OCTOBER, 2025

CC:IPS

IMPLEMENTING NEXT GEN CALL HANDLING

Table of Contents

Purpose of this document

This document has been developed to assist Emergency Service Organisations understand the principles and primary benefits of implementing Next Generation (NG) Emergency Communications Networks (ECN) and provides some guiding questions to help Organisations assess their current state and the effort that will be required to transition to a NGECN.

What is Next Gen (NG)?

Emergency Communications Networks (ECN) are the lifeblood of public safety proving caller access to national emergency assistance through numbers such as 9-11, 112, 999, 000, and 111.

Next Generation (NG) Public Emergency Communications Networks should deliver a significant upgrade to the traditional voice-based systems, enhancing the way emergency services communicate and respond using a wide range of media. However, a true NG system should not be considered a fixed deliverable, but rather a system which exploits the latest capabilities from end-to-end whilst being capable of further evolution to take advantage of new technologies as they emerge.

An NG ECN system, using current technology, should be expected to include the following key features:

- **IP-Based Communication:** Internet Protocol (IP) networks, allowing for more efficient data transmission and integration with a wide range of communication technologies.
- **Multimedia Messaging:** Unlike traditional voice-only calls, NG ECN will enable the transmission of texts, images, videos, and other data, as well as enable emergency communications centres to receive, process, and analyse all forms of data. This will help Public Safety Answering Point (PSAP) staff gain a better understanding of emergencies and assist accessibility where voice or written messaging is not an effective means of communicating with a caller.
- **Improved Location Accuracy:** An NG ECN offers enhanced location services, using GPS and other technologies to pinpoint caller locations more accurately, which is crucial for timely responses, including in some country's location delivered in three dimensions.
- **Interoperability:** The system supports interoperability between emergency communications centres and among different emergency services, including emergency responders in the field, and jurisdictions, enabling all types of requests for emergency assistance and associated data to be seamlessly shared without the need for proprietary interfaces. This will improve coordination across borders and during large-scale incidents or disasters.
- **Data Management:** NG ECN will incorporate advanced data management tools, enabling better analysis and reporting, which can enhance emergency response strategies and support evidence gathering.
- **Enhance Caller Information:** An NG ECN could provide call handlers with additional information about the caller, subject to privacy requirements, such as medical history or specific hazards, improving response effectiveness.
- **Resilience and Reliability:** The architecture of a NG ECN should actively prioritise resilience, ensuring continued operation during emergencies, such as natural disasters.
- **Standards:** NG emergency calling systems are built to commonly accepted standards, facilitating interoperability between systems and market competition.

Overall, a coordinated NG ECN deployment will modernise emergency response systems, making them more efficient, effective, and capable of handling the complexities of today's communication landscape. They will allow the public to be more quickly located, assist PSAP staff to more quickly assess emergencies and support responders to deploy the right resources to the right location.

Key Definitions

Next Generation 9-1-1/999/112

The term 'Next Generation 9-1-1/999/112' means an Internet Protocol-based system that:

- Ensures interoperability;
- Is secure;
- Employs commonly accepted standards;
- Enables emergency communications centers to receive, process, and analyse all types of requests for emergency assistance;
- Acquires and integrates additional information useful to handling requests for emergency assistance; and
- Supports sharing information related to requests for emergency assistance among emergency communications centers and emergency response providers.

Interoperability

The term 'interoperability' means the capability of emergency communications centers to receive requests for emergency assistance and information and data related to such requests, such as location information and callback numbers from a person initiates the request, then process and share the requests for emergency assistance and information and data related to such requests with other emergency communications centers and emergency response providers without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

Commonly Accepted Standards

The term 'commonly accepted standards' means the technical standards followed by the communications industry for network, device, and Internet Protocol connectivity that:

- Enable interoperability; and
- Are developed and approved by a standards development organization that is accredited by a standards development body in a process that is open to the public, including open for participation by any person, and provides for a conflict resolution process;
- Are subject to an open comment and input process before being finalized by the standards development organization;
- Are consensus-based; and
- Are made publicly available once approved.

Requests for Emergency Assistance

The term 'requests for emergency assistance' means a communication, such as voice, text, picture, multimedia, or any other type of data that is sent to an emergency communications center for the purpose of requesting emergency assistance.

Standards

- The following represents the international Standards that constitute and affect the component parts of an NG ecosystem.
    - Advanced Mobile Location (AML) – ETSI TS 103 625. The Standard for the identification of the location of emergency calls via mobile devices and the transmission of that data to PSAP systems.
    - The Third Generation Partnership Project (3GPP) is a global collaboration between telecommunications organizations that develops and maintains technical specifications for mobile networks. It ensures that mobiles across the globe can utilise networks as they travel – any system proposed that does not utilise recognised standards will ultimately reduce effectiveness of emergency call handling and prevent emergency organisations from work effectively together. Any implementation of an NG emergency call handling capability must be based on recognised standards.
    - The NENA i3 Standard for Next-Generation 9-1-1 ("i3") refers to the NG9-1-1 system architecture defined by NENA, which standardizes the structure and design of Functional Elements making up the set of software services, databases, network elements and interfaces needed to process multi-media emergency calls and data for NG9-1-1. This is the standard for North America and has or is becoming the basis for similar specifications in Europe, Australia, and New Zealand.
    - The NENA NG-PSAP/ECC a comprehensive, good practice which serves as the technical specification for the interfaces and system functionality for Functional Elements (FEs) and Services comprising the NENA i3 Solution for the Next Generation 9-1-1 Public Safety Answering Point / Emergency Communications Center (NG9 1 1 PSAP/ECC). At a high level, NENA-STA-023 defines the system and technical capabilities the NENA i3 solution uses to receive, process, and log 9-1-1 emergency service requests. This NG9 1 1 PSAP/ECC standard utilizes many of the Internet Engineering Task Force (IETF) standards to maximize interoperability across Internet Protocol (IP)-connected systems.
    - Security is a critical component of the NG ecosystem. ISO/IEC 27001, provides a framework for organizations to manage information security risks and ensure the confidentiality, integrity, and availability of their information assets. This standard defines the requirements for an Information Security Management System (ISMS) and is widely recognized as a benchmark for information security best practices. With the advent of Artificial Intelligence (AI), ISO 42001 has been developed as an AI management system standard that provides a framework for organizations to manage their AI systems, including security. It focuses on responsible AI development and use, addressing security concerns, data protection, and transparency. Further, Jurisdictions may consider the development of their own guidelines for cyber security, referencing established guidelines such as the Cybersecurity and Infrastructure Security Agency (CISA) – 911 Cybersecurity Best Practices Package)

Gap Analysis

Using the Standards noted in the previous section, a gap analysis may be undertaken to determine:

- The current position in your jurisdiction?
    - An NG system is not just a collection of components; it is a set of components that are able to share information within and beyond your individual organisation using consistent standards not proprietary processes.
    - A base requirement will be an IP-based network, but this is only a foundation upon which additional, industry standard capabilities are layered.
- The capabilities that would benefit the public, call handlers or responders in your jurisdiction?
    - Revolution or Evolution? Timing can be important; the relationships and linkages that exist within your jurisdiction will prevail despite the systems in use. Therefore, is the infrastructure throughout the whole jurisdiction due for replacement at the same time (Revolution) or will your jurisdiction need to undertake carefully planned changes that build into an NG system (Evolution). There are benefits to both approaches – a blank sheet of paper allowing a once in a generation revolution will be challenging and potentially traumatic, but equally transformational. A longer-term programme implementing changes at the point that components reach end-of-life may be more cost-effective but will take longer to achieve potential benefits.
    - Understanding which capabilities can provide benefits to the public, call handlers and/or responders and understanding which will require revolution and which can be implemented in an evolutionary programme is essential.

Where would changes be required to implement NG ECN capabilities?

- At Core telephony/network
    - The expectations of the public are now extremely high, many quickly adopt new capabilities and as such there is huge pressure on the telecoms industry to meet those expectations. It will rarely be the case that the majority of the public will not have modern telephony to at least match that which has been rolled out in PSAP's.
    - There are however outliers; the cost of new devices means that not everyone will be in a position to use the latest capabilities, network availability may impact upon the availability of some capabilities even where the public can afford it – this may be the case, for example, where callers are in remote locations or connectivity is otherwise impacted. Therefore, fallback to basic capabilities should always remain a consideration.
- PSAPs

  - Where there is aggregation of the call handling process then economies of scale may be possible which assist in implementing technological advances more quickly and consistently.
  - For smaller PSAP's it may require careful consideration of steps required to ensure that developments are delivered which work effectively and are cost-effective.
  - It should always be considered that the PSAP is never the end of the process – the effective design of call handling systems must ensure that information and intelligence, in a variety of forms, can be 'flowed' right through to responders where it will assist in a more effective response.
  - Emerging specifications (NG-PSAP/ECC) provide a comprehensive architecture bridging call handling and CAD, providing a standards-based method to have a complete specification for all functions withing a communications center.
- Responders
  - The introduction of NG systems will allow an increasing level of information and intelligence to be shared with control rooms and responders. It is therefore important to consider whether each piece of information would assist a responder when travelling to scene or during the resolution of an incident. It is important to remember that travelling to an emergency is inherently riskier than a normal journey and that when at an incident the quantity of information can become overwhelming, as such anything passed to responders should be considered likely to be useful in successful incident resolution.
  - In the US, the Emergency Incident Data Object (EIDO) suite provides a set of standards for creating, conveying, and managing incident information in a uniform way. This allows data to be seamlessly shared across domains and agencies during an incident, including at the PSAP, dispatch, and the field—even in mutual aid events.

Business cases supporting capabilities.

- Within APCO International's Definitive Guide to NG911 there are useful sections on business cases and governance which will assist in persuading decision makers of the importance of introducing NG systems as well as the steps required to do so.
- It is also essential that the introduction of NG systems is not seen as 'part of the day job' – to be achieved effectively a robust programme, supported by the requisite resources is essential.

Cyber Security

There is more frequent, sophisticated, and intense hostile activity taking place in cyberspace. There is also global evidence that critical systems make attractive targets for hostile states and malicious cyber actors.

It is therefore essential that cyber-security is considered at the earliest stages as NG systems are developed and implemented. Designs must consider minimising the potential access points into call handling systems and ensuring that each one is appropriately protected.

Almost every jurisdiction will now have a national strategy for cyber defence, and most will offer advice and guidance on how to protect systems, it is essential that this is considered at the earliest stage.

- TODO: Standards based NG cybersecurity framework for North America (NG-SEC, PCA, i3_

Reference Links

The following represent a list of references to the Standards and other documents Jurisdictions might refer to when considering their current position and progression to a NG ecosystem.

STANDARDS

Location Identification Standard

- ETSI TS 103 625 - V1.3.1 - Emergency Communications (EMTEL); Transporting Handset Location to PSAPs for Emergency Communications - Advanced Mobile Location
-

3GPP Standard

- The 3rd Generation Partnership Project (3GPP)
-

i3 Standard

- NENA i3 Standard for Next-Generation 9-1-1
-

Security Standard

- ISO 27001 - ISO/IEC 27001:2022 - Information security management systems
- ISO 42001 - ISO/IEC 42001:2023 - AI management systems

GUIDELINES AND REFERENCE DOCUMENTS

NG Transition

- APCO Canada: NG911 Transition Roadmap for Canadian PSAPs
- APCO International: Guide to NG911
- NENA NG-PSAP/ECC Standard (pending)
- NENA Emergency Incident Data Object (EIDO) suite

- Electronic Communications Committee (ECC) Report 361

Security

- 911 Cybersecurity Best Practices Package, July 2023
- https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook
- America's Cyber Defence Agency
- The UK National Cyber Security Centre
- NENA Security for Next Generation 9-1-1 Standard (NG-SEC)

OTHER

- https://www.nena.org/page/standards
- Standardisation work - EENA
- Standards - APCO International