NICC ND 1432 V1.1.1 (2015-03)

NICC Document

SIP-PBX Configurations to Support Emergency Service

NICC Standards Limited

Michael Faraday House,
Six Hills Way,
Stevenage
SG1 2AY

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

NOTICE OF COPYRIGHT AND LIABILITY

© 2015 NICC Standards Limited

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be that printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

http://www.niccstandards.org.uk/publications/

If you find errors in the present document, please send your comments to:

mailto:help@niccstandards.org.uk

Copyright

All right, title and interest in this document are owned by NICC Standards Limited ("NICC") and/or the contributors to the document (unless otherwise indicated that copyright is owned or shared with a third party). Such title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no representation or warranty is given as to their accuracy, completeness or correctness. You may freely download, copy, store or distribute this document provided it is not modified in any way and it includes this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based on this document provided that you clearly indicate that it was created by yourself and that it was derived from this document and provided further that you ensure that any risk of confusion with this document is avoided.

Liability

Whilst every care has been taken in the preparation and publication of this document, neither NICC, nor any working group, committee, member, director, officer, agent, consultant or adviser of or to, or any person acting on behalf of NICC, nor any member of any such working group or committee, nor the companies, entities or organisations they represent, nor any other person contributing to the contents of this document (together the "Generators") accepts liability for any loss or damage whatsoever which may arise from the use of or reliance on the information contained in this document or from any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to download copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless each Generator in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal or other right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

The NICC Standards Web site contains the definitive information on the IPR Policy and Anti-trust Compliance Policy

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary, NICC Standards Ltd.,

Michael Faraday House,
Six Hills Way,
Stevenage
SG1 2AY

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by the NICC EmLoc Work Group.

Introduction

Emergency 999 and 112 calls are directed to an Emergency Handling Authority (EHA) for triaging which Emergency service is required. The EHA also determines, as far as is reasonably possible, the location of the caller. For calls from fixed lines the EHA determines the location from the caller's Calling Line Identity (CLI), and for this purpose holds a mapping from the CLI to location, based on information maintained by the Service provider/Communications Provider (CP). For calls from mobile originations the location is obtained from digits derived from the cell mast and appended to the 999 number.

The Emergency Handling Authority (EHA) needs the caller's location in order to direct the call to the Emergency Authority (EA) covering the geographical area of the caller. An approximate location (such as postcode) is usually sufficient to determine the EA.

The Emergency Authority itself needs to know the caller's precise location in order to dispatch someone to the site. For geographically fixed callers this location information should at least be the full postal address of the caller's location. This information is currently passed over a data path between the EHA and EA separate to the voice delivery. For mobile callers, approximate location information is currently provided by the mobile network based on cell coverage information, with further information needed to derive the precise location from the caller themselves.

The Emergency Authority should receive a phone number which can be used to return a call to the caller, or the caller's site. This number is also used by the EHA and throughout the system for record purposes.
For residential service the Calling Line Identity (CLI) is sufficient for both location and call back. For single site businesses the CLI is also sufficient.

Many modern businesses operate across multiple physical sites, with centralised PSTN breakout. This is particularly prevalent since the advent of SIP-PBXs. In such multi-site operation the usual use of CLI by the EHA to determine location breaks down, because a network provided Network Number identifies the location of the PSTN access, not the site from which the emergency call originated. It is this problem, and potential solutions to it, which this document examines.

1 Scope

The present document is concerned with emergency calls from fixed multi-site enterprises, where the challenge is to determine from which site the emergency caller is calling. Configuration options are described which maximise the possibility to derive the caller location, given currently deployed technology.

1.1 Note on terminology

This document follows the terminology used in [1]. In that document there are two variants of CLI defined: Network Number, signifying the physical point of connection or subscription to the CP's public network; and Presentation Number, used for display at the terminating phone. It is the Network Number CLI which is generally used by the EHA for determining location and emergency service call back. (In certain circumstances the Presentation Number CLI may be used; see section 5.4.)

According to [1], when using SIP signalling the Network Number is carried around the public network in the P-Asserted-Identity header field. A P-Asserted-Identity header field may be included in an INVITE request sent by a SIP-PBX to the CP, but it is the CP who is responsible for the accuracy of the Network Number, and the CP may disregard the field if received from an enterprise. Instead, the CP will provide a Network Number/P-Asserted-Identity header field from information reliably available to it. This information may include physical access, subscription, a verified From header field, or some other source.

In SIP the Presentation Number, when available, is carried in the From header field. The CP will accept a From provided by a SIP-PBX and use it as the Presentation Number if it can be verified as reliable, or if a 'Special Arrangement' has been agreed to trust the enterprise to provide a Presentation Number. The CP may also use a verified From header field as the Network Number.

In this document the term "PBX" or "SIP-PBX" is used to mean any system which generates calls from an enterprise to a CP. This includes a variety of systems not traditionally identified as PBXs, such as routers and SBCs. While this document is focussed on SIP signalling, the principles apply in an analogous way to IP-based PBXs other than SIP (for example H.323) and non-IP based PBXs (such as TDM PBXs).

2 References

2.1 Normative references

2.2 Informative references

[1] ND1016 Requirements on Communications Providers in relation to Customer Line Identification display services and other related services

[2] ND1035 SIP Network to Network Interface Signalling

3 Definitions and abbreviations

3.1 Definitions

Calling Line Identity/Identification: (From [1]) A telephone number representing the calling party. The CLI may be a Network Number or a Presentation Number.

Emergency Authority: The emergency service answering point responsible for the required regional emergency service.

Emergency Handling Authority: A centralised agency which receives emergency calls and triages them for distribution to the appropriate EA.

Emergency Location Identification Number: A CLI associated with a site location (in a multi-site deployment) which may be used on an emergency call to identify that the call originated from that site. A return call to an ELIN should return to an appropriate answering point for that site (for example the security desk) or may, through the use of specific PBX functionality, return to the phone from which the emergency call originated.

Enterprise Network Maintainer: The person or organisation configuring and maintaining the enterprise voice network. This may be the Service Provider/Communications Provider (CP), the enterprise, or a third party.

Network Number: (From [1]) The digits that comprise a unique E.164 number that unambiguously identifies the point of ingress of the call to a Public Electronic Communications Network.

Nomadic User: An end user of a fixed telephony service able to log in and make calls from many locations, thus making the caller’s CLI unsuitable for determining location.

Presentation Number: (From [1]) A number nominated or provided by a subscriber to be used for Display Services and can be used to make a return or subsequent call.

SIP-PBX: The enterprise’s point of SIP signalling interconnection with the Service Provider.

3.2 Abbreviations

CLI	Calling Line Identity
CP	Communications Provider
DDI	Direct Dial-In
EA	Emergency Authority
EHA	Emergency Handling Authority
ELIN	Emergency Location Identification Number
IP	Internet Protocol
NN	Network Number
PBX	Private Branch Exchange
PN	Presentation Number
SBC	Session Border Controller

SIP	Session Initiation Protocol
TDM	Time Division Multiplexing
VPN	Virtual Private Network

4 Multi-site enterprises and remote users

Many modern businesses operate across multiple physical sites, with centralised PSTN breakout. This is particularly prevalent since the advent of SIP-PBXs. In such multi-site operation the usual use of CLI by the EHA to determine location breaks down, because a network provided Network Number identifies the location of the PSTN breakout, not the site from which the emergency call originated.

Network Number CLI is also insufficient to determine location in other scenarios, including where the enterprise has remote end users distributed across the internet, for example home workers with phones connected to the enterprise over a private VPN over the internet.

These configurations are depicted in figures 1 and 2.

This document identifies configuration options available to the enterprise Network Maintainer to allow the Emergency Service to operate quickly and reliably in such multi-site deployments.

In some use cases it may not be possible to indicate the caller’s location to the EHA, even with optimal configuration. In such cases the configuration should be arranged such that the EHA derives the caller’s location as indeterminate, or nomadic. This indicates to the EHA operator that the location should be obtained verbally from the caller.

A similar requirement applies to situations in which the caller’s location can be reasonably assumed, but not with 100% certainty. (For instance, where a particular remote internet user usually works from home, but could be located anywhere.) In these cases the EHA should derive the caller’s location as indeterminate, but ideally also with the caller’s likely address. With this configuration the EHA operator will ask the caller for their location and, if at the address recorded on the EHA system, the call can be processed with speed and reliability.

Not all CPs provide the same options for Emergency Service configuration, and the enterprise and its Private Network Maintainer must work with CPs to determine the most appropriate option for the particular enterprise’s desired configuration and for the safety of its employees.

5 Emergency service configurations for multi-site enterprises

5.1 Background: Description of the problem

A schematic for the situation where an enterprise has multiple sites served by a centralised PSTN break-in/out is depicted in Figure 1. The location of the PSTN break-out cannot be used to determine the location of a caller to the emergency services.

Note: Some enterprises may install more than one PSTN break-out point. This is usually done to provide route/circuit resilience, and does not change the fact that the location of the PSTN break-out cannot be used to reliably determine the location of a caller to the emergency services.

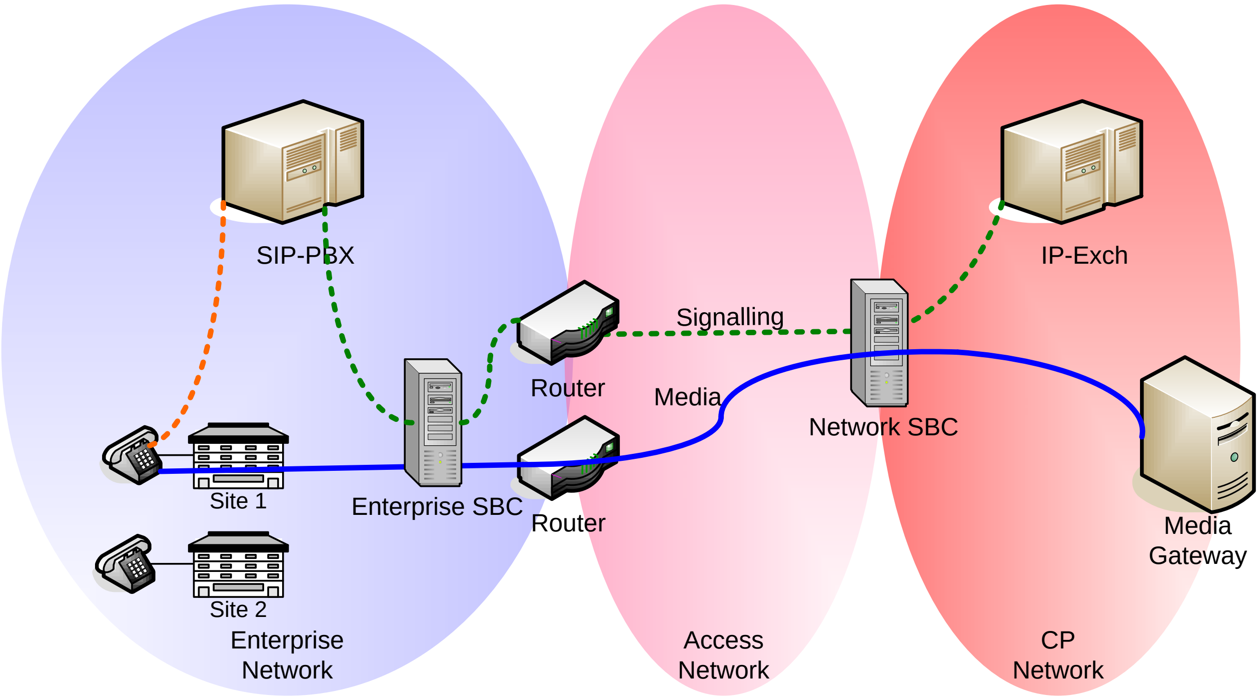

Figure 1 Example Multi-Site enterprise with centralised public network access

Notes:

- Figure 1 shows the network access signalling system being SIP. In practice any signalling protocol could be used.
- The Access Network provides IP connectivity between the enterprise and the CP network. It may be operated by the CP, or by another provider. There may be a network of routers in the Access Network.
- IP-Exch is a network IP exchange, and is the network SIP signalling entity.
- The media gateway converts the media stream, typically to the TDM domain. This is just one potential endpoint for the media stream; others include another SBC, another SIP-PBX, or a SIP client.
- Currently the EHA resides on a TDM network i.e. beyond the media gateway, and not reachable using SIP signalling all the way.

- Individual users (indicated in the diagram by a telephone) are potentially mobile or could have multiple devices at different locations.
- In a hosted/cloud SIP-PBX deployment the SIP-PBX may be located in the Access or Service Provider Network.

5.2 Solution 1: Remote site local lines

One “low tech” but functional way to provide accurate emergency service location for a multi-site configuration is to install dedicated local PSTN access from each remote site, for example using analogue lines, and route emergency calls across these local lines where they will pick up the same location determination procedures as residential lines. Typically only one local line for each site would be used.

Such local lines may also provide local survivability, so as to continue PSTN service where normal access from the site to the central SIP-PBX has been lost. If so, measures should be put in place to ensure emergency service calls take precedence over non-emergency calls; for example by reserving circuits or by pre-empting any other calls.

Where all local lines at a site are already carrying emergency calls, a new emergency call must route through the central SIP-PBX and would typically route through the main PSTN breakout; in this case the originating site information would be lost.

Adding local lines to a site is a solution which has been used to date, but it runs counter to the architecture of using of a centralised PSTN break-out. A typical deployment may see the enterprise adding analogue lines to the remote site’s VoIP configuration, and this mix of old and new technology will add cost to the overall enterprise solution as well as being a regressive solution. It also adds complexity and is not feasible in many scenarios including the case when the enterprise system is entirely centralised or hosted by a third party CP.

5.3 Solution 2: DDI as Network Number

Where individual end users have their own PSTN DDI number, this number can be signalled to the network as CLI on an outbound call. It may be possible for the CP to use this user provided number as the Network Number in PSTN signalling, and hence making it available to the EHA. Not all CPs and not all network access types will support the capability to take a user provided number, verify it, and use it as the Network Number. Coordination between the enterprise, the Enterprise Network Maintainer and the CP will be needed to ensure this is possible and to configure the arrangement.

Note that this requires the Enterprise Network Maintainer to take some actions for providing valid CLI information, and to provide CLI to location mapping to the CP for entry into the EHA’s database. Since the Enterprise Network Maintainer bears no legal responsibility for doing this, the CP should flag the CLIs in the EHA database as “unreliable”. This “unreliable” marking is a flag available within the EHA database against a CLI/address. The effect of marking a CLI location as unreliable is to cause the answering agent to ask for confirmation of the caller’s location. If verbally confirmed the stored location should allow the emergency call to progress rapidly and reliably to the required EA.

Note that this solution does not cater well for individual users who are regularly nomadic between sites.

5.4 Solution 3: DDI as Presentation Number

Where the CP does not support the copying of a user provided CLI into the Network Number field, either generically or on a particular access type or in a particular deployment, then it may still be possible to copy the CLI into the Presentation Number field. It would not be permissible, for example, to copy a user provided CLI into the NN field which the CP is unable verify; the user provided CLI might not be verifiable because it is hosted by a different CP or for some other reason.

Since the PN CLI is carried in signalling as far as the EHA, it is possible, at least in theory, for the EHA to use it to derive the caller's location. For this to work the CP must have an agreement with the EHA to use the Presentation Number, so the enterprise/Enterprise Network Maintainer must obtain confirmation from the CP before this method can be considered.

As with the Network Number mechanism, the Enterprise Network Maintainer must proactively provide the CLI to location mapping to the CP, but bears no legal responsibility for doing so. Hence the CP should mark all such CLI location mappings as "unreliable" in the EHA system.

Note that this solution does not cater well for individual users who are regularly nomadic between sites.

5.5 Solution 4: Site specific DDI number

Many SIP-PBXs support a multi-site emergency service in which the normal CLI is overwritten with a site specific CLI on emergency calls. Such site specific CLIs are sometimes referred to as Emergency Location Identification Numbers, ELINs.

The SIP-PBX may derive which site an emergency call originated from on the basis of the caller's IP address, or by other means. The caller's CLI would be replaced by the ELIN only on emergency calls. The SIP-PBX can also sometimes be configured such that a return call to the ELIN routes to an appropriate answering point at the caller's site, for example the reception, security office, or the user initiating the emergency call.

The SIP-PBX may support enhancements to this basic ELIN service, for example to allow a pool of ELINs with a linkage between the ELIN used on a particular call and the last emergency caller to use that ELIN. This allows emergency call tracking and call back to the original caller using the ELIN.

This method can be used in conjunction with the Network Number or Presentation Number means of transferring the CLI to the EHA described above. Again, since the mechanism requires the Enterprise Network Maintainer's actions to function correctly, the CP should mark ELIN's locations as ”Unreliable”.

Users who are nomadic between sites are implicitly supported with this method, making it more dependable where nomadic service is offered.

However, for this mechanism to work, accurate configuration of the SIP-PBX is necessary, and this must be maintained as new sites are added, or as the IP network is reconfigured. If changing Enterprise Network Maintainer, enterprises using this method must ensure that the configuration is reliably passed from one Network Maintainer to the other.

5.6 Solution 5: Enterprise specified NN

A SIP-PBX may include a P-Asserted-Identity header field within the SIP INVITE request to the CP network. The CP proxy server may screen this value and, if accepted as valid, use it as the Network Number on the call, and as the ELIN for location determination.

If using this option on an emergency call the SIP-PBX shall set the P-Asserted-Identity header field to an ELIN appropriate to the caller's location, and the CP screening function shall be configured to accept such ELINs as valid and use the received P-Asserted-Identity header field as the Network Number and convey this to the EHA.

As with solution 4, the Enterprise Network Maintainer must take care to accurately configure the enterprise network to ensure an appropriate P-Asserted-Identity header field is used on the call.

6 Emergency service configurations for remote internet users

6.1 Background: Description of the problem

A schematic for the situation where an enterprise has remote internet users is depicted in Figure 1. The location of the caller cannot be determined by the SIP-PBX, nor by the EHA.

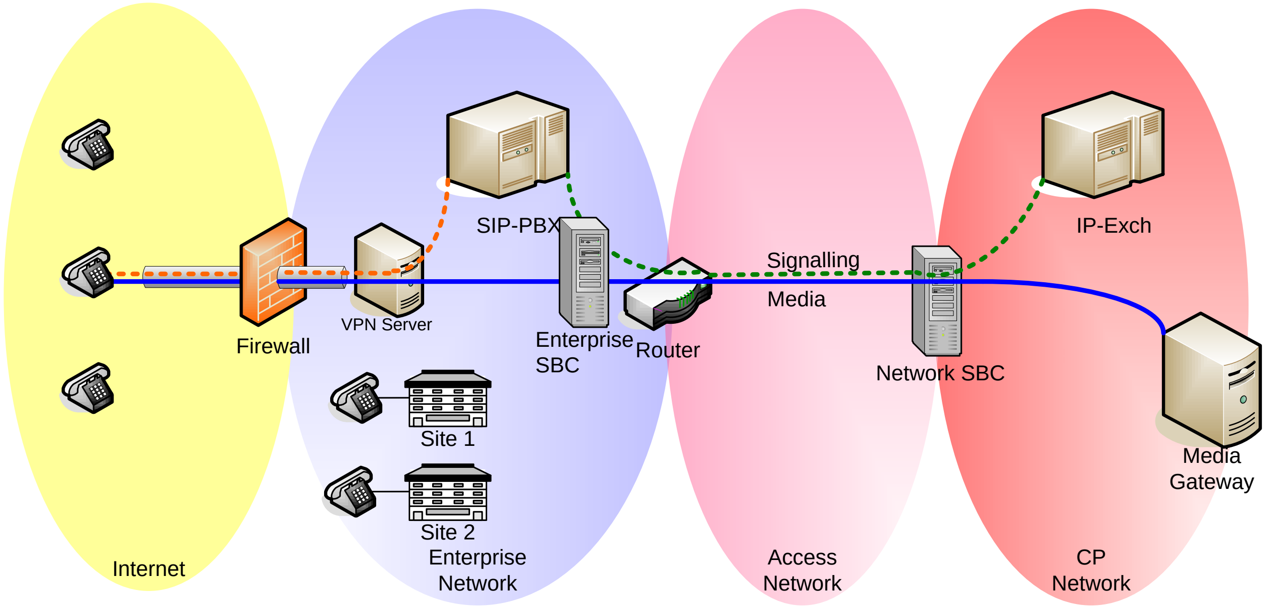

Figure 1 Enterprise with remote Internet users

Notes:

- IP addresses presented to the SIP-PBX for signalling and towards the public network for media will be addresses on the VPN server, and bear no fixed relationship to the end-user or the end-user's internet IP address.
- Users may log in from various locations over the internet, and may use various internet access means, including using mobile access.
- Individual users may sometimes connect through an enterprise site and other times through the internet access. The end-user's DDI number cannot be used to distinguish whether the user is on-net or accessing from off-net.

6.2 Remote users as nomadic

It is generally impossible for a SIP-PBX to be aware of the location of a remote user. The remote user's IP address, for example, may be one allocated from a VPN pool, and provide no information as to the user's location. The remote user's service login or DDI number may also provide no clear indication of the caller's location, as the location may vary from day to day. In such cases the user's location cannot be reliably determined.

However, as far as emergency service is concerned, a location should be provided even in circumstances where nothing can be inferred about a caller's location, in preference to providing no location at all. This allows at least a start point for investigations, should the verbal request for location also draw a blank. A suitable address might be the enterprise head office address. Such a location should be flagged with the “Unreliable” qualifier.

Consequently, for such remote users, options are to:

- Send the caller’s DDI number using one of the mechanisms previously described, marking the DDI in the EHA system as “Unreliable” with an agreed default address of the enterprise’s main site; or if it is known that the remote user normally works from a particular address (their home for example) then this address could be recorded in the EHA system.
- Send a specific ELIN for all remote users, with the ELIN location in the EHA system being “Unreliable” with an agreed default address of the enterprise’s main site.

.

7 Considerations when configuring multi-site solutions

The solutions for providing multi-site emergency call working described in sections 5.2 to 5.6 can involve complex configuration, and usually require co-ordination of data across enterprise IP network, enterprise voice service, CP Access network, and EHA. Unsurprisingly these can easily be misconfigured, and once configured can get out of alignment, potentially resulting in an incorrect location being derived on an emergency call. They also rely on information provided from the enterprise network, which lies outside the remit of Ofcom General Condition 4, and hence the information provided may not have been subjected to the same scrutiny for accuracy as CP provided information.

For this reason it is advised that all CLIs which may be used in these solutions are marked in the EHA data as requiring validation by the emergency services operator.

Further, it is recommended that test calls are made after initial configuration, and following any reconfiguration. When making test calls it may be necessary to make a call using each of the digit combinations 112, 9-112, 999 and 9-999 (where ‘9’ is assumed to be the PSTN breakout prefix), and this from a variety of sites and locations within each site. This can add up to a considerable number of test calls.

For each individual test call it would be desirable to make an emergency service call and confirm with the emergency services operator that the address seen is that of the calling location. Unfortunately, this is not practical given the number of test calls required; the emergency service operators perform an important service and should not be occupied by non-essential test calls that could delay genuine emergency calls.

Instead the Enterprise Network Maintainer should consider other alternatives:-

1. They should check whether the CP provides any facility to check the correct address results from an emergency call. For example, the CP may make available a “pseudo emergency number”, which can be configured on the SIP-PBX like 112 and 999, with all the number and CLI manipulations associated with those emergency numbers, but rather than routing to the EHA instead routes to a network service providing location information to the caller. For example, the information may be a readout of the derived postcode associated with the caller’s CLI, taken from the CP’s copy of the EHA CLI to location translation.

2. They should arrange with the CP to check their configuration processes for allocation of Network Number/Presentation Number and location data for just a small number of users and sites across the range of services provided (including remote users if needed), to be confident the process will work on extensions at all sites. The CP will agree the number of test calls to be made and follow the approved test process with the EHA.

History

Document history		
V1.1.1	March 2015	Initial publication