EENA Operations Document

Mobile Identity

Platform for the Emergency services

Title	Mobile Identity Platform for the Emergency Services		
Version	1.0		
Revision date	12/04/2018		
Status of the document	Draft	For comments	**Approved**

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Authors and contributors to this document

This document was written by members of EENA:

Authors	Country/Organisation
David Halliwell	UK, Creativity Software

Contributors	Country/Organisation
Cristina Lumbreras	EENA

Legal Disclaimer

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Table of contents

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

1 Executive Summary

Mobile Identity seeks to provide relevant information to the emergency services in a faster and more efficient way.

Mobile devices are now a primary communication channel for many citizens, and account for over 70% of all emergency calls. This device is now used to identify consumers for many services, such as banking, so this document looks to explore how it could be used to provide a caller's identity to help save lives.

If we can identify a caller – from their mobile device - then we can improve our response, especially if we can help establish any relevant information. We can achieve faster call resolution and management and therefore reduce costs and provide an enhanced response for emergencies. Callers are identified, and this is a very useful tool to fight against false calls and prevent malicious attacks.

We need a new model for mobile identity – irrespective of mobile device and network connection. Mobile identity can be achieved using the Mobile Station International Subscriber Directory Number (MSISDN) as a key that allows the emergency services to 'unlock' the information needed to help resolve calls. Identity and other relevant information could be provided when an emergency call is made to help respond to the call in a fast and efficient way.

Reliable, secure technology now exists that makes this mobile identity model achievable and worth investigation. The use of mobile is increasing, as are the challenges of identifying the users of them. Mobile identity, alongside mobile location, would provide emergency services a powerful set of tools to help them efficiently and effectively respond to callers in the future.

2 Acronyms

- AML – Advanced Mobile Location
- CAD – Computer Aided Dispatch
- GDPR - General Data Protection Regulation
- MIP – Mobile Identity Platform
- MNO - Mobile Network Operator
- MSISDN - Mobile Station International Subscriber Directory Number
- PSAP – Public-Safety Answering Point, i.e. the Emergency call center
- SIM - Subscriber Identity Module

3 Introduction

The effective and efficient handling of emergency calls saves lives. The faster a PSAP operator can log the call and direct the appropriate resources, the better chance of a quick and successful resolution of an emergency call.

In the past, calls to the emergency services were from fixed line phones. Each fixed line phone number had a corresponding name and address and all of this was public information. So, the caller rang the emergency number and the PSAP operator would be able to know the name and address of the caller - based on the phone number. Even calling from a public phone box, the operator would know the location of the caller from the phone number. Knowing this information when receiving the call meant that the PSAP operator could successfully guide the call, dispatch resources and, most importantly, save time.

With 70% of all emergency calls across Europe being made on a mobile phone there are now greater challenges in the efficient resolution of these calls. For example: determining an accurate location of the caller from a mobile phone is more difficult compared to fixed line phones. With mobile phone use set to increase in the future the emergency services need to ensure that calls received from mobile phones can be handled and resolved as effectively and efficiently as possible.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Compared to the past, emergency calls from mobile phones have a complete lack of information. In many countries, no name, no address and often just a broad cell tower location, only revealing which city they're in. This lack of information means that the PSAP operator may have to begin each call with a blank screen - asking for basic details such as name and trying to establish the issue and the location every time.

Recent experience with Advanced Mobile Location[1] (AML) on Google Android handsets has shown great success when the user isn't required to do anything, other than call the emergency services.

Identifying callers would be useful for the emergency services. When the call is received the PSAP operator would immediately see the caller's identity information – name, address. This would lead to faster call handling, data entry and quicker response times.

The goal from any mobile identity solution for the emergency services would be, as a minimum, to provide name and address details similar to the fixed line phone model. This would speed up the work required for the PSAP operator and help to resolve the call faster and confirm that the person is not a malicious caller. Any additional identifiers and information that could be provided during the call would provide additional benefits of speed and efficiency.

4 The Case for Mobile Identity

4.1 Definition of Mobile Identity

The term "Mobile Identity" is broad and has multiple meanings and applications - including for online authentication, using digital signatures and the use of a SIM card to function as an identity tool.

Mobile Identity is a complex and technical subject and is being used in many different industries, most notably in the Financial Services sector. It is used in the banking sector to identify the caller for financial transactions, using fingerprints and voice recognition from their mobile device.

For the purpose of this document the definition of Mobile Identity is using a caller's mobile device or number to identify and provide more details to the emergency services.

At a simple level if a caller's mobile device could provide the PSAP operator their name, address and date of birth this would certainly help initiate the call in a quicker and more efficient way.

4.2 Mobile Identity for the Emergency Services

If the caller can be identified, accurately, through their mobile phone then it could be used to improve the response and service the emergency services provide. This can make call resolution faster, potentially saving more lives.

Mobile Identity for the emergency services could use the caller's mobile device or number to provide useful information to the PSAP operator, such as the caller's:

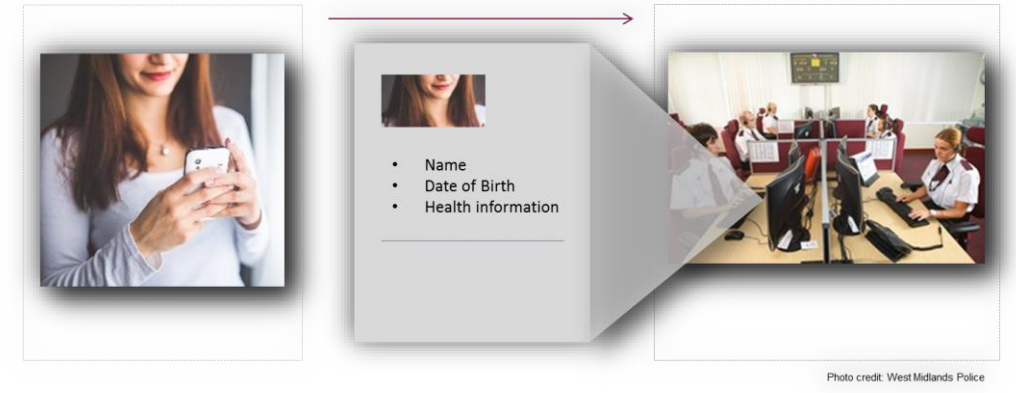
- Name
- Address
- Date of Birth – therefore age
- Gender
- Country of residence
- Main language
- Key health information - i.e. if the person has diabetes, heart condition, etc (if allowed by the data protection legislation).

[1] http://www.eena.org/pages/aml#.WXipDoiLRhE

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

4.3 Mobile Identity in Action

The following example demonstrates the potential benefit and significance of being able to identify mobile callers.



- A mobile call is made to 112 and received by the PSAP.
- The call taker immediately can see the caller's name, address, date of birth, country of origin and language
- If the caller is from a different country and requires language assistance, then the call could be automatically answered by a speaker of their language. This reduces the time on the call and increases the speed of the response from the emergency services.

4.4 Benefits to Emergency Services

Mobile Identity can benefit the emergency services by providing information about the caller immediately. This helps guide the call and establish basic information faster. Any additional information, such as health information, could be used to help establish potential causes of illnesses and help resolve the situation faster.

The benefits for emergency services from Mobile Identity would include:

- **Caller's trustability**
  Information about the caller will be available. PSAP operators could identify malicious and hoax calls enabling them to focus on genuine emergency calls.

- **Faster call handling**
  As the basic details - name, address - are received from the caller the call can be managed faster. The operator starts with contact details so can focus on the emergency and resolve the call faster.

- **Faster resource allocation**
  Make sure that the right resources are allocated to the person faster. For example a person with a known heart condition who makes a 112 emergency call may need to go to a specialist hospital. Identifying this caller and establishing this requirement quicker can help save their life.

4.5 Summary

Mobile Identity can help to provide relevant identifying information to the emergency services. This would help PSAP operators make faster decisions, reduce call times and provide a faster resolution of emergency calls.

The ability for the emergency services to receive personal information from mobile callers can help save time and lives.

5 Delivering Mobile Identity

The ability to identify mobile callers provides many benefits for emergency services and would significantly help PSAP operators with faster and efficient call resolution.

There are 3 main methods to deliver Mobile Identity for the emergency services as follows:

- Device-Based - i.e. mobile application
- Mobile Network-Based
- Centralised Platform

5.1 Device-based Method

The device-based method for Mobile Identity relies on a mobile application (app) being installed on the caller's phone. This app would hold their personal identity information.

When the person makes an emergency phone call the app could then transfer their personal information to the emergency services automatically. As the caller provides this information it would be up-to-date and accurate, with specific health-related information that they choose to share.

Mobile apps have already been used for 112/999/911 emergency services worldwide to good effect. A mobile app can provide an accurate location, personal and even medical details to the emergency services when the caller chooses to use one.

However, apps rely on people downloading and keeping them on their mobile devices to be effective. Even if you can get people to download an app, keeping it on their mobile over the long term is difficult. Although it could save your life, app storage constraints and switching to new devices often mean that apps are removed. As an emergency app is used very infrequently it probably is one of the first apps to be removed, unless you have a serious medical condition. This means that the number of people using these apps would not be significant enough to improve the emergency service response as a whole.

Also, only 78% of mobile phones in Europe are smartphones[2], so 22% of phones cannot load and use an app. This equates to millions of people and millions of emergency calls that could not use an app to share their identity.

Although apps are very useful and provide a lot of benefits, the reliance on users having a smartphone and downloading an app means their impact may be limited.

5.2 Mobile Network-Based

The mobile network-based method for Mobile Identity would provide basic information to the emergency services. It would replicate what was available from fixed line phones, so name and home address would be able to be accessed and shared with the emergency services.

When the person makes an emergency call a request is sent to the network to access their information. This returns basic contact details which can then be pushed to the PSAP centre. Much in the same way that their mobile location is shared currently with the PSAP centre, the network could also provide identity information of the caller.

This method had not been possible in the past as many mobile networks remained private. Recently the introduction of Application Programming Interfaces (APIs) has allowed greater access to the mobile networks to develop shared commercial solutions.

[2] https://www.gartner.com/newsroom/id/3323017

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

The networks do hold identity information on all its subscribers, including name, address, date of birth, as well as financial information. So, like the past telephone directories they do have data on every phone number on their network.

However, the biggest challenge with this method is the availability of APIs and the access to mobile networks is currently inconsistent. The issue of privacy and data security would also be a major concern to the mobile networks and their subscribers. Enabling external providers to access information on their customers would be a concern for mobile networks.

However, for the emergency services the mobile networks can, and have shared information - such as the mobile location of the callers - so sharing identity details would be a possibility.

5.3 Shared Platform

This method relies on a centralised, shared database of mobile phone numbers and their owners. For each mobile number there would be information on the owner's name, address and any additional details that may be of use to identify the person.

The person makes an emergency call and when the PSAP centre receives the call they request identity information from the centralised platform. Using their mobile number as a reference the platform looks up and sends back all the information it has stored on the caller.

Although this is a simple system the biggest issue would be privacy. The information stored in a single system would reveal mobile callers, their addresses and potentially sensitive health information. Ensuring that the platform is secure and that the data would only be used by the emergency services would be vitally important.

Current data protection laws do provide exclusions to share data with the emergency services. The shared platform model should be explored as a viable solution for the emergency services.

Advantages and disadvantages of Mobile Identity methods:

	Device-based	Network-based	Shared platform
Advantages	• Simple • Highly accurate information • Users in control	• Not reliant on users • Real-time access information from network • Works across all handsets	• Works across all handsets • Works across all networks • Secure information available on request
Disadvantages	• Requires an app • Relies on users to maintain app and their information • Only works on smartphones	• Gaining access to the networks • How old is the information held by the networks • Subscriber information only held for contract customers - not pay-as-you-go, in most countries	• Data security • Privacy concerns • Managing the data
Conclusion	Minimal impact to most callers	Basic information available for contract customers only (in most countries	Viable system if data privacy is not an issue

For these reasons the rest of this document will look at the viability and development of a Mobile Identity Platform (MIP), its capabilities and the potential it could deliver for the emergency services. It would be worth investigating network-based identity as a first step towards a centralised Mobile Identity Platform.

5.4 Main Issues delivering Mobile Identity Platform

The shared MIP is a viable method that works across all networks and mobile devices. However, privacy, data security and collecting the information are all issues that would need to be resolved.

5.4.1 Privacy concerns

Privacy is a major issue and is at the forefront of any discussion about mobile identity. Personal and confidential information - especially health related - has to be controlled and be secure. In fact numerous laws are in place to control the use of data, including a new EU law called the General Data Protection Regulation (GDPR)[3] coming into force in May 2018. These laws are on top of and in addition to individual country laws that define and regulate the use of personal information.

In the past, fixed line phone numbers and their corresponding name and address was available publicly. Anyone could access this information in their library or in their local phone directory. With mobile numbers this information is no longer public and is maintained and controlled by the different mobile phone networks.

Although privacy and data protection laws may be seen as a barrier to a Mobile Identity Platform, they're often exemptions for the emergency services.

For example, Germany has traditionally had the strictest laws and requirements for data protection and the use of personal information in Europe. In their federal Data Protection Act it states the data can be used by Government agencies if it helps preserve the person's vital interests'[4], i.e. helps save their life.

The act of making an emergency call indicates a level of consent from the caller. They are looking for help and therefore it could be argued, that the sharing of data is legitimate to help preserve the callers 'vital interests' and, potentially, save their life.

The sharing of personal data already happens during a 112 emergency call. Details provided to the PSAP are shared with the police or the ambulance service. The caller's' location is provided and shared amongst different emergency services. All in an effort to help them be protected and to provide the most appropriate service for their needs.

5.4.2 Data security

Any system handling and managing personal information needs to be secure and not publicly available.

It should not be able to be accessed and searched, even by public authorities. Instead the information, and the identity of the caller, should be only be revealed when they make an emergency call. The act of making an emergency call signifies permission to share information with the emergency services.

Data security of the MIP would have to be very strong to ensure public confidence and to prevent any criminal access and interference with the data.

[3] http://www.eugdpr.org/

[4] https://www.gesetze-im-internet.de/ - Section 4c - Exceptions

5.4.3 Information Collection

The principle of a shared database to provide MIP is only as good as the information that it contains. Collecting and maintaining the data would be a significant challenge that would need to be addressed.

Beginning with an empty system you have the challenge of where to start collecting information and how much to gather. The mobile networks would be the main source of information - as they hold the mobile numbers and have basic contact data.

The data, that PSAPs record, could also be a good source of information. Calls are received from mobile numbers and names, addresses and call details are recorded in the CAD system. This data could be centralised into the MIP and combined with information from the mobile networks to ensure as accurate a record as possible.

Information could also be sourced from the public themselves - who chose to provide relevant health information to the authorities, such as they have diabetes, heart conditions or smoke.

All of these issues in developing the MIP are achievable and we need to work together. Collecting and storing information requires strong, secure systems. Ensuring data security, helps with privacy concerns. The key is that the information is only available under specific conditions, when the caller makes an emergency call. If they do not make the call then the information cannot be accessed, under any circumstances.

5.5 The core requirements - Mobile Identity solution

Based on the main issues with a Mobile Identity system there are some key requirements that need to be part of any successful deployment.

The 6 main requirements would be as follows:

1. Doesn't require users to do anything on their mobile phones when making the call
2. Not reliant on specific phones or smartphones
3. Private data kept confidential
4. Personal data is only available when an emergency call is made.
5. Data available regardless of system or regional PSAP structures
6. Information must be available quickly and immediately for the PSAPs

Doesn't require users to do anything on their mobile phones when making the call
The experience with AML has shown that a system that automatically works simply when a call is made is close to fool proof. The user has nothing to remember and nothing to download and keep on their phones. They call and then their identity would be provided.

Not reliant on specific phones or smartphones
For any system to have a major impact for the emergency services it has to work on all handsets and work on both smartphones and feature phones. It also has to cover all mobile callers to the emergency services, not just calls from specific handsets or mobile networks.

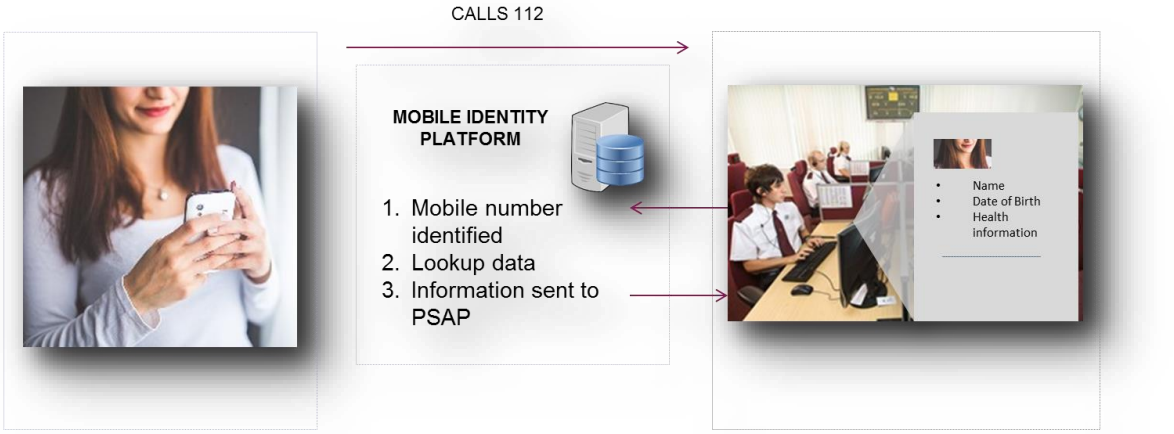
Private data kept confidential
It is critical that all private data is kept private and be compliant to all laws. The data has to remain locked and not be freely available at all times. Not even the PSAP or public authority should be able to access it unless there is an emergency and it is in the interests of preserving someone's life.

Personal data is only available when an emergency call has been made
When the caller contacts the emergency services they have indicated that they need help - to potentially preserve their vital interests and to save their life – or to be a witness to a crime. The action of making the call to the emergency services provides their permission - acts as an opt-in. Only when they make the call can the information can be shared with the emergency services.

Data available regardless of system or regional PSAP structures
The Mobile Identity data needs to be made available and be usable across different PSAP systems and structures. It needs to work across different Computer-Aided Despatch (CAD) systems and in different countries. Ideally, personal data should be made available across Europe for anyone calling 112 in an emergency.

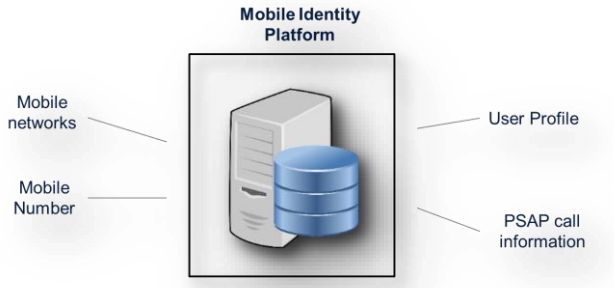
Information must be available quickly and immediately for the PSAPs
The purpose of the Mobile Identity system is to provide information to help speed up the call. Therefore it is important that the information is made available immediately to the PSAP operator, be accessible in their own systems and within seconds of receiving the call.

5.6 Mobile Identity process



In the Mobile Identity process, the caller dials 112 and makes the emergency call. The mobile number is recognised and data is retrieved and then displayed to the PSAP operator. The data available can be pushed or pulled into the CAD system so it is displayed immediately on their screen. This would pre-populate the data entry screen and might provide some direction or guidance to the operator.

5.7 Sources of data



In order to provide data and a Mobile Identity for each caller any system would have to pull from various sources of available data. The most significant sources of data include the Mobile Network Operators (MNOs), user profiles and PSAP call information.

Mobile networks
The MNO for the caller has information that can be useful for Mobile Identity solution. The network holds information about the subscriber's name, address, date of birth and device information. Device information contains information about the type of device, its behaviour - i.e. when it was last used, if call forwarding is activated or whether the SIM has been changed recently.

User Profile
For specific high-risk users, i.e. they have diabetes, or a heart condition, users could opt to provide additional information to the emergency services. Providing a user profile as a service, or connecting to digital health services, a caller's profile could provide this information directly to the PSAP operators when they call 112.

PSAP call information
The PSAPs have call data for each call made, and from which mobile number. This includes call times and dates, mobile locations received and details about the reason for the call. This information could be used to develop a profile for each caller and assign a priority or risk status. So when they make another emergency call this risk status would be visible.

5.8 Summary

A Mobile Identity system can help the emergency services by providing useful and vital information to them quickly. Enabling them to provide the right resources, faster, helping save more lives.

The Mobile Identity platform needs to be secure and work regardless of mobile device and network. It shouldn't be reliant on the caller to do anything, other than initiate a call to the emergency services. To ensure security the platform needs to be kept separate to all other systems and only be accessible to the PSAP on their network.

The act of calling the emergency services indicates consent and provides permission to access and share personal data from the caller with the PSAP.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

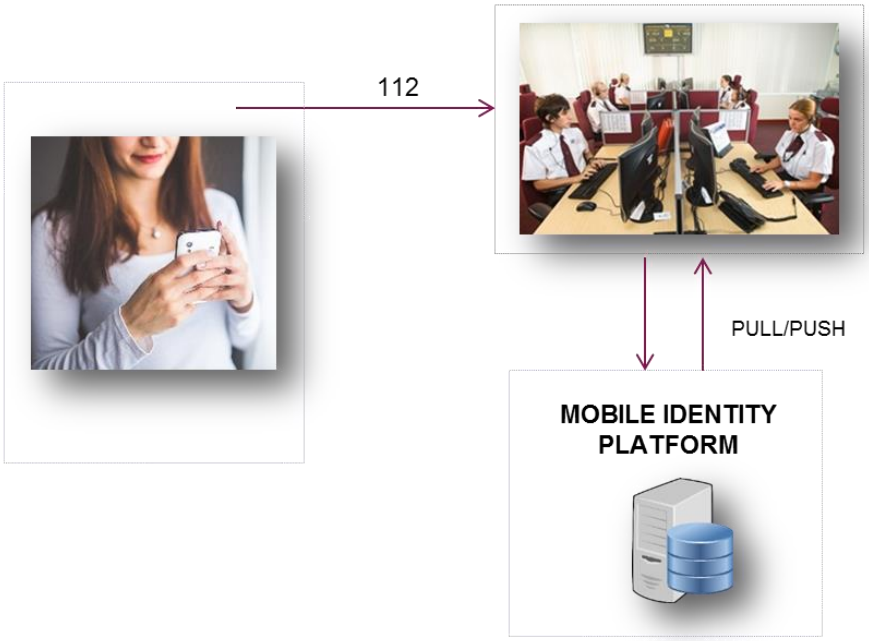
6 Mobile Identity Platform (MIP)

6.1 The MIP

As a separate system to the PSAPs infrastructure, the MIP would have to work seamlessly with all their current systems.

The MIP acts as a secure repository of information on each caller's identity. As stated it is not accessible without an emergency call being made. This ensures that the call acts as an opt in and the provision of data to the PSAP complies to all data protection laws.

The operation and process of the MIP is straight-forward as shown in the diagram below.



A call is made to the emergency services, using 112, on a mobile. As the PSAP centre receives the call a pull request is made to the MIP to provide the information held on the number.

The MIP service retrieves data and then sends this to the PSAP CAD system. Immediately the operator can see the data populate the CAD system for that mobile number.

After the call, data could be shared back to the MIP securely, either updating the contact record or enhancing the information recorded alongside the number.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

6.2 Key Features

Mobile number used as a key
The mobile number, or more correctly Mobile Station International Subscriber Directory Number (MSISDN)[5], is unique. In fact it is unique worldwide and is more unique than name, address or even date of birth. The mobile number is tied to a specific user so it's a good way to identify a unique caller.

Using the MSISDN as an identifier for the emergency services has many advantages. Firstly it does not require an app and the number is separate to the device, its type or its capabilities - whether it's a smartphone or not.

If the user has a mobile contract, or has registered with a mobile network then their personal details are recorded and held with the MNO. This connection between mobile number and a person's details means you can accurately know that this number belongs to a particular individual.

All calls are made from mobiles with numbers. In fact you cannot make a phone call without a mobile number (MSISDN). This means that all calls and therefore people, using the mobile number, can be uniquely identified.

When a caller rings 112, their phone number is identified by the PSAP. Like all calls, the phone number, most of the time, is visible to the person receiving and accepting the call. This has been the case for many years - so using this number as a unique identifier is straightforward.

Emergency call is the lock
In order to maintain privacy, the data should be kept separate to the PSAPs systems and be inaccessible unless there's an emergency call. A call to 112 will then allow the data to be passed to the PSAP. The combination of the mobile number, as the key, and the emergency call, as the lock means that you need both to access the information. One without the other is useless - only with both do you get the identity information. This provides protection for the personal data of the caller. The call to the emergency services indicates that help is required and therefore could act as an opt in to provide information to the PSAP.

Changes to mobile device detected through the mobile network
Sometimes users change their mobile numbers. Although this happens less often, because numbers can be ported from one network to another, changes in numbers means a change in the caller's identity. Fortunately, these changes are recorded in the mobile network. The MIP by communicating with the mobile network would know when a number had changed user or was inactive. This information can be used to amend the record and, more importantly, protect the user's confidential information.

Data from mobile network can be updated in real-time
The MIP can look for data from the mobile networks in real-time. It may be more realistic to periodically update the MIP - daily, monthly or quarterly as required.

Shared database
Ideally the MIP is available across Europe and not exclusive to specific regions or areas. When calls are received and logged it could be updated. Data is sent and received using standard, open communication standards. Standard protocols can be used to ensure that integration is simple and straightforward without complex integration work.

[5] https://en.wikipedia.org/wiki/MSISDN

Blockchain technology
As part of the MIP it would be worth considering Blockchain technology. Developed and used with Bitcoin, a digital currency it is one of the most secure, distributed databases that exists.

> **Definition (according to Wikipedia):**
>
> *"A blockchain is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks."*

Rather than hold all the data centrally the Blockchain would distribute records across a network of servers. This decentralisation and the encryption of the Blockchain make it one of the most secure stores of data.

The use of Blockchain technology for the MIP opens up the possibility of distributing mobile identity records across multiple, or all, PSAP centres in Europe.

With individual MIP servers, utilising Blockchain connections, in each PSAP centre - connected by a secure VPN connection - data could be updated and accessed from anywhere. Any changes of data would update across all servers in the chain before it could be made available. Only authorised Blockchain servers with valid connections would have access to the MIP database.

The concern over data security and the sensitivity of personal information makes the use of Blockchain technology an attractive one. It is already being used successfully to maintain secure financial transactions, identity and the storage of medical records.

6.3 Benefits

The deployment and use of a MIP helps provide useful caller information to the emergency services. This allows them to become more effective in their handling and management of calls. The main benefits for the MIP include:

- Users don't need to remember anything
- Minimises privacy concerns
- Easy to integrate
- Fast access and provision of data to PSAPs - works 24 hours a day, 365 days a year
- Hoax, fake callers can be identified and managed
- Language, country of origin, can be used to route the callers

Users don't need to remember anything
Using the MIP model there is no reliance on mobile device, or its specific capabilities. Instead it uses MSISDN as the key to unlock the data. This means it works across all mobile devices, users and doesn't require separate apps. The only action the caller has to do is contact the emergency services using 112, or the equivalent number in the country.

Minimises privacy concerns
Using the MSISDN as a key and unique identifier keeps the callers personal information private. The data is locked until a call to the emergency services is made. As the emergency services is an exemption to data protection laws then a call to 112 signifies permission to use personal data to help them.

Easy to integrate
The MIP would be a separate centralised system that connects through standard, open protocols. There would no additional systems and integration would be straightforward.

Fast access and provision of data to PSAPs
The MIP would work 24 hours a day, 365 days a year and provide fast access of data to PSAPs.

Hoax, fake callers can be identified and managed
The MSISDN is unique and linked to specific callers. Each and every false call can be linked to the mobile number and over-time this could build a profile for the caller. When the mobile number calls again this information could be visible to the operator to help them manage the call more efficiently.

Language, country of origin, can be used to route the callers
The MSISDN unlocks data and could provide information such as language and country of origin. This is known immediately as the call is received and could be used to route the call. Different language specialists could receive the call immediately - even answering the call in their language. This would drastically increase the speed of an effective response and save time in allocating the appropriate resources.

6.4 Summary

Mobile is now the primary method to call the emergency services across Europe. The MIP provides secure and fast access to personal, and health information to the emergency services.

The MIP helps PSAPs:

- Receive caller information immediately
- See personal and contact information
- Access health-related information
- Establish Priority - based on high risk medical conditions
- Identify potential hoax / false calls

The Mobile number, or MSISDN, acts as a unique key when combined with a call to the emergency services to 'unlock' their personal data. This data is then pushed, or pulled, to the PSAP system. This ensures that the personal data is kept private and confidential.

Data from mobile networks, PSAPs and the caller themselves can help provide important health information quickly and easily.

Most importantly, all of this can be achieved without the caller doing anything other than calling 112, or another relevant emergency services number.

7 Applications for the Emergency Services

The following are some examples how the Mobile ID Platform can be used by the emergency services to help improve their operational efficiency.

Applications for Emergency Services - Mobile Identity in action:

Mobile device identification

Data received from the network would contain device information, including model, and manufacturer. This could make the identification of the mobile device easy. Some PSAPs ask their callers to switch on their location, Wi Fi and data connection and then call them back. This is a way to try and get an accurate mobile location from the device. If a caller has them switched off, it takes longer to establish a location. By knowing this data when the call is received then the operator could advise the person as appropriate, especially if no accurate location is received from the caller.

The mobile medical bracelet

Your mobile could act as a virtual medical bracelet. Many people, with serious medical conditions, choose to wear a medical bracelet - or band - that contains details of their conditions and perhaps their medications. In the event of an emergency, the paramedic can open the bracelet and see their medical details. Therefore their medical details are private until an emergency - then their details are revealed.

In the same way, the mobile using the MSISDN can be used as a virtual medical band. The call is made from a unique number (MSISDN). As the call is to the emergency services, perhaps even to a specific emergency service, such as the Emergency Medical Service, this opens the information stored connected to this number. This could store any sort of information, name, address, date of birth and medical information.

Calls triaged

Using the information stored against the mobile number could be used to automatically triage and manage the calls. At the least the operator could see the additional information and be able to make fast and efficient decisions to improve their response times. It could be possible to automatically triage the calls based on the information known about the number. Patterns of behaviour could be sophisticatedly built up and calculated make predictions over the severity and urgency of each call. This becomes very powerful when you combine data from multiple sources, in particular the call and CAD system. A simple scoring system could be used to score each caller and then route accordingly.

The calls could be triaged based on need. As the caller rings, the information unlocked by their number is used to add a priority onto a PSAP operator's screen or even to activate a particular call script or form. If the caller has a cardiopathy then it may be appropriate to assume that this may be a leading reason why they are calling. This could be done within seconds of the call being received and the operator and the CAD system has the ability to use this information to resolve the call as quickly as possible.

For example: if a caller has had a history of abuse or has been the victim of multiple attacks and has called the emergency services 2-3 times over the last week, it would be safe to assume that this may be the reason they are calling now. Using the data in an intelligent way means that this caller could be responded to a quicker way. Knowing their home address or the address where most of the attacks take place, already when receiving the call makes checking the location and getting a police response to them much faster.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Conversely, if appropriate, calls could be reduced in priority. If a caller makes lots of bogus and false calls then it may be appropriate to change the contact response based on this information. Obviously, you will always answer all calls but you could route and handle the calls differently if you strongly believed it to be a bogus call. The management and handling of these calls could be more effectively closed and resolved then if you assume that everyone has a genuine emergency.

Faster location identification

Knowing the home location of the mobile users as they call, and / or the recent locations of their calls could be used to estimate and establish a location faster. As the call is received the PSAP may receive a location from the network (Cell ID), an AML message and with MIP would know their home location. This information could be used to select the best available location. At the times when an AML message fails the operator would know their home location.

Multiple calls and therefore multiple location results could be used to develop a pattern that could be used to estimate locations faster when receiving a call. For example: if a caller to the emergency services calls multiple times, all from their home, when they call again it could be assumed that they are at home. Although this is not always the case, knowing and using this information, can make the selection and allocation of resources quicker. This could be achieved in a few clicks by the operator, especially if the CAD system has already used the number to pre-populate the system with their basic details - including home address.

Faster language allocation

When the call is made the country of origin of the number is known. Specific information on the caller and their language may also be known. Knowing that a call received in Germany is from a Romanian is important. Using this information the call could be automatically allocated to a person who can speak that language, or access a translator online. So immediately the call is made it could be answered in the language appropriate for the caller.

Use of Call scripts

If call scripts are utilised, perhaps to ask and capture specific questions, then having the intelligence around the mobile number would be very useful and could trigger scripts to be available or to be used. If someone has a specific medical condition and they call the emergency services - then the probability is that the medical condition may be a contributing factor to their emergency. Even knowing things like medications and therefore potential side-effects may help operators and the emergency professionals to establish causes and actions to take even before they arrive on scene.

Resource allocation

If someone has a known cardiopathy and the nearest heart hospital is a helicopter ride away, it would be useful to know this before any resources get to the patient. Knowing this and establishing this may be the reason for the emergency could change the resources called upon and sent to the scene. Not knowing this, would mean that more time is spent on scene making this assessment. Using the enhanced information linked to the mobile number means a faster and more effective response by the PSAP operator, by the first responders and alerts them all about the potential resources that may be required to help. This also means that the casualty is transferred to the right hospital / next step quicker than traditional methods.

All along the emergency chain - from call, to response, to resolution - the enhanced mobile information can speed this up. The more data and information stored with MSISDN, the more value and speed that could be increased especially for the people who, unfortunately, have to call the emergency services multiple times.

7.1 Summary and next steps

The Mobile ID Platform provides the emergency services many applications that can quickly enhance and improve their current operations.

All of these applications are available to PSAPs immediately on setup and is mostly independent to their current technology and systems. The more sophisticated applications - that interact with the call handling systems - will need greater integration than just providing the callers data to the main PSAP system.

These applications and others make the MIP an attractive, effective and secure addition to the PSAP operation and one that can be implemented fairly quickly.

The concept of Mobile Identity and the practical application of this through a MIP can help provide PSAP and public safety organisations with valuable and actionable information. To ensure that the emergency services can benefit from this innovation we would suggest carrying out some proof of concept first.

8 EENA Recommendations

The previous chapters of this document contain many requirements linked with mobile handsets. The following list complements those requirements:

Stakeholders	Actions
National Government	Ensure data protection laws include exemptions for the emergency services, when needed to save lives
Emergency services	Provide feedback to EENA and relevant public safety agencies on the use of Mobile ID model to improve operational efficiency. Ask your representatives whether Mobile ID Platform can be deployed in your country
MNOs	Improve location and data access to help provide identity to emergency services and enhance 112
Handset and mobile OS manufacturers	Refer to the EENA Operations Document: "Mobile Handset Requirements - Communication to Emergency services[6]"

[6] http://www.eena.org/publications/handset-requirements#.WfiE_WhSyUk

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org