network to roam to. In that sense, the user is aware of the roaming service. However, we cannot consider the manual registration alone as consent from the customer to pay additional fees, if any. It is necessary to notify the users about the additional fees of national roaming with clear messages (e.g. sms as for international roaming).

To allow only a manual selection of the network it is important to set up hard reject message with network forbidden. In this case only the network is stored in the forbidden list included in the SIM card and can only be selected manually by the user.

In both cases described above, national roaming can be authorized by the visited operator at national level or according to Location Area Code (i.e. LAC) in order to target the zones affected.

Cost structure

Costs could be billed in the commercial agreement between the providers who enable this capability: pre-agree lump sum or on a reciprocal basis as described in the previous schemes. Roaming costs, as a VAS, could be supported by the subscribers who manually select the roaming network. They acknowledge the national roaming capability and related costs. However, as described in the technical set up, the manual selection of a hosting network does not represent a valid consent of the customer to support extra costs. In this sense, clear message are necessary to raise the awareness about the additional costs.

Pros, Cons and issues/challenges

The main advantage is the range of customers who can enjoy the continuous service. Every customer can manually switch between networks in case the home operator's network is not available during an outage. The costs of this solution could be directly charged to the customers as they manually activate the service and received a clear message informing them about the extra costs they are subject to in case of national roaming. In that sense, they are aware that national roaming is a VAS. This creates important incentives for the providers to deploy this solution.

The main disadvantage and challenge is the possible breaches in the market competition. It could potentially decrease the willingness of operators to deploy a resilient network. Indeed, it is easier to carry on the networks of competitors during an outage, especially if the costs are supported by the customers. As a consequence, it is important to set up different thresholds in terms of number of subscribers impacted, location areas impacted, expected duration of the outage, etc. according to which the solution will be activate to allow the providers to use this service only in case of serious incidents.

In addition, an important popularity of this scheme could cause an overload and threaten the service quality for original subscribers of the visited network. However, the configuration per LAC, ranges of classes of IMSIs allows a smaller negative impact on service quality for the visited operator's customers. The visited network has only to support the users communicating in the areas affected by the network breakdown.

Lastly, this solution does not represent the most appropriate solution for Machine-to-Machine communication. Indeed, with a manual solution, the SIM cards in the machine will not be able to switch networks without a human intervention, which is not possible in most cases.

All things concerned, this solution can benefit to the entire society which has the choice to opt-in or not. A threshold is necessary to avoid any abuses.

Netherlands - an example of implementation

Following the outage of Vodafone in 2012, the Netherlands searched for a resilience solution in case of an operator outage. As a result, the three operators (Vodafone, KPN and T-Mobile) have concluded regional roaming agreements that would allow each two providers to temporary serve the third provider's customers in case of an outage. The coverage will not be necessarily national as the agreement could enter into force for a specific region of the country only.

General set up:

In case of important outage, affecting more people than the predefined thresholds (500,000 customers affected and the network recovery time is expected to be longer than three days), national

roaming agreements are used to provide primary post-paid services (Voice and SMS) to customers. According to the exceeding of the thresholds and in concert with the partner operator this solution can be activated without the involvement of the NRA in the process

Other services (machine to machine, data) are not included due to the possible waterfall effect and the viable alternatives. For example hosting of rescued customers could impact the network of the hosted operator. A national survey is currently being conducted regarding critical infrastructures communications to identify interdependencies, assess impacts and find (technical) solutions. For data, Wi-Fi is currently considered as an alternative. This is due to the large volume of traffic of mobile connectivity where roaming of data will most likely quickly overload the visited network. For this reason data connectivity should be backed up by other means such free public Wi-Fi and fixed broadband connections that can be made available in the affected area.

Two operators take over the traffic of the third operator experiencing an outage. The quality of service for other users (from the helping operators) is closely monitored. Operators have their own SLAs with their customers, based on KPIs. To be able to take over more traffic from the guest operator, these key performance indicators can be lowered by the helping operators. Operators have defined together a minimal level as a maximum to lower their KPIs during RR. However, in case a critical level is reached in the network, each operator has the right to stop hosting foreign customers.

Technical set up:

National roaming is forbidden in the Netherlands. As a consequence, the international roaming infrastructure cannot be used and a dedicated infrastructure is set up to support this scheme. Furthermore, this solution is only possible in case of access network breakdown and not in case of core network breakdown.

In order to use this service the customers need to manually select the new network on their device. Since the migration of users is done in different batches of IMSIs, they may have to try several times until they successfully connect to a foreign network, depending on whether they are part of the already migrated batch of IMSIs or not. Once they return on an area covered by their home network, users are switched automatically to their home network.

All the operators' websites, customer support as well as employees are responsible for raising customers' awareness on what actions need to be taken in case of outage.

Costs:

Costs for traffic handling during the activation period will be charged based on the European roaming tariffs. In case the regular KPIs of the host operator will be lowered to enable handling more traffic of the guest operator, the host operator runs the risk of breaking SLA agreements with its own customers. Negotiations for reimbursements of related penalties or claims are underway between the wholesale departments of the operators. Those negotiations are done separately between each two operators under confidentiality (Chinese wall) to ensure that competition will not be breached.

5.3 Automatic roaming for a fixed set of SIM cards

In this third approach national roaming works only for a specific set of SIMs (or a specific number range) controlled both in terms of users and usage by the NRA. These specific SIM cards are distributed by the NRA at the beginning of the outage to targeted users identified with a national risk assessment and need to be retrieved or deactivated as soon as the network affected by the outage is recovered. This strong control by the NRA avoids abuses and uses outside the scope of resilience. The regulator is responsible for distributing the SIM and decides if it should be activate depending on the expected impact of the outage.

This scheme could be promoted by the NRA but voluntary agreed by providers, or totally obliged by the NRA. The costs for the extra service (the possibility to roam) are paid by the NRAs or the operators depending on the agreement.

Technical set up

The scheme requires specific SIM cards capable to have more than one home operator. In that sense, they should be set up and registered in the HLR of every provider included in the roaming agreement. This technical specificity ensures the efficiency of the roaming scheme during extended types of outage, including HLR breakdown. Operators' networks are flagged as equivalent home operators' network in the SIM card which allows the selection of any of those in manual or automatic mode. As they all have the same priority, the stronger signal determines the network to select.

No reject messages are needed in this case.

Cost structure

Even if the scheme leverages on the existing infrastructure, it requires the development and the implementation of specific SIM cards capable to have more than one home operator. In addition, it requires some organizational costs regarding the definition of the commercial agreement between operators and the administration of the designated SIMs. Indeed, SIMs cards need to be distributed by emergency centres during the outage which creates distribution and storage costs. These costs can be supported by the regulator or by the operators depending on the agreement.

Costs of usage need to be supported by the operator affected by the outage in order to keep their willingness to have a resilient infrastructure.

Pros, Cons and issues/challenges

The main advantage of this scheme is the very limited impact on competition. As this service is highly controlled by the NRA, the risks of abuses or uses of services outside the scope of resilience are very low. In addition, as the cost of use is supported by the providers affecting by the outage, it does not decrease their willingness to invest in a resilient network.

In addition, national roaming for a fixed range of SIMs decreases significantly the risks of network congestion for the hosting operator. Depending on the number of emergency SIMs, it does not require any increase of capacity and does not strengthen the quality of service for other customers.

The main disadvantage of the scheme is the limited benefit for customers. Only a limited number of specific customers (mainly vital public functions) are insured against the impact of an outage and can use a continuous mobile service. These customers are chosen by the NRAS which controls the distribution of SIM cards.

In addition, the organizational burdens are quite important: emergency centres need to be implemented to control and distributed the SIMs in case of outage. It represents the main challenge of this solution: being able to distribute the SIMs card timely and efficiency to guarantee a limited breach of mobile communications services.

All in all, it represents a pure solution of resilience, targeted only public vital functions.

Sweden - an example of implementation

In Sweden, the regulator (PTS) has implemented an emergency roaming scheme since 2008. The scheme is based on voluntary agreements between the operators (i.e. Telenor, Tele2, TeliaSonera and Tree), and regards a limited number of SIM cards (4,000) to roam nationally.

These 4,000 SIM cards are called emergency SIM cards and are distributed beforehand to specific crisis centres for use only in case of serious disruption of electronic services or communication networks. That disruption could be the breakdown of multiples operators with a long expected time to restore the infrastructure. The regulator decides whether the emergency roaming cards should be used or not, following requests from the county administrative board concerned by an outage. If the regulator agrees then the SIM cards are distributed to those parties. The use of these cards is restricted to vital public functions chosen by the NRA. This means that SIMs are not always available to targeted customers but highly controlled by the regulator. Once the networks of affected operators are restored, SIM cards are returned to the crisis centre. The use is only allowed for a specific period of time.

The user of these specific emergency SIM cards can automatically connect to any available networks, depending on the quality of signals.

PTS has financed the implementation of this scheme as well as the acquisition of SIM cards, together with subscriptions. However, the operators have to support the costs associated with their use. If such costs should become unreasonably expensive for an individual operator, the regulator shall compensate the operator[46].

5.4 Ad-hoc activation of roaming with automatic selection

A fourth technical solution is the ad hoc activation of national roaming, only in specific geographic areas affected by the outage, relying on the automatic network selection mode on the customers' phones or classes of IMSIs

The USA is a similar example of this solution.

Technical set up

This ad hoc activation of national roaming can be configured according to two different models:

- National roaming is configured but not authorized in neither the home operator's HLR or on the visited network's HLR. When the home operator experiences a network breakdown, national roaming is authorized in the core networks of both parties.

- National roaming is configured and authorized in the home operator's HLR but not authorized in the visited network. In case of outage, the visited network authorizes the national roaming for affected users in order to immediately activate the resilience service.

Of course, in this last case, the visited operator would have to configure specific Reject Cause Value messages, in order not to allow national roaming in case there is no incident. As the scheme needs to work on automatic network selection mode, light reject messages would need to be used. Indeed, with light reject messages, the concerned network does not enter into the forbidden networks list which allows the user to automatically switch to this network in case the location registration request becomes positive (only in case of outage).The Reject Cause Value messages are described in the section 2.3.2.

In both cases described above, national roaming can be authorized by the visited operator at national level or according to Location Area Code (i.e. LAC) or ranges/classes of IMSIs In this last

[46] PTS (2008), Facts about emergency roaming

scenario, national roaming is only activated for the specific geographic area affected by the outage. LACs are configured directly in the core network of an operator and can be defined according to geographic areas, number of users, and group of antennas or specific technical features (e.g. an area covering a railway line).

Cost structure

Costs are billed as defined in the commercial agreement between the providers who enable this capability. It can be a pre-agreed lump sum with the amount calculated in advance based on patterns or on a reciprocal basis where both operators (home and visited) calculate the traffic generated during the outage and the visited network charges the home operator based on some pre-agreed price per minute.

As the service is automatic for customers, they are not required to take any action to switch operators which means that they could not be aware of the change of operators' network. For that reason, customers are charged according to their actual tariff plan as they would have made a call on their home network.

Pros, Cons and issues/challenges

The main benefit of this approach is the assistance to the entire society affected by the outage: every customer affected switches automatically to another network in case of outage of their home operator. This benefit comes without any extra cost to the customer.

However, as a challenge, the visited network has to support an important additional traffic. This peak of traffic could potentially affect the quality of service for the hosting customers. At the extreme, it could potentially create a congestion of network for the hosting operator

Nevertheless as national roaming is configured by LAC it allows a smaller negative impact on service quality for the entire visited operator's base of customers. The visited network has only to support the users communicating in the areas affected by the network breakdown. As a result, it keeps the negative impact of national roaming concentrated in the area affected by the outage.

Lastly, there is a challenge, especially for NRA, to stimulate the operators to conclude such agreements. Indeed, even if they can use the existing international roaming infrastructure (with slightly adapted capacity), the variable costs to support can decrease their incentives to agree on this scheme.

Nevertheless, the working costs avoid any abuses and keep the incentives of operators to develop a resilient and redundant network. Indeed, more resilient is the network, less probable operator would have to appeal to this service.

All in all, this resilient solution is beneficial for the entire society without additional costs for customers. NRA has an important role to play to promote it and stimulate the operators to engage with each other to deploy such a scheme despite their possible important costs.

5.5 Roaming permanently activated by the customer

A second extreme approach to implement national roaming is to set it up permanently between two or more operators. This approach is similar to the international roaming: at any time customers can access the network of another operator which has signed a national roaming agreement with their home operator in order to use mobile communication services. However, this service needs to be activated by the customer and is subject to additional fees.

Australia is the main example of this solution even if the purpose is different in that case (extend coverage in rural areas).

Technical set up

The device connects in priority to its home operator's network to avoid unnecessary costs. In case the network of its home operator is not available, it connects to the second priority network which is the network of the operator which has concluded a national roaming agreement with the home operator. The home operator directly sets up the priority networks in the SIM card of its users.

No reject messages are required if the services has been activated by the customer as the roaming is permanently activated.

This set up works in both automatic and manual mode, depending on the user's preferences.

Cost structure

Costs are billed as defined in the commercial agreement between the providers who enable this capability. In a pre-agreed lump sum, the operators calculate in advance an amount of money to be paid. This amount can be accurately calculated beforehand by well know patterns of traffic for each region and time. As long as that amount is set, then the disrupted operator pays the visited operator that amount after the incident has been resolved. Alternatively, the operators could agree to settle the invoice, based on a reciprocal basis, i.e. they both calculate the traffic generated during the outage and the visited network charges the home operator based on some pre-agreed price per minute.

This service, as a VAS, is supported by the subscribers who request it. The billing method is in line with the international roaming service.

Pros, Cons and issues/challenges

The main advantage is the large ranges of customers who can benefit from this value added service. Indeed, national roaming is always enabled and the customer who wants to ensure a continuous service is in charge of the opt-in and supports the additional costs.

The main disadvantage and challenge is the probable breaches in the market competition. In this scheme the operators are basically federating their networks. This is a highly regulated area by the EU and should be considered only in very specific scenarios for a limited time. The incentives to develop a complete and resilient network can be impacted as user can always choose to which network to roam even besides outages. It also means that operators have less control over the traffic and users on their networks. As a consequence, it is important to set up disruptive fees to avoid users to usually roam on competitors' networks.

In addition, an important popularity of this scheme could cause an overload and threaten the service quality for original subscribers of the visited network. Nevertheless, operators could configure restrictions and prioritize their own customers.

All things concerned, this solution can be easily used out of the scope of resilience by the users. Abuses can easily appear and the threat of competition breaches is important. As a consequence, this solution is not advised by ENISA.

6 Recommendations

In the following recommendations section, you can find a set of actions that could need to be taken to ensure an appropriate level of resilience in electronic mobile communications in your country and be prepared in case of large scale outage.

Recommendation 1: Discuss portfolio of solutions offered

ENISA is aware that each Member State has a different regulatory approach and telecom market. For these reasons this report presents a portfolio of solutions that can be applied based on the different markets and regulations:

- No roaming
- Ad-hoc activation of roaming with manual selection
- Automatic roaming for a fixed set of SIM cards
- Ad-hoc activation of roaming with automatic selection
- Roaming permanently activated by the customer

Member States are invited to use this as a starting point for the discussion of national roaming as a resilience solution with the mobile telecom operators. In this way they can use these options as a basis to tailor their own solution taking into consideration their own legal constraints and needs and agreements among operators. Competent authorities should discuss them with the operators so that national, technical and legal constrains are clear and make sure that operators are aware of the different technical options in case of need.

It is important to stress that national roaming is an appropriate and cost-efficient solution in case of access network breakdown. However, additional measures need to be taken to mitigate issues related to core network breakdowns or other outages not covered by national roaming.

Recommendation 2: Promote National Roaming awareness

Each Member State should work with interested parties such as mobile operators on National roaming solutions awareness in case of outages. It is important that the outcomes of this study are shared among the operators and NRAs of each Member States and appropriate knowledge to face this kind of events is developed. It is of utmost importance that all stakeholders work together to develop countermeasures and mitigation activities to minimize impact of large scale or prolonged outages and to assess the impact on critical infrastructures.

Recommendation 3: Favour mutual aid agreements

One of the most important instruments for operators in facing large scale outages is the definition of mutual aid agreements. Each competent authority should favour this kind of agreement between parties as advanced means of emergency preparedness as this solution allows overcoming legal and competitive barriers and proving to be effective in these scenarios.

Recommendation 4: Identify clear thresholds in case of activation

In case one of the above solutions is selected, ENISA invites the competent authority to define clear thresholds both in users affected and time limit in order to facilitate the emergency response. It is important that these thresholds take into account incident trends and single business continuity plans. Moreover they should also cover emergency engagement procedures and the coordination between operators.

Recommendation 5: Prioritize voice and SMS

Another important recommendation includes services prioritization. In case of activation of national roaming as a resilience solution not all the traffic should be transferred at one time on the other operator in order to avoid congestion. Moreover for the same reason only voice and best effort SMS should be roamed on the second network, leaving data connectivity out of the solution, in order to use cell phones only for emergency communication and avoid overload of the visited network. This is due to the large volume of traffic of mobile connectivity where roaming of data will most likely quickly overload the visited network. For these reasons data connectivity should be backed up by other means such free public Wi-Fi that can be made available in the affected area.

Recommendation 6: Favour open Wi-Fi as alternative solution for data connectivity

Following the previous recommendation, data connectivity should be transferred to available wireless networks. In case of a mobile operator outage, in order to allow data connectivity from mobile devices, free public Wi-Fi hot spots should be considered an option. Visited providers should be allowed to open their proprietary spots in order to alleviate the traffic and allow IP based communications. Moreover also other providers and private citizens should be allowed to open their connectivity in case of outages due to natural disasters as it happened during the 2012 Emilia earthquake[47] emergency, relieving in this way the visited network from a possible congestion and allow its use only for emergency communications.

Recommendation 7: Establish a M2M inventory

M2M communications relying on 2G/2.5G/3G/3.5G/4G are used in public transport automotive, tracking & tracing, remote maintenance & control, metering, POS/payment, consumer electronics, healthcare and security sectors. Outages on a mobile provider could affect these sectors and could have cascading consequences on other critical services and therefore everyday life of large part of the population. Considering the current trend and growth of these technologies it is auspicated that every Member State start to develop with providers an inventory of all these SIMs per service and provider in order to assess the possible impact and define a comprehensive continuity plan in case of outage. This should enable to face a scenario where, for example, the public transport of a major metropolitan area relies on 2G SIMs of a particular provider. When this provider is affected by a major outage disturbing the mobility of millions of people, there should be a timely assessment of the impact and the activation of back up activities.

Recommendation 8: Be prepared for an eventual mobile network outage

The continuous reliance on mobile communication and its expected growth paired with the current trend on incidents requires Member States to be prepared for eventual network outages of mobile providers. Enterprise business continuity plans prove to be efficient but they do not eliminate completely the risk and cascading effects. Member States should consider

- a comprehensive national risk assessment framework that takes into account not only single provider's business continuity plans but

[47] Sharing vs. the earthquake in northern Italy: a cause for hope (2012) http://edgeryders.eu/protecting-and-enhancing-commons/mission_case/sharing-vs-earthquake-northern-italy-cause-hope

- envisions also waterfall effects on the population and critical services as government and public transport for example.

Scenarios like the one in which the affected national mobile provider has a large penetration that includes also

- SIMs used in public utilities and transport
- dykes/dams
- power grids
- MTM controls

should be envisioned and ad hoc back up plan defined.

Recommendation 9: Identify key people within Critical Infrastructure services

Key people and key services should be identified and emergency preparedness plan should be defined accordingly. In facing an emergency, one of the critical steps is to identify the critical services and key people. Member States should build awareness and invite public and private sector to assess their reliance on the mobile network. Moreover they should invite all the possible stakeholders to identify key people within the most critical services and include them into the national risk assessment framework in order to activate back up procedures. Eventually this would require a civil contingency agency or competent organization to keep an updated list of these services and people to be used during emergency.

7 References

EU Legislation

- European Parliament and Council (1998), DECISION No 128/1999/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 1998 on the coordinated introduction of a third-generation mobile and wireless communications system (UMTS) in the Community
- European Parliament and Council (2002), 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)
- European Parliament and Council (2009), DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services
- European Parliament and Council (2012), REGULATION (EU) NO 531/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2012 on roaming on public mobile communications networks within the Union.

Other papers

- 3GPP Organizational Partners (2013), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application (release 12)
- 3GPP Organizational Partners (2009), 3rd Generation Partnership Project : Technical Specification Group Core Network Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (release 9)
- ARCEP (2012), Avis n° 2012-1627 de l'Autorité de régulation des communications électroniques et des postes en date du 20 décembre 2012 sur la demande d'avis de l'Autorité de la concurrence relatif aux conditions de mutualisation et d'itinérance sur les réseaux mobiles
- Bhutan InfoComm and Media Authority (2012), Consultation Paper on National Mobile Roaming, Royal Government of Bhutan
- ENISA (2012), Annual Incident Reports 2011: Analysis of the Article 13a incident reports of 2011
- European Parliament (2006), Technical Issues on Roaming: Transparency, Technical Aspects and Data – Overview related to the proposed regulation on Roaming
- GSMA (2012),Mobile Infrastructure Sharing
- Ministerie Van Economische Zaken – Directoraat general Energie, Telecom & Mededinging (2013), Resultaten Regional Roaming, DGETM-TM / 13061025
- Nepal Telecommunications Authority (2011), Consultation paper on National Roaming, Kathmandu
- Ovum (2013), Country Regulation Overview - Finland
- Ovum (2013), Country Regulation Overview - Italy
- Ovum (2013), Country Regulation Overview - Norway
- Ovum (2013), Country Regulation Overview - Poland
- Ovum (2013), Country Regulation Overview - Sweden
- Ovum (2013), Mobile Phone and Smartphone Forecast 2013–2017, Devices and platform

- Ovum (2012), Country Regulation Overview – Austria
- Ovum (2012), Country Regulation Overview - Denmark
- Ovum (2012), Country Regulation Overview - Ireland
- Ovum (2012), Country Regulation Overview - Spain
- Ovum (2012), Mobile Network Sharing Deals Analyzer: 2H11–1H12, Telco Strategy
- Ovum (2012), Mobile Regional and Country Forecast: 2012–17, Telco Strategy
- PTS (2008), Facts about emergency roaming
- Sutherland E. (2011), The regulation of national roaming, International Telecommunications Society, 18-21 September 2011, Budapest
- Telecom Regulatory Authority of India (2013), Consultation Paper on review of Tariff for National Roaming, New Delhi
- Regional Roaming, Cross-operator strategy for the continuation of primary mobile telecom services during large scale 2G/3G voice outages, T-Mobile, KPN, Vodafone (2013)

Internet pages

- Berry Review (2012), AT&T & T-Mobile Enter Into Emergency Roaming Agreement for Hurricane Sandy, http://www.berryreview.com/2012/10/31/att-t-mobile-enter-into-emergency-roaming-agreement-for-hurricane-sandy/ viewed on the 09/08/2013
- BVI Platinum (2013), CCT Network Woes Continue; Digicel/CCT Reach New Roaming Agreement, http://www.bviplatinum.com/news.php?page=Article&articleID=1357663206 viewed on 08/08/2013
- Fitchard, K. (JUL. 13, 2012), Why are mobile networks dropping like flies? Gigaom, http://gigaom.com viewed on 01/07/2013
- Goldman D. (2011), FCC requires national data roaming for all, CNN Money http://money.cnn.com/2011/04/07/technology/fcc_wireless_roaming/index.htm viewed on the 08/08/2013
- GSMA Intelligence (2013), Data Dashboard, https://gsmaintelligence.com/data/ viewed on 01/07/2013
- Heck J (2013), AT&T wireless customers experience service outages, Business Journal, http://www.bizjournals.com viewed on 01/07/2013
- Kroes N (2013), “I will fight with my last breath”: why we need a telecoms single market, http://blogs.ec.europa.eu/neelie-kroes/telecoms-single-market-ep/ viewed on 02/07/2013
- Renault M (2012), Orange s'explique sur la grande panne de juillet, Le Figaro, http://www.lefigaro.fr viewed on 01/07/2013
- Reuters (2012), Vodafone Dutch service disrupted by fire, Reuters, http://www.reuters.com viewed on 01/07/2013
- Smith, G (2013), Boston Cell Service Unavailable After Marathon Explosion, The Huffington post, http://www.huffingtonpost.com viewed on 01/07/2013
- Spencer B, (2013), Mobile users can't leave their phone alone for six minutes and check it up to 150 times a day, Daily Mail, http://www.dailymail.co.uk viewed on 02/07/13
- Telegeography, Play looks to close national roaming deal with PTC, Telegeography, http://www.telegeography.com viewed on 01/07/2013
- Vodafone Australia, National roaming, http://www.vodafone.com.au/personal/services/coverage/nationalroaming viewed on 08/08/2013

Annex A: Glossary of terms

- AuC: Authentication Center
- BSC: Base Station Controllers
- BTS: Base Transceiver Station
- EIR: Equipment Identity Register
- HLR: Home Location Register
- IMSI: International Mobile Subscriber Identity
- IN: Intelligent Network
- LAC: Location Area Code
- MNO: Mobile Network Operator
- MSC: Mobile Switching Center
- MVNO: Mobile Virtual Network Operator
- NR: National Roaming
- NRA: National Regulatory Authority
- RCV: Reject Cause Value
- SIM: Subscriber Identity Module card
- SLA: Service Level Agreement
- VAS: Value Added Services
- VLR: Visited Location Register

TP-01-13-765-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

doi: 10.2824/25397

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu