CEPT ECC
Electronic Communications Committee

ECC Report 301

Provision of Caller Location Information from Private/Corporate Networks

approved 22 May 2019

0 EXECUTIVE SUMMARY

The purpose of this ECC Report is to draw attention to, and to put focus, on certain aspects of emergency calls from "private/corporate networks". The Report is mainly focused on emergency caller location information from private/corporate networks but also explores the issue of access to public emergency numbers including the pan-European emergency number, 112. The Report aims to raise awareness of these important issues.

For the purposes of this Report, a private/corporate network is an electronic communications network, set up by a legal entity or organisation, which is connected to the public electronic communications networks. In this sense a private/corporate network could be run by any type of organisation such as a company, a university, a municipality, a hospital or an airport, essentially, any legal entity using electronic communications. The term "private/corporate networks" is used to describe this type of network throughout this Report.

A private network could also be run by a private person in their home or properties. Electronic communications networks set up by private persons for the sole use of their families in their homes or in their geographically delimited private property are not considered to be within the scope of this Report.

This Report is a logical follow up to the conclusions of ECC Report 225 [1] on "Establishing Criteria for the Accuracy and Reliability of the Caller Location Information in support of Emergency Services".

Section 6.4.3 of ECC Report 225 provides a solution for the problem under consideration as follows: *"One possible solution might be to establish a procedure to pinpoint calls from business networks, for example by requiring the owner of a corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide a timely location update and route the emergency calls to the appropriate PSAPs. For example, it is possible for the management of the corporate network to manage its own caller location database and provide the appropriate information to the public service provider to route the emergency call to the correct PSAP"*.

At the European Union (EU) level, the legal situation today is that private/corporate networks are considered outside of the scope of the Universal Service Directive which contains provisions for access to emergency services and the provision of caller location information. However, Article 109 of the European Electronic Communications Code (EECC) [3] states that:

"Member States shall promote the access to emergency services through the single European emergency number '112' from electronic communication networks which are not publicly available but which enable calls to public networks, in particular when the undertaking responsible for that network does not provide an alternative and easy access to an emergency service."

This clearly addresses the issue of "access to emergency services" but not the provision of caller location information. Nevertheless, it is reasonable to assume that any regulatory requirement on access to emergency services from private/corporate networks would then lead to further discussions on the provision of caller location information.

The Report examines the current situation in European Conference of Postal and Telecommunications Administrations (CEPT) countries based on a questionnaire circulated earlier in 2018. The questionnaire aimed to gather information on any initiatives implemented at the national level, whether regulatory or voluntary, to deal with access to emergency services from private/corporate networks and the provision of emergency caller location information. It was considered that national level regulation in some countries, other than electronic communication regulation, may contain provisions that oblige private/corporate networks to ensure access to emergency services and to provide caller location information.

The Report also describes the technical aspects of providing of caller location information using Internet Protocol (IP)-based protocols and work around solutions that may be implemented where legacy network technology is used. Some country-specific case studies are described.

The Report concludes that there is an issue with caller location information from private/corporate networks and as these types of networks are typically used in places of employment, the safety and wellbeing of employees is paramount. There is no harmonised legal framework that adequately addresses this issue at present. However, the EECC does contain a provision that requires Member States to "*promote the access to emergency services through the single European emergency number '112'".*

Member States will have until the end of 2020 to transpose the EECC into national law and it will be interesting to see how this provision *"to promote access"* is implemented across Europe and if the situation regarding caller location information for emergency calls from private/corporate networks improves materially. Member States will have flexibility in how they implement this provision at the national level.

Therefore, the Electronic Communications Committee (ECC) will consider an update of this Report in due course after the impact of the EECC's provisions has been assessed following transposition.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Explanation
CEPT	European Conference of Postal and Telecommunications Administrations
CLI	Calling Line Information
DDI	Direct Dial In
EC	European Commission
ECC	Electronic Communications Committee
EECC	European Electronic Communications Code (entered into force on 20 December 2018)
ECRIT	Emergency Context Resolution with Internet Technologies
EENA	European Emergency Number Association
ES	ETSI Standard
ESO	European Standards Organisations
ESRF	Emergency Service Routing Function
ETSI	European Telecommunications Standards Institute
EU	European Union
FICORA	Finnish Communications Regulatory Authority (Now Traficom)
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IP PBX	Private Branch Exchange with Internet Protocol connectivity
ISDN	Integrated Services Digital Network
LO	Location Object
Loc-ID	Location-ID
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NGN	Next Generation Network
NRA	National Regulatory Authority
NTP	Network Termination Point
PABX/PBX	Private Automatic Branch eXchange
PIDF-LO	Presence Information Data Format Location Object
PSAP	Public-Safety Answering Point
PSTN	Public Switched Telephone Network
PT ES	Project Team Emergency Services established by the CEPT/ECC's Working Group Numbering and Networks
RFC	Request for Comments
SIP	Session Initiation Protocol
SOS DB	SOS Data Base

URI	Uniform Resource Identifier
USD	Universal Service Directive
UUI	User to User Information
VoIP	Voice over IP
VPN	Virtual Private Network

1 INTRODUCTION

The purpose of this ECC Report is to draw attention to, and to put focus, on certain aspects of emergency calls from "private/corporate networks". This Report is a logical follow up to the conclusions of ECC Report 225 [1] on "Establishing Criteria for the Accuracy and Reliability of the Caller Location Information in support of Emergency Services".

1.1 FINDINGS IN ECC REPORT 225

Chapters 6, 7 and 8 of ECC Report 225 examine the different characteristics of providing caller location information for emergency calls originating on fixed, mobile and nomadic voice services and the merits of the various technologies available. However, the issue of location data for routing is only addressed in Chapter 6 (related with fixed services) and more specifically in Section 6.4.3 ("Corporate networks and building complexes") where several points on the topic are presented. There is also some information in Chapter 8 related to nomadic services.

From the relevant points of Section 6.4.3, ECC Report 225 provides a solution for the problem under consideration as follows: *"One possible solution might be to establish a procedure to pinpoint calls from business networks, for example by requiring the owner of a corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide a timely location update and route the emergency calls to the appropriate PSAPs. For example, it is possible for the management of the corporate network to manage its own caller location database and provide the appropriate information to the public service provider to route the emergency call to the correct PSAP"*.

In Chapter 8 of ECC Report 225, it is concluded that it should be possible to significantly improve on the provision of caller location information for nomadic Voice over IP (VoIP) services once the M/493 standardisation work has been successfully completed within European Telecommunications Standards Institute (ETSI). The relevant conclusion states that: *"it should be possible to establish a procedure to pinpoint calls from business networks where nomadic services are provided, for example by requiring the owner of a corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide timely location update and route the emergency calls to the appropriate PSAPs"*.

1.2 AIMS AND SCOPE OF WORK ADDRESSED IN THIS REPORT

Publicly available electronic communications service providers have clear regulatory obligations regarding access to emergency services and the provision of caller location information for emergency calls. Providing access to public emergency numbers from private/corporate networks is not addressed in telecommunications legislation. Some countries, such as Finland, have introduced regulation in this area and these nationally specific scenarios are described in Chapter 5.

Ideally, dialling rules should be established from within private/corporate networks to accommodate emergency services short numbers, such as 112, and calls to emergency services should display a valid and dialable Calling Line Identification (CLI). CLI can also play an important role in providing location information. Each terminal within a private/corporate Private Automatic Branch eXchange (PABX) network has an internal extension number which could form part of a Direct Dial In (DDI) telephone number. For example, a PABX network could have a 5-digit internal numbering plan. Those 5 digits could correspond to the last 5 digits of an E.164 telephone numbering range. When external calls are made, a unique CLI for each individual extension could be presented to the Public Switched Telephone Network (PSTN) and the extension number could correspond to an actual location within the corporate premises from which the call originated. For emergency calls, this is important when compared to the practice of presenting a single "lead number" as CLI for all calls originating within a private/corporate network where no reliable information is provided to the Public-Safety Answering Point (PSAP) to determine caller location. Chapter 2 describes proposed legislation at the European level which may lead to mandatory requirements on private/corporate networks to ensure access to public emergency numbers in the future.

This Report is mainly focused on emergency caller location information from private/corporate networks but also explores the issue of access to public emergency numbers.

2 DEFINITION OF A PRIVATE/CORPORATE NETWORK.

Private networks were typically wireline networks set up for the sole internal use of an organisation established on a delimited geographical area. Private networks were often referred to as corporate networks. In this sense a corporate network could be run by any type of organisation such as a company, a university, a municipality, a hospital or an airport, essentially, any legal entity using electronic communications. A private network could also be run by private persons in their homes or properties. Corporate networks were typically connected to public networks at various points to facilitate national and international communications. This connection with the public network was usually defined by a number of entry lines in the routing tables of a PABX agreed with the service provider which defined rules to allow for communications with the public network. Without this connection to the public network, the corporate network was in fact a closed user group invisible to, and thus unreachable from, the public network.

Corporate networks were centralised or distributed depending on the organisation's size and geographic footprint. Distributed corporate networks were typically connected via wireless point-to-point links or leased lines connecting different sites under strict usage rules set by the authorities and under commercial agreements with service providers. The location of an emergency call originating from a corporate network was defined by the installation address or terminating point of the public line(s) connected to the corporate network. All communication within a corporate network remained within the predefined geographical boundaries of the site, whether centralised or distributed.

The liberalisation of the electronic communication market and the introduction of new technologies now facilitate a very diverse range of topologies for corporate networks using fixed, mobile and IP-based technologies. Various sites of a single organisation can now be linked and communications unified over different sites in a single, virtual entity which is spread out over different geographical sites which can be situated in different countries across the globe. The connection point with the public network can now be situated at a single site of the corporate network. An emergency call originating from such a network will "break out" at the site where the connection point with the public networks is established, usually creating the impression for the emergency services that the emergency assistance is needed at the break out site.

In many countries during the liberalisation process, private networks were often defined by the negation of the definition of public networks. This created some ambiguity as to the nature of private networks and where the border existed between the private network and the public network. Question arose regarding the extent to which such a network was truly private and whether or not certain obligations relevant to public networks should apply. At some point a private network was considered a network not crossing the public domain. This definition is useful, for example, when considering the internal cabling of an apartment building: A service provider connecting a subscriber in that building through that cabling infrastructure is extending the public network to the termination point in the end user's premises. The use of wireless technology makes this process even more ambiguous as the wireless signal very often extends into the public domain.

Nowadays, technologies allow for an employee to be able to work at any site of an organisation while keeping a single, unique identification within the corporate network. When handover between (wireless) base stations of the corporate network occurs, this use is called mobile. When the connection is fixed for the duration of the communications or work session, be it wireline or wireless, this is referred to as nomadic use. Some organisations do not even have a central physical location, but link all their employees by a virtual corporate network which is now commonly offered as a service by electronic communications service providers. The challenge in either of these scenarios is to determine the geographical location of an employee initiating an emergency call.

In the last few decades, the concept of a private network evolved from a well-defined and limited network allowing for electronic communications between the members of a group of people situated in a delimited, single geographical area; to a service for a group of people that can communicate in a privileged way with each other but who benefit from all the features of a public network and appear to be an integral part of it to the those who are not part of it.

For the purposes of this Report a private network is an electronic communications network set up by a legal entity or organisation, which is connected to the public electronic communications networks. Corporate networks are usually operated by organisations or companies and are considered to be private networks in

this Report. The term "private/corporate networks" is used to describe this type of network throughout this Report. Electronic communications networks set up by private persons for the sole use of their families in their homes or in their geographically delimited private property are not considered to be within the scope of this Report.

3 LEGAL FRAMEWORK

3.1 EU LEVEL

The regulatory approach to private/corporate networks may vary from country to country.

At an EU level, the legal situation today is that private/corporate networks are considered outside of the scope of the Universal Service Directive (USD). This was confirmed by the European Commission (EC) in 2013 in a reply to a parliamentary question on 112 calls from private networks [2] which stated: *"Article 2 of the framework Directive defines 'end-user' and 'user' as a person using or requesting a 'publicly available electronic communications service'. Persons who call within 'private' networks would not qualify as persons who use publicly available electronic communications services. Accordingly, the scope of the Universal Service Directive does not extend to 'private' networks. Therefore the Universal Service Directive does not oblige Member States to ensure the right to access to the 112 emergency number for persons using 'private' networks. These private networks often have, however, their own emergency numbers and personnel which serve as an interface with the public emergency services".*

According to the EC interpretation, a user calling within a private network is not an "end-user" as defined in the Framework Directive Articles 2 (h) and (n). Therefore the obligation in Article 26 of the USD would not apply.

However, Article 109 of European Electronic Communications Code (EECC) [3] states that:

"Member States shall promote the access to emergency services through the single European emergency number '112' from electronic communication networks which are not publicly available but which enable calls to public networks, in particular when the undertaking responsible for that network does not provide an alternative and easy access to an emergency service."

This provision clearly addresses the issue of "access to emergency services" but not the provision of caller location information. Nevertheless, it is reasonable to assume that any regulatory requirement on access to emergency services from private/corporate networks would then lead to further discussions on the provision of caller location information from private/corporate networks also. The ECC will monitor these developments closely.

3.2 NATIONAL LEVEL WITHIN CEPT MEMBER COUNTRIES

In order to better understand the situation within each European Conference of Postal and Telecommunications Administrations (CEPT) country, a questionnaire was circulated on 5 March 2018. The questionnaire aimed to gather information on any initiatives implemented at the national level to deal with emergency calls originating on private/corporate networks and emergency caller location information. It was considered that national level regulation in some countries, other than electronic communication regulation, may contain provisions that oblige private/corporate networks to ensure access to emergency services and to provide caller location information. There were 15 responses from 14 CEPT countries to the questionnaire.

3.2.1 Provision of access to emergency services from private/corporate networks

In almost all countries who responded to the questionnaire it is possible to call emergency services from private/corporate networks. Three respondents who did not answer the specific question stated that it was probably the case but, as it is not a matter for electronic communications regulation, no statistics are available. Therefore, it cannot be confirmed if it is possible from all private/corporate networks. One respondent also noted that, for caller location, the location information provided to the PSAP referred to the public network termination point. One respondent stated that as the private/corporate network is connected to the PSTN, the call leaves the private network and becomes a PSTN call and therefore access to emergency services should be provided.

Nine respondents to the questionnaire consider calls to emergency services from private/corporate networks to be a subject for telecommunications legislation in their respective countries while 5 respondents considered it not to be a regulatory matter. Finland, Norway, Slovenia and Switzerland all responded "Yes" to this question and further details of the legislative provisions and technical solutions implemented in these countries are discussed in Chapter 5. One respondent again commented that when the call is passed to the PSTN it becomes a matter for telecommunications legislation while another respondent stated that the call is treated like any call to emergency services that originates on a fixed or mobile network.

Of those countries who responded that calls to emergency services from private/corporate networks are not a subject for telecommunications legislation in their respective countries, facilitating access to public emergency numbers is provided on a voluntary basis without legislation or guidelines.

3.2.2 Provision of caller location information for emergency calls originating on private/corporate networks

Respondents were asked if it was possible to provide caller location information for calls to public emergency numbers made from within private/corporate networks to the emergency services. Nine respondents stated that it was possible while four respondents stated that it was not. One respondent stated that the information provided by the operator refers to the public network termination point which, of course, may not be reliable in a distributed private/corporate network. In Finland, the manager of the private network together with the responsible telecommunications operator must ensure that the location information is available. In Sweden, a database exists with calling party numbers and address information. The PSAP can get address information from this database. If a local telecom network is configured so that local extension numbers are sent with the call then that information about the number is available in the address database and the right location can be ascertained. However, in most cases this is not implemented. A similar database is implemented in Spain which contains the physical address of the Network Termination Point (NTP) and the associated numbers or blocks of numbers. In Norway, there are some public network providers that have their own databases that can be populated with end user location information by the private/corporate network. The Slovak Republic stated that it would be possible to provide caller location information if the operator of the private network would update their service provider with the correct information. Switzerland has a solution based on Location-ID (Loc-ID) which is discussed in further detail in Chapter 5.

Although it is currently not possible to provide additional location information for emergency calls from private networks in Germany, the transmission of caller location information provided by the subscriber side is specified for Session Initiation Protocol (SIP)-based services in the new technical directive on emergency calls which came into force in 2018. Service providers must implement these requirements within the next three years.

On the question of whether or not caller location information for calls to public emergency numbers made from within private/corporate networks is specifically a subject of telecommunications regulations, only Finland, Norway, Slovak Republic and Spain stated that it was a regulatory matter and provided links to the relevant regulations. Where caller location information is not specifically a subject of telecommunications regulations but is available, three respondents stated that it is on a voluntary basis without legislation or guidelines.

3.3 RULES FROM OTHER AUTHORITIES

In most, if not all, CEPT countries there are general legislative provisions or guidelines to safeguard the health and safety of employees in the workplace. An authority at the national level is normally responsible for ensuring compliance with the legislation or guidelines (e.g. Health and Safety Executive (United Kingdom) and Health and Safety Authority (Ireland).

In some countries there may be health and safety provisions which cover calls to emergency services from the workplace. In Germany for example, the Occupational Safety and Health Act (Arbeitsschutzgesetz, ArbSchG) [15] requires that the employer shall ensure that in an emergency the necessary contact to agencies outside of the establishment, in particular as regards first aid, emergency medical care, rescue work and fire-fighting are established. Belgium has a similar obligation in legislation on safety and wellbeing in the workplace.

4 LOCATION DATA FOR EMERGENCY CALLS FROM PRIVATE/CORPORATE NETWORKS

This section of the Report deals with emergency caller location information from national private/corporate networks and private/corporate networks that cross national borders. A number of scenarios are described.

4.1 PRIVATE/CORPORATE NETWORKS WITH DISTRIBUTED LOCATION

Emergencies can happen anywhere, at any time. When they do occur, citizens usually react by grabbing the closest communications device and calling 112, or whatever national public emergency number is known to them, for help.

Many companies have offices in different locations and these offices may be connected through an internal network, where only a single office (e.g. the national headquarters of a company) or a subset of offices (e.g. head office and main subsidiary offices) is connected to the public telephone network. Thus, 112 calls placed from remotely connected offices could be answered by a PSAP serving a different geographical area. The private/corporate network owner and the public network provider should cooperate so that the architecture allows correct routing of the emergency calls. Further, this cooperation should aim to ensure correct location information is presented at the PSAPs.

The problem is similar when a citizen is calling from, for example, a university campus or a building complex. The address stored in the customer database for the originating telephone number is often the address of the main building (i.e. a billing address) and not the actual location of the office or the location where the call was initiated.

As described in ECC Report 225 (section 6.4.3), one possible solution might be to establish a procedure to pinpoint calls from business networks, for example by requiring the owner of a corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide a timely location update and route the emergency calls to the appropriate PSAPs. For example, it is possible for the management of the corporate network to maintain an internal caller location database and provide the appropriate information to the public service provider to route the emergency call to the correct PSAP.

4.2 EMERGENCY CALLING FROM MOBILE EXTENSIONS

Mobile operators now offer services which provide a company with an internal virtual mobile network where it is possible for employees to use mobile handsets to contact each other on internal extension numbers. In case of emergency calls from mobile handsets that are mobile extensions, it is advisable that the handset defaults to the public mobile network when an emergency number is dialled. With this approach the correct calling line identification for the public network (i.e. the correct mobile number rather than just an internal extension number) is displayed. PSAPs will then receive a valid and dialable CLI with the emergency call and also handset-derived or network-derived caller location information.

4.3 LOCATION DATA FOR ROUTING EMERGENCY CALLS TO REGIONAL PSAPS

Besides the provision of caller location information to the PSAP, which may be tolerant regarding delays of tens of seconds, the proper routing of the emergency call to the regionally responsible PSAP is an additional challenge. The provision of location information required for routing must not delay the call setup significantly as every second counts in an emergency situation. The necessary information for routing needs to be preconfigured in the originating networks, if routing to regionally responsible PSAPs is required.

4.4 CROSS-BORDER ROUTING OF EMERGENCY CALLS

Emergency calls from multi-national corporate networks may require that call setup in the public telephone network has to cross national borders. This is in general not supported for the time being. The group ECRIT (Emergency Context Resolution with Internet Technologies) of IETF (Internet Engineering Task Force) developed RFCs (Request For Comments) to support emergency calls in the Internet [7] and an addressing scheme for the different PSAP types (fire brigade, ambulance, etc.) [6] [5]. However, these RFCs have not yet been implemented in the Next Generation Network (NGN) interconnection interfaces of the large telephone network providers. Emergency calls are in general considered as national calls and international switches are configured to block international calls to national short numbers (e.g. +32112 for Belgium would be blocked).

National connections (exits) to the public telephone network for each national segment of a multi-national corporate network can be considered as a work-around for this issue of cross-border emergency calls (i.e. local breakout to the public network just for emergency calls).

4.5 TRUST IN NETWORK-PROVIDED AND USER-PROVIDED LOCATION INFORMATION

PSAPs use location information coming from different sources. Network provided information is described in Chapter 4 of this Report. Location data can also be provided by the terminal equipment where available. Location information can also be provided by the user during the call.

If emergency calls are made from a PABX network, the location information provided to the PSAP is generally the 'installation address' of the network, which is often the head office address. If an emergency call is made from an organisation with many branches, it is generally not the branch address, which is provided to the PSAP, but rather the head office/installation address.

This could have disastrous consequences for an emergency caller as the call could be routed incorrectly and/or emergency resources could be dispatched to the incorrect address because such routing and dispatch decisions are based on the address that is presented to the PSAP. As mentioned before, a possible solution is to require the owner of a private/corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide a timely location update for, and route the emergency calls to the appropriate PSAPs.

Network-provided location information can be considered as trusted but PSAPs will also consider location information provided verbally by the caller and/or handset-derived location information provided by the terminal equipment before dispatch decisions are made. In case of false calls the user-provided location information, and sometimes hacked or manipulated location information provided by the terminal, are intended to disguise the actual location of the emergency call.

5 TECHNICAL ASPECTS

5.1 GEOLOCATION HEADER IN SESSION INITIATION PROTOCOL (SIP) TRUNK SPECIFICATION

As already outlined in ECC Report 265 [8], the Session Initiation Protocol (SIP) is a communications protocol commonly utilised for VoIP. SIP has the advantage that with its Geolocation header field it can submit more location information to the PSAP during call setup than with Public Switched Telephone Network (PSTN) / Integrated Services Digital Network (ISDN). The SIP Geolocation header field is defined in Request for Comments (RFC) 6442 [9] and RFC 4119 [10] defines the Presence Information Data Format – Location Objects (PIDF-LO), which contain the location information in Multipurpose Internet Mail Extensions (MIME) bodies. RFC 5139 [11] describes PIDF-LO types and RFC 5491 [12] describes how to constrain, represent and interpret location information in a PIDF-LO.

RFC 6442 [9] specifies three SIP header fields:

- Geolocation, which carries a reference to a Location Object (LO);
- Geolocation-Routing, which grants permission to route a SIP request based on the location value;
- Geolocation-Error, which provides error notifications specific to location errors.

Private/corporate networks are mostly connected to the public telephone networks via SIP trunks, which can support many phone calls in parallel. The SIP Forum's technical recommendation SIP connect version 2.0 [13] provides a basic set of specifications for SIP trunks. This specification outlines the specific requirements for emergency calls including the specific use of the Geolocation header field to convey location information from the private network, which may enable the service provider to route an emergency call to the appropriate, regionally responsible PSAP.

5.2 SOLUTIONS FOR PSTN AND ISDN

Private/corporate networks typically use Direct Dial In (DDI) to handle incoming calls and to distinguish outgoing calls if necessary. The DDI digits, which identify the individual extensions of a PABX, can be used to provide additional information in the calling party number field when establishing emergency calls towards the serving public network. This may help the telephone service provider identify the location of the caller if appropriate information had been previously exchanged between the company holding the PABX and the public network operator at the time the trunk line is commissioned.

The solutions described in Section 4.5 below work for VoIP as well as for PSTN and ISDN.

5.3 TRANSPORT OF LOCATION INFORMATION FROM DIFFERENT SOURCES IN THE "PUBLIC TELEPHONE NETWORK"

ISDN provides options to transport location information but in the past it was not considered to transport location information from different sources (although possible with Location Number and User to User Information (UUI) parameters in parallel). As ISDN is phased out, it is reasonable not to consider this network technology for future enhancements to support the transmission of location information from private/corporate networks side by side with location information provided by the public network. With Voice over IP (VoIP), more options are available and this is also due to the fact that location information can be transported using header fields in SIP with the call setup messages and in parallel using Internet Protocol (IP) connectivity to transport location with other protocols e.g. HELD (RFC 5985) [16]. Managing different transport mechanisms simultaneously requires a more complex architecture like the one for ETSI ES 203 178 [17].

The protocol SIP alone already provides means to handle location information from different sources because this protocol allows the presence of more than one geolocation header fields in a SIP-INVITE message and even more than one location objects (PIDF-LO with one geolocation header field. Different sources could be distinguished by using the different PIDF-LO types ("tuple", "device" or "person") but it

seems more appropriate to use the newly defined "location source parameter" as outlined in draft RFC "Location Source Parameter for the SIP Geolocation Header Field [19]. This parameter is utilised in the ETSI M/493 related standard ETSI ES 203 283 [18]. Using the location source parameter has the advantage that call control entities processing the SIP messages don't have to dig into the PIDF-LO, which is an XML element attached to the SIP INVITE, but finds information about the location information source in the Geolocation header field itself.

5.4 ETSI M/493

As already outlined in ECC Report 225, the European Commission mandated ETSI to develop standards to overcome the issue of estimating the location of a nomadic caller (Mandate M/493 “Standardisation Mandate to the European Standards Organisations (ESO) in support of the location enhanced emergency call service“). In a first step ETSI developed a functional architecture which covers all parties (network and service providers) involved in an emergency call, and outlines all the necessary information which needs to be exchanged. In a second step of the work according to M/493 the protocols for the interfaces and entities of the defined architecture have been developed.

The architecture focuses on public networks and public service providers, but could be extended to private networks as well. Annex A of ETSI ES 203 178 [17] defines an extension to the main architecture and *"how to handle network elements that change packet flow identity information between the access network and the VSP call control. These network elements that include NAT/PAT devices and VPN tunnel endpoints are ... referred to as FlowChangers".* The Network Address Translation (NAT) between a corporate network and the public network or a Virtual Private Network (VPN) tunnel for a corporate network connection can be considered as a FlowChanger. The mechanism defined in A.2 and A.3 of ETSI ES 203 178 can be applied to help with the estimation and transport of caller location information in corporate networks as well.

The work on the protocols for the individual interfaces of the architecture in ETSI ES 203 178 was finalised in November 2017, and the results were published in ETSI ES 203 283.

5.5 WORK AROUNDS

For each location of a private/corporate network, local exits to the public network for emergency calls could be considered as a workaround for the location information and routing problem. In case of international private/corporate networks at least one exit per country could help to avoid cross-border routing.

Also the use of a mobile handset with a basic mobile voice service at the work place for emergency calls only will provide basic location information (Cell-ID) to the locally responsible PSAP.

5.6 TECHNICAL SOLUTIONS

In Chapter 2, a summary of the results to an ECC questionnaire are discussed. The questionnaire results also provided information on technical solutions implemented in some countries to deal with caller location information from private/corporate networks. These solutions are described in the following sections of this chapter. As these are national solutions, cross-border routing of emergency calls, which could be necessary for multi-national private/corporate networks, are not covered.

5.6.1 Finland

In Finland the National Regulatory Authority (NRA), Traficom, can only regulate the public network. It’s regulation 33 E/2011 M [20] defines how the public network must route the emergency calls from private networks if appropriate information is received from the private network, according to FICORA's recommendation Rec 309/2014 S [21]. This recommendation contains guidelines for routing emergency traffic from corporate networks. Corporate networks mean here a corporate network's internal IP networks, PABX networks and other corresponding networks. The recommendation is mainly targeted at telecommunications operators and holders of corporate networks. Hereafter are the main points of this recommendation:

5.6.1.1 Emergency traffic from corporate networks

If the private network knows the location of the caller it is recommended that the called number is in a format

3979 abc 112

where *3979* is a part of a subscriber range reserved for this purpose by FICORA and abc is the code for the municipality where the appropriate PSAP is situated.

The interface exchange of the public network receiving this number format will make the number conversion from *3979 abc 112* to a hexadecimal routing number *0X(Y) 0C abc 112* which is the format that the public network uses when routing emergency calls:

- *0X(Y)*: the area code to the telecommunications area where the PSAP is situated;
- *C*: the hexadecimal character C;
- *Abc*: the code for the municipality where the appropriate PSAP is situated.

Upon agreement on a corporate connection to the public telephone network, it must be ensured that the gateway exchange can handle the relevant emergency routing numbers originating from a corporate network.

5.6.1.2 Location determination in private networks

There are different options how the location can be determined in the private network (private network responsibility that the information is correct but not regulatory issue):

- automatic network functions (in that case the holder of a corporate network is responsible for ensuring that the emergency call routing numbers transferred from the corporate network to the public telephone network correspond to the emergency caller's geographical position. The holder of the corporate network must inform users of possible restrictions);
- manual setting by the private network operator based on installation site;
- municipality setting by the user himself.

There is also a recommendation that when the private network is implemented using mobile phones (e.g. virtual private network) emergency calls are routed directly via the mobile network and the calling number is the mobile number of the customer (this way it is possible to use the normal location system of the public network).

5.6.1.3 Emergency call dialling

It is recommended that in private networks the user can make an emergency call in both of the following ways:

- By dialling only 112;
- By dialling a prefix for outgoing traffic and 112.

5.6.2 Switzerland

In Switzerland, the technical and administrative regulations on emergency call requirements apply to all telecommunication service providers who offer the publically available telephone service. They specify the routing of emergency calls from the calling fixed network or mobile telephone subscribers to the alarm centres (PSAPs) of the police, the fire brigade, the Samaritans, ambulance services and helplines for children and young people. They regulate how an emergency call at the interconnection interface is forwarded from one telecommunication service provider to another and how identification of the caller's location is transferred to the emergency services. These regulations exclusively concern emergency calls, i.e. calls to numbers *112, 117, 118, 143, 144* and *147*.

As part of this regulation, special dispositions for private/corporate networks were specified, mainly for the PSTN/ISDN technology. For the routing of emergency calls public telephone service providers must delegate

tasks by contract to their customers who operate a private/corporate network in Switzerland with several internally linked sites. For example, they are allowed to select a location number or the routing number themselves, and to finally forward the emergency call via the subscriber/network interface. The routing numbers, including the prefix *989*, cannot be chosen by customers on their handsets, such connection attempts must be intercepted and rejected.

If tasks are delegated to users as part of the routing of emergency calls, these users must be carefully informed and instructed in detail on these tasks and on the application, by analogy, of the prescriptions and their annex.

Then, on the horizon of the migration from PSTN to IP technology, the impact on emergency calls passed from private/corporate networks became significant. VoIP emergency calls from anywhere in Switzerland arrived in PSAPs unrelated to the caller's location, this being due to the only consideration of the location of the VoIP gateway. Historically (PSTN technology) this was not an issue for the PSAPs, as the phone numbers were assigned to fixed lines, regardless of the access network, allowing to track the location and address for any phone number. As a result of the migration, the Swiss incumbent (Swisscom), was quickly confronted with the pressing demand of its large customers for a reliable solution allowing the correct location and routing of emergency calls passed from networks from large companies using VoIP telephony.

In coordination with the development of the ETSI ES 203 178 [17] and ES 203 283 [18] standards and with SIP INVITE Swisscom has therefore developed an interesting solution based on the introduction of a simple concept: a Location-ID (Loc-ID). The VoIP service customers get a Loc-ID per location and are responsible to assign it to its IP-range. In accordance with ES 203 178 and ES 203 283 there is a clear separation of functions between the access network provider (responsible for positioning) and the VoIP service provider (responsible for querying the Location-ID or Location Reference from the access network and for the routing of the emergency calls).

This solution, offered now by Swisscom to its business customers (private/corporate networks) using compatible Private Branch Exchange with Internet Protocol connectivity (IP PBX) (Swisscom requires from the IP PBX manufacturer/suppliers information how their systems support this solution and the new abovementioned ETSI standards), covers the most important requirements for a correct treatment of the VoIP emergency call:

- identify an emergency call;
- generate routing information from the location information;
- retrieve the associated site ID (Location Reference in the related ETSI standards);
- transmit the location ID in the call setup (SIP INVITE);
- call back to the emergency caller by the PSAP, based on the presented caller number;
- support all Swiss national emergency numbers (112, 117, 118, 144, 143, 147, 1414) without restriction.

The solution is based on three key components: one is the configuration of the Loc-ID in the access networks, the second is the determination of the Loc-ID during an emergency call and the third is the transport of the Loc-ID.

The process works in this way:

- A company obtains a VoIP Location-ID (Loc-ID) for each of its locations/subsidiaries at the centralised address registry (SOS Database at Directories). The Loc-ID is assigned to the IP addresses of the branches in the IP PBX. The assets (addresses: Loc-ID) are stored in the Emergency Service Routing Function (ESRF) of the Emergency Call Service Provider (Swisscom in this case);
- An emergency call is passed via VoIP;
- The IP PBX detects the call and adds the corresponding Loc-ID to the SIP header;
- The ESRF resolves from the given Loc-ID the responsible emergency region and determines the call routing to the PSAP, which is returned to the VoIP Gateway;
- Utilising the Loc-ID, the ESRF resolves the actual location (address) where the call originated and sends it to the SOS Database;
- The PSAP looks up the location/address using the telephone number (CLI) as the key;

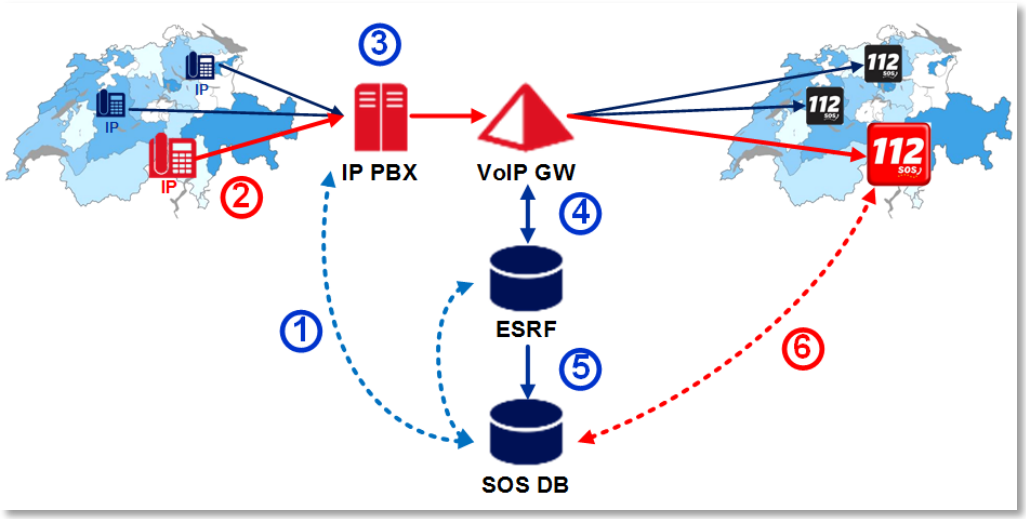

Figure 1: Principle of the VoIP Location-ID (Loc-ID)

The Loc-ID is an index to an 8-digit decimal number between 10.000.000 and 99.999.999, like a number plate. These plates, of course only virtually, are installed anywhere in the private network where the VoIP phones are connected and channelling the number and the coordinate. Unlike coordinate and address elements a Loc-ID is more easily transported through the various protocols. The Loc-ID includes location information for at least geographic coordinates and address. In a recovering or moving of the site a new Loc-ID must be obtained.

Table 1: Example of Loc-IDs with physical references

VoIP Location-ID	Coordinate	Address
16594730	7.248o, 47.133o	Rue de l'Avenir 44, 2501 Bienne
24558793	7.059o, 47.134o	Summit of Chasseral
12964881	7.334o, 46.222o	Hangar 1, Sion Airport, 1950 Sion
33878401	6.958o, 46.062o	Bottom station, Cable car Vertic Alp, 1925 Le Châtelard
19732456	9.836o, 46.499o	Chalet Alfredo, 7500 St. Moritz

The advantages of the Loc-ID are:

- addresses can change at any time;
- loc-ID work also for "non-existing" addresses like e.g. airport-buildings, dams, bunkers;
- allows to localise additional buildings at one address;
- assigned phone numbers or URIs can change at any time;
- loc-ID is bound to geographical objects (points, lines, polylines, polygons);
- loc-ID is supported within LS of IP PBX;
- resolution from Loc-ID to address is fast;
- loc-ID is not an internal address-ID of operators.

The only disadvantage of this solution is the administrative overhead of managing the location database.

5.6.3 Norway

The owner of the private/corporate network is closest to having knowledge on the whereabouts of the different terminals and to maintain a database/register of this information. This semi-static information can

either be transmitted to the public network access provider, or the owner of the private/corporate network can directly insert and maintain information through a dedicated interface provided by the access provider. This could be a web-interface to the provider's database/register or to a national centralised database. In both cases, these databases must be accessible for the PSAPs whenever emergency calls are received. In both cases, there must be some cooperation between the owner of a private/corporate network and the provider of the public network access. Thus, the responsibility for these solutions is common and shared. In combination to this, and in order for the emergency call to be routed to the nearest PSAP, the operator terminating emergency calls distributes to the originating access provider a table of long numbers of the local PSAPs in the different areas, so that the calls can be geo-routed. Such solutions are partly in operation in Norway.

5.6.4 Belgium

In Belgium, a number of operators offer solutions for routing an emergency call originating within a private/corporate network to the geographic competent PSAP.

A first solution is creating a local break-out from the router/PABX at a site. The result is that the call breaks out to the local publicly available electronic communications network and thus will be routed to the PSAP closest and competent for dispatching help to the site. The PSAP may require additional information as it will usually get the address of the reception on site, and of course, the site may be quite large.

A second solution is that the local postal code is embedded in the signalling information of the call when it is delivered to the PSAP receiving the call. Based on that information the PSAP re-dispatches the call to the PSAP closest to the location of the emergency call. Again, the PSAP handling the emergency call has to request additional information for being able to dispatch help correctly. Both solutions are acceptable and workable for the emergency services.

6 CONCLUSIONS AND OUTLOOK

It is clear that there is an issue with caller location information from private/corporate networks and as these types of networks are typically used in places of employment, the safety and wellbeing of employees is paramount. There is no harmonised legal framework that adequately addresses this issue at present. The EECC contains a provision that will require member states to *promote the access to emergency services through the single European emergency number '112' from electronic communication networks which are not publicly available but which enable calls to public networks, in particular when the undertaking responsible for that network does not provide an alternative and easy access to an emergency service."*

Member States will have until the end of 2020 to transpose the EECC into national law and it will be interesting to see how this provision *"to promote access"* is implemented across Europe and if the situation regarding caller location information for emergency calls from private/corporate networks improves materially. Member States will have flexibility in how they implement this provision at the national level.

Therefore, the ECC will consider an update of this Report in due course after the impact of the EECC's provisions has been assessed following transposition.

ANNEX 1: LIST OF REFERENCES

[1] ECC Report 225: "Establishing Criteria for the Accuracy and Reliability of the Caller Location Information in support of Emergency Services", October 2014"

[2] Answer provided on behalf of the European Commission to a parliamentary question from Mr. Phil Prendergast MEP on the subject of 112 calls from private networks, available here

[3] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code(Recast)

[4] RFC 5012: "Requirements for Emergency Context Resolution with Internet Technologies",January 2008

[5] RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", January 2008

[6] RFC 5069: "Security Threats and Requirements for Emergency Call Marking and Mapping", January 2008

[7] RFC 6443: "Framework for Emergency Calling Using Internet Multimedia", December 2011

[8] ECC Report 265: "Migration from PSTN/ISDN to IP-based networks and regulatory aspects", May 2017

[9] RFC 6442: "Location Conveyance for the Session Initiation Protocol", December 2011

[10] RFC 4119: "A Presence-based GEOPRIV Location Object Format", December 2005

[11] RFC 5139: "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", February 2008

[12] RFC 5491: "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", March 2009

[13] "SIPconnect Technical Recommendation Version 2.0", December 2016

[14] Recommendation FICORA 309/2011 S: "ROUTING OF EMERGENCY TRAFFIC FROMCORPORATE NETWORKS"

[15] Act on the Implementation of Measures of Occupational Safety and Health to Encourage Improvements in the Safety and Health Protection of Workers at Work (Arbeitsschutzgesetz, ArbSchG), available here

[16] RFC 5985: "HTTP-Enabled Location Delivery (HELD)", September 2010

[17] ETSI ES 203 178: "Functional architecture to support European requirements on emergency caller location determination and transport", April 2014

[18] ETSI ES 203 283: "Protocol specifications for Emergency Service Caller Location determination and transport", September 2017

[19] Draft-IETF-SIPCORE-LOCPARAM-00: "Location Source Parameter for the SIP Geolocation Header Field", August 2018 (expires February 2019).

[20] FICORA 33 E/2011 M: "Regulation on routing and ensuring regulatory traffic (unofficial translation)" May 2011

[21] FICORA 309/2011 S: "Routing of Emergency Traffic from Corporate Networks, September 2011