Digital Social Alarm Protocol Guidance

Application Guidance

TS 50134 Part 9: IP Communications Protocol

Developed by TSA Special Interest Group 10

Contents

1. Introduction

As Communications Providers continue to migrate towards All IP networks, they are increasingly converging voice traffic onto their IP infrastructures which may have an adverse impact on the reliability of in-call, analogue tone based protocols.

The impact differs per region but is increasing across the UK. In addition, cellular technology is increasingly used next to broadband and optical fibre solutions.

This guidance is designed to be used in conjunction with the Technical Specification 50134-9 which defines the IP communications protocol for social alarms, optimised for communication between stand-alone hybrid or digital alarms and Alarm Receiving Centres.

This Technical Specification can be purchased from the BSi on the following link: https://shop.bsigroup.com/products/alarm-systems-social-alarm-systems-ip-communications-protocol

This guidance has been produced by TSA Special Interest Group 10 (Digital Interoperability) and is designed to accompany the UK implementation standards of Technical Specification 50134-9 which was approved by CENELEC (European Committee for Electrotechnical Standardisation) on 28th May 2018. Further information regarding TSA Special Interest Group 10 can be found on the following link: https://www.tsa-voice.org.uk/campaigns/special-interest-gro/interoperability-integration-/

Neither this guidance nor the Technical Specification include all the necessary provisions of a contract and compliance with both the Technical Specification and this accompanying guidance cannot confer immunity from legal obligations.

2. Overview

A social alarm is a device that provides two stages of communication when the alarm is triggered:

1. An initial message exchange between the device and the ARC to provide details such as the type of alarm activated, the location of the alarm and the status of the alarm itself. Historically this message was made up of a series of audible tones, this specification ensures that the message exchange is completely digital over an IP network (either fixed line or SIM)
2. The second stage of the alarm consists of the voice call between the device and the ARC which follows successful receiving and understanding of the initial message exchange. The voice call could be a VoIP call over a fixed line or SIM or indeed it could be a standard mobile call.

This guidance is primarily aimed at ensuring that the digital social alarm emergency call is set up in a consistent manner to allow for interoperability between devices and ARCs of different manufacturers.

The focus is specifically placed upon key elements of the Technical Specification where there is room for interpretation and therefore, by providing guidance in those areas, will lead to a more consistent application of the specification.

The guidance is primarily intended for use of social alarm devices providing life-critical solutions to alarm users, however, it is recognised that non-social alarm providers will use elements of the TS50134-9 standard to connect their devices (e.g. IoT devices / smart speakers / Wi-Fi only devices etc.…) to Alarm Receiving Centres and cloud platforms where agreed.

3. Key Guidance

The following application guidance has been provided to assist organisations to follow industry best practice in terms of the configuration of digital social alarm solutions using the common digital protocol TS50134-9.

3.1 Protection of voice/data during transmission

The specification states that personal or sensitive information must not be transmitted over an unsecure connection without encryption. Although each organisation with procurement responsibility for the digital social alarm solution should determine whether the information being transmitted is personal or sensitive (as part of a Data Protection Impact Assessment), it is strongly recommended that, as a minimum, one of the following approaches is taken:

3.1.1 End-to-end encryption of voice/data

According to the standard, the minimum level of encryption of voice/data is as follows for transmission on open or private networks:

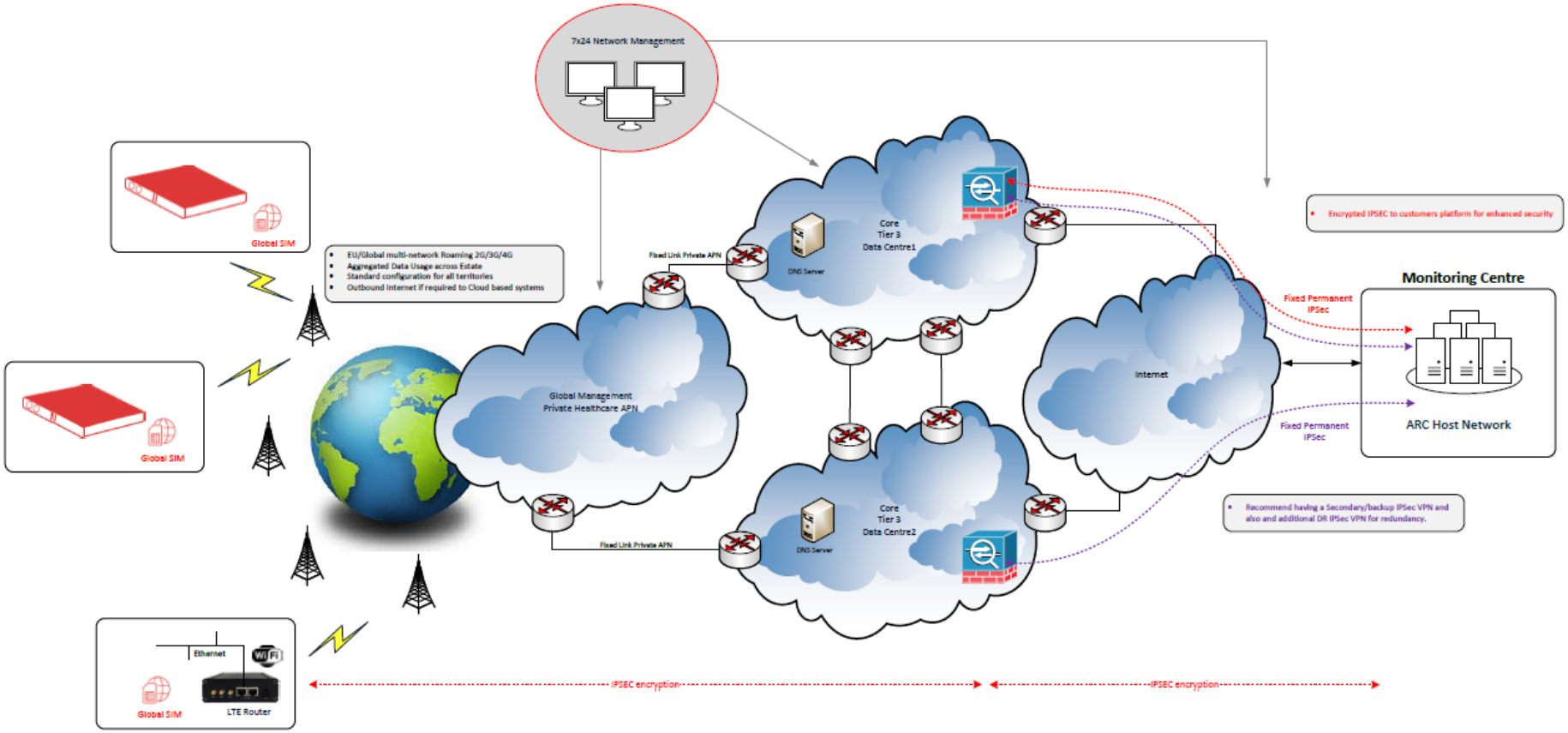
- Transport Layer Security (TLS) transmission – v1.2 or higher
- International Telecommunication Union (ITU) X509 certification
- Local Root Certificate Authority (CA) Certificate verification
- Cryptographic algorithms AES-128
- Secure Real-time Transport Protocol (SRTP) for voice transmission

3.1.2 Virtual Private Networks

An alternative to end-to-end encryption is to use an end-to-end Virtual Private Network which protects the voice/data in a private ‘tunnel’ to prevent illegal access to either media type. For this to be an effective method of protection, the following must apply:

- The VPN (or a combination of VPN and TLS) must run completely end to end from the device to the ARC without any media being left unprotected at any stage of the transmission
- In the interests of open interoperability, ARCs should be able to provide multiple VPN supplier options for devices and other connectivity
- Where cellular transmission is employed, the VPN must use private Access Point Names (APN) to provide a secure point of entry
- Private IP addresses must be employed to provide non-routable locations for the media to be transmitted to and from.
- A second VPN should be set-up to account for situations when the solution is set to Disaster Recovery mode

High Level Generic VPN Network Diagram



3.2 Network Address Translation (NAT) traversal

To ensure accurate signaling towards social alarms behind NATs, the following key settings must be in place between social alarm and ARC:

- TLS connection re-use must be supported per SIP outbound extension defined in RFC 5626
- The social alarm must send Carriage Return and Line Feed (CRLF) keep-alive messages per section 3.5.1 in RFC 5626.
- Social alarms must support symmetric Real-time Transport Protocol (RTP) as per RFC 4961 to enable NAT traversal of media.
- Social alarms must support Session Traversal Utilities for NAT (STUN) in line with RFC 5389 to enable NAT traversal of media.

In addition, some key recommendations that should be aligned between social alarm and ARC as part of the deployment:

- New TLS connections may originate from SIP register requests to ensure there is a communication path for inbound voice related SIP Invite requests.
    - If the deployment doesn't require support for inbound voice calls, connections may be established with originating SIP invite requests.
        - In this case the connection must be established until end of the call to ensure subsequent SIP requests in the dialog can pass through.
- If the communication starts with a SCAIP SIP message request, the established TLS connection must be kept open until incoming SCAIP messages have been received.
    - If these indicate that a SIP call will be placed or received the same connection must remain open for subsequent SIP Invite requests.

3.3 Resilient Service Discovery

Resilient Service Discovery should be used by the social alarm to discover and route voice/data traffic to the servers provided by the ARC. To ensure a highly reliable service the ARC should consist of multiple servers with traffic distributed across those servers to ensure a high level of availability. As traffic increases over time, more servers should be added and made available for the social alarms.

To maximise the resilience of the service, the ARC should support SIP Server Discovery (as specified in RFC 3264, locating SIP servers.) and the social alarm should support the use of Domain Name System (DNS) Name Authority Pointer (NAPTR) and Service (SRV) records to locate the servers and the relevant port for VoIP transmission.

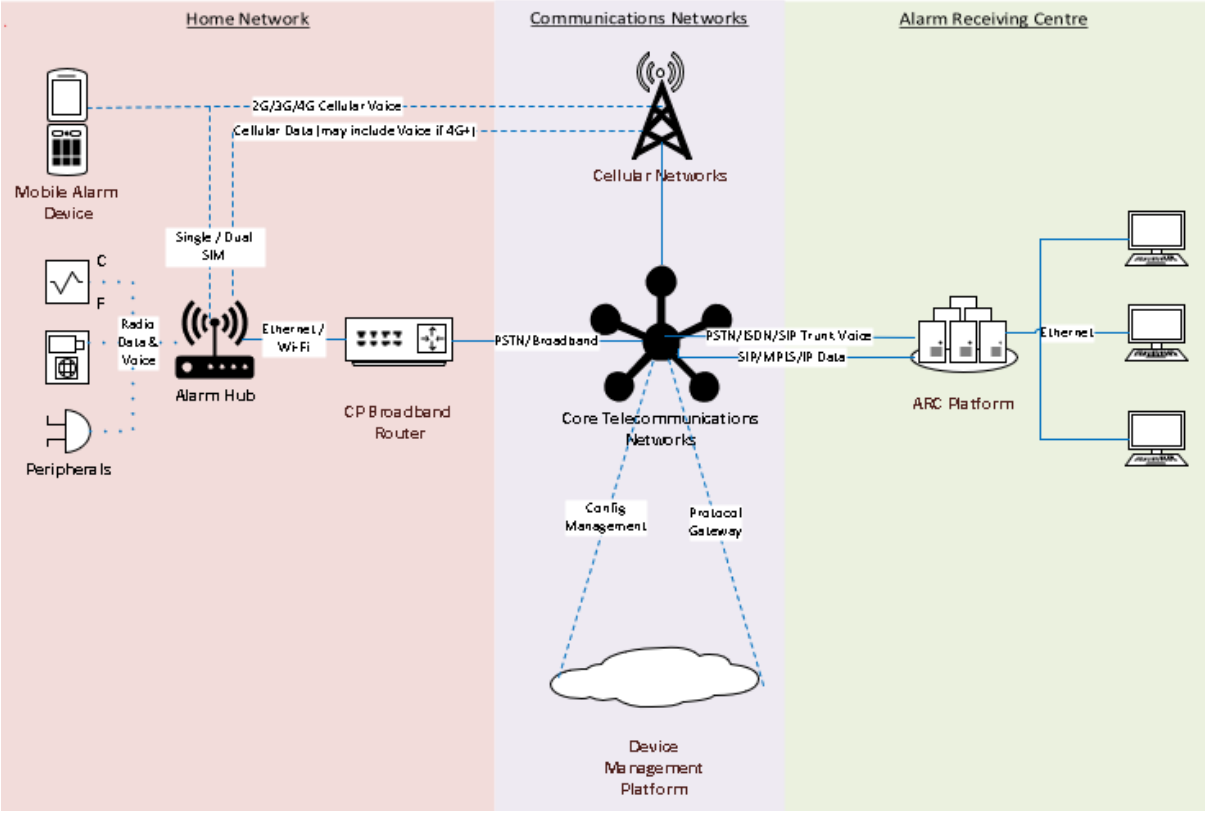
The social alarms should also honour the DNS Time To Live (TTL) value to ensure that the DNS cache is updated continuously since the topology of the service, as well as other cloud-based response centre solutions, change from time to time.

The resolved DNS SRV records will return multiple hosts for the service and it is therefore important that the social alarm follows the procedures in RFC 3264 to distribute the traffic across the hosts. In the event of a failed connection the social alarm should attempt to establish a connection with another of the hosts received from the DNS.

3.4 Speech Profile

The TS50134-9 specification is clear in that it allows for the voice and data elements of the alarm call to be conducted through a variety of transmission methods.

The diagram below gives an indication of the combination of transmission paths and types that are currently in operation in the UK. It is important to note that, for many of the possible transmission paths, the voice element of the alarm call can be initiated by the device or by the ARC which can have an impact on the cost profile for the solution.



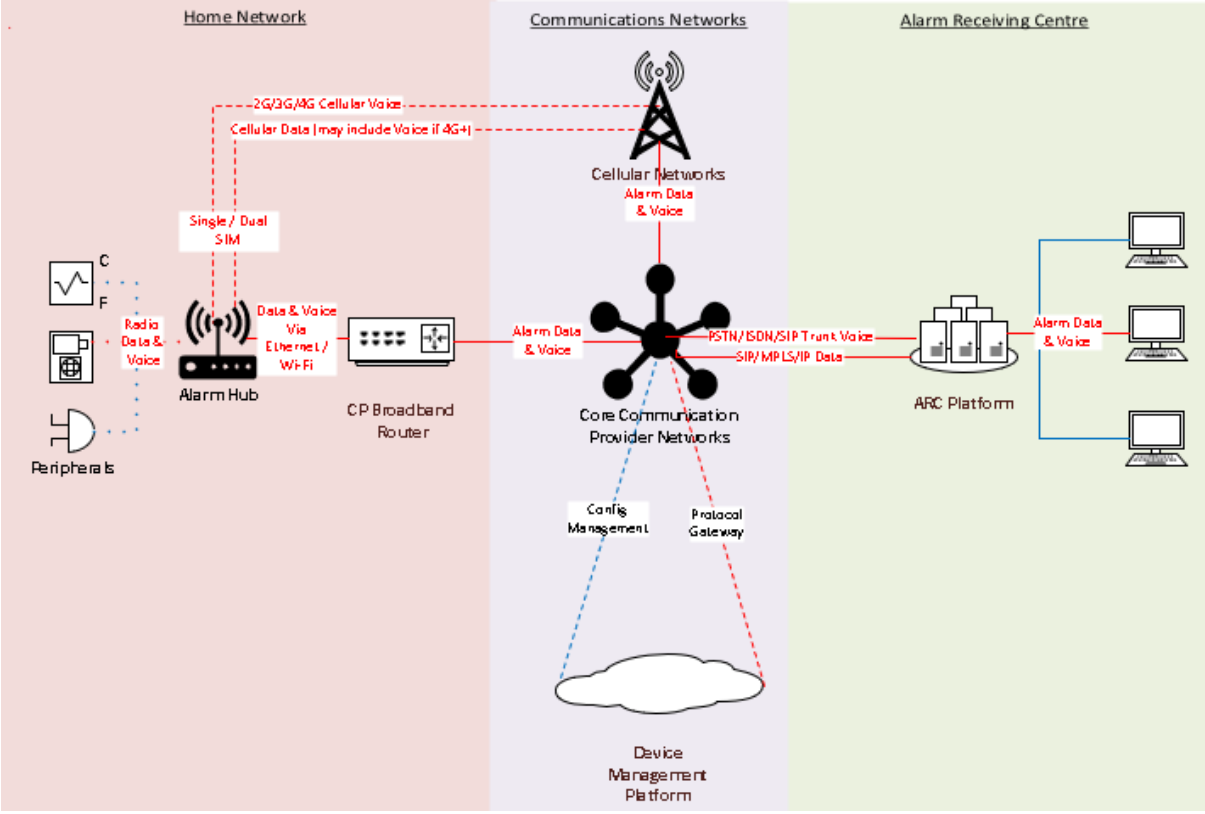
ARCs should provide connectivity for all methods of communication and social alarm suppliers should be clear about which methods of voice communication that they support to enable the procuring organisation to make a decision that fits their strategy.

3.4.1 Alarm Voice & Data connected via SIM and Ethernet/Wi-Fi

The transmission path highlighted in red below shows a combination of transmission paths using either single or dual SIM card from the Alarm Hub or Ethernet/Wi-Fi connection via the alarm user's home broadband router.

The solution can be configured to select either SIM(s) or Ethernet/Wi-Fi as the primary method of transmission with the other method as the backup in case of primary failure.

The Hub and SIM card(s) can be set up to transmit the data and voice as Voice over Internet Protocol (VoIP)packets or the data can be transmitted via the SIM card(s) as IP packets whilst the voice can be transmitted over the same SIM card(s) as standard 2G/4G voice calls. If the transmission path is via the broadband router then the alarm data and voice information will be transmitted as VoIP over fixed IP telecommunications networks.

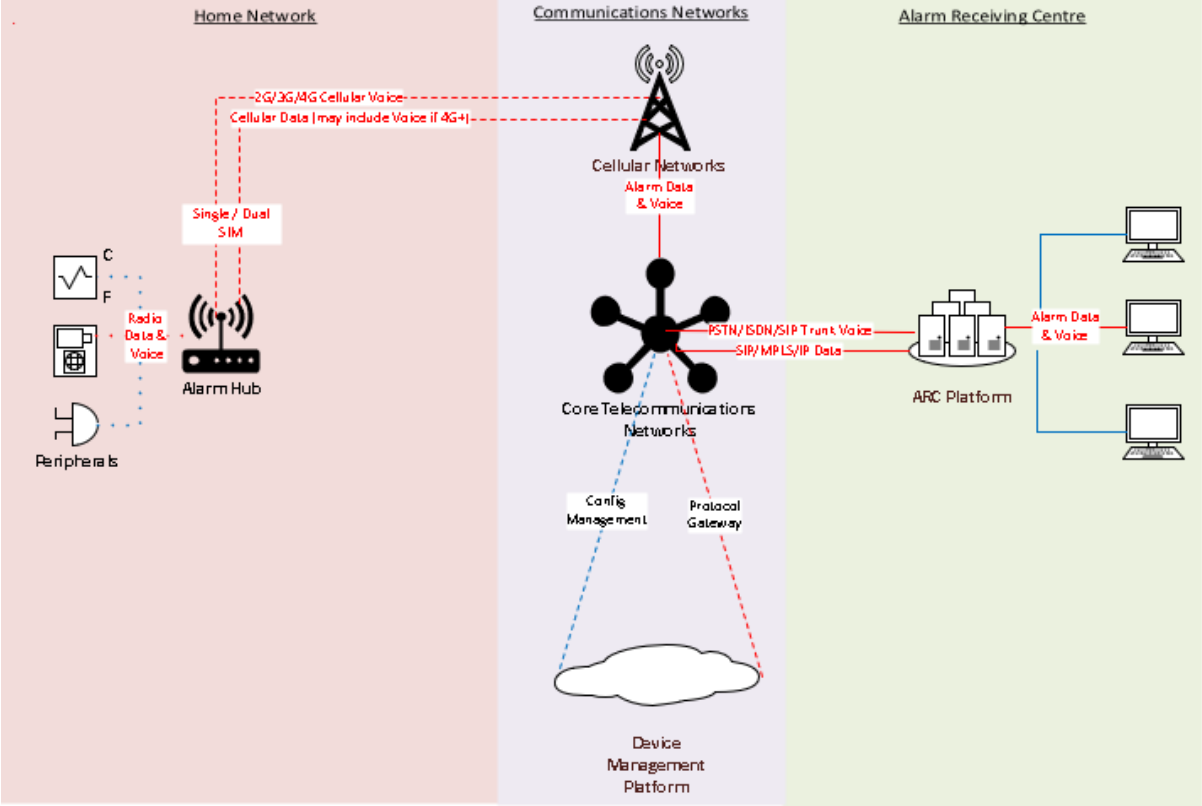


3.4.2 Alarm Voice & Data connected via SIM only

The transmission path highlighted in red below shows the route from a triggered peripheral in the home, via the alarm hub in the home which contains either single or dual SIM cards which

transmits both the voice and data via both cellular and core telephony networks to the Alarm Receiving Centre.

As above, the SIM card(s) can send the voice and data as VoIP packets, or the data can be sent in the form of IP packets whilst the voice connection can be made as a standard 2G/4G cellular call.



It should be noted that when the solution is reliant on a single SIM card with a single communication method to the ARC, the risk of solution failure is higher than when there is either a combined SIM/Broadband option, a multi-SIM option or a single SIM/multi-IMSI option

3.4.3 Alarm Voice & Data connected via Ethernet or Wi-Fi only

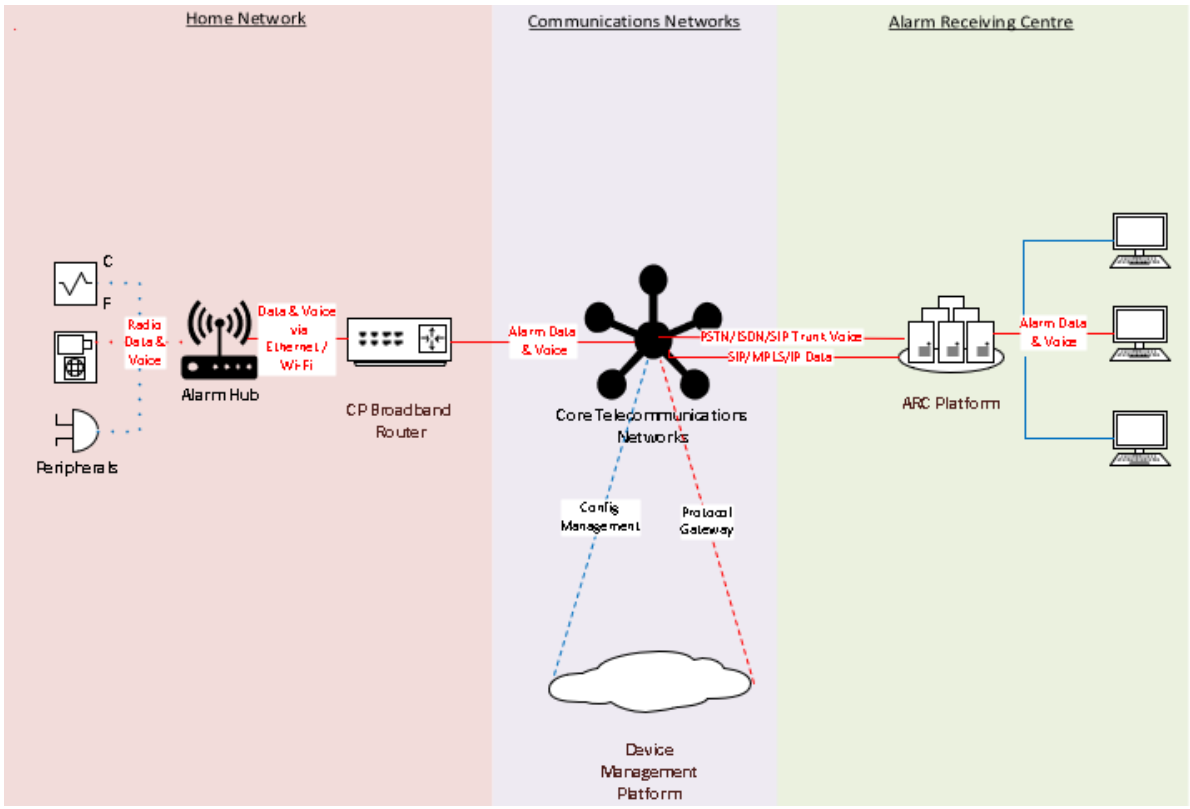
The transmission path shown below is the configuration for an Ethernet/Wi-Fi connection via an alarm user's broadband router without any SIM cards involved. The alarm data and voice are transmitted using VoIP packets over the core telecommunications networks operated via Openreach, Virgin, KCom etc…

With regards to the use of Wi-Fi instead of or as well as ethernet, EN 50134-5 references EN 50136-1 and states either Wi-Fi or an ethernet connection between the local unit and the router would be acceptable, so long as performance criteria, tested by the relevant solution installer, are met.

For this configuration, it is important to note that although the social alarm will meet UK standards for appropriate battery backup (24 hours minimum), there are several points along the transmission path which have either no battery backup as standard or less than 24 hours:

- The CP broadband router does not have any battery backup provided as standard and therefore the overall solution will fail to connect to the ARC during any mains power outage.
- Some CP's (e.g. BT / Talk Talk) have committed to providing battery backup to a cohort of users that they agree are vulnerable but those batteries will provide a maximum of 1 hour of backup in the event of mains power outage
- Street Cabinets that provide non-FTTP services are fitted with 4-hour battery backup units (for outages lasting longer than 4 hours, engineers are normally able to swap out batteries from other street cabinets that are still under mains power)
- Openreach Exchanges each have a diesel generator that can provide 7 days of power to an exchange in the event of a power outage

EN 50134-3 references the need for the alarm unit to monitor the availability of the alarm transmission path (including the components of that path) and generate local indicators when the transmission path is unavailable but there is no suggestion that the alarm unit becomes non-compliant to social alarm standards if the CP router does not have a battery backup.



It should be noted that, whilst connecting a digital alarm to a single broadband router only connection is preferable to connecting an analogue alarm to a broadband router, there are risks to this type of solution as it relies entirely on the service user's internet connectivity set-up and power to operate successfully.

In addition, there is an added risk that battery backup is not provided as standard to broadband routers so a mains power failure will cause the solution to fail

3.5 Heartbeats & Periodic Test Calls

The specification requires clarity with regards to the definition of Heartbeats and Periodic Calls so this application guidance intends to provide a definition of both Heartbeats and periodic calls as well as configuration guidance

3.5.1 Device Polling from Device to DMP

A device poll is regular communication between the social alarm and the Device Management Platform (DMP) which is a web-based portal that allows organisations to view the status of their social alarms in close to real time and configure those devices remotely via Over The Air (OTA) updates. DMPs will receive information every few seconds or minutes from the digital social alarms and alerts will be generated by those DMPs if, for example, there is a change of status of one or more social alarm or if one of the social alarms has not provided a 'poll' for several minutes.

EN 50134-5 contains several clauses which relate specifically to transmission path alerting and the following are set out in EN 50136-1:

- It is the primary responsibility of the system provider to ensure standards are met
- In the absence of a managed service, it is the responsibility of the service provider to meet those standards
- The set out the availability target, the transmission target and the verification interval target for the alarm transmission path

In conjunction with the standards referenced above, heartbeats are not governed by the TS50134-9 standard, a recommendation from the Special Interest Group responsible for development of this guidance is that an alert should be raised to the Service Provider if no heartbeats are received within a time period agreed between the manufacturer and the Service Provider. The alert to the Service Provider should take the form of an acknowledged notification method agreed with the Service Provider to take appropriate further action to investigate why the connection to the social alarm has been lost, whilst ensuring that those alerts are not prioritised over life-critical calls.

3.5.2 Heartbeat between Device and ARC

Whilst the heartbeat provides reassurance of the link between the social alarm and the DMP, the periodic call proves the link between the social alarm and the ARC. It is important that there is a distinction drawn between the two as whilst the heartbeat can indicate that the device has power, for example, it cannot alert that the connection to the ARC has been lost without a periodic test call taking place.

In the analogue social alarm world, a periodic call would be scheduled to take place every 28 days to provide reassurance that the alarm was still operational. In the digital world, this reassurance can be provided on a more regular basis (albeit with just the data aspect of the call) and is provided using specific status codes in the Message Request/Message Response fields. These periodic test calls can be set to occur in intervals lasting between 1 minute and 1,440 minutes (1 day). It is recommended that, to maintain the successful operation of the ARC platform that each social alarm is set to provide a periodic (data-only) test call every 1,440 minutes and those calls should be set at different times for each alarm to prevent any testing overload and, additionally, to avoid peak call times. ARC Platforms should set these periodic alarm calls to auto-answer.

Where the device has two communication paths (e.g. dual SIM / SIM & Ethernet/WiFi), the minimum expectation is that the primary communication path from the device is tested on a daily basis, it is recommended, where possible from a technical and resource perspective, that both primary and secondary communication paths from the device should be tested.

As the periodic test calls form part of the critical call flow, it is the responsibility of the Service Provider to ensure that they have the right process in place for missed periodic calls to be flagged for further action. As all periodic test calls are received by the ARC platform rather than the DMP, it is expected that the ARC platform will be able to schedule a daily report as a minimum to highlight any social alarms that have not connected a successful test call to the ARC within a 24-hour period.

As the periodic call does not establish a voice connection, there remains the need for the Service Provider to test the voice connection monthly with the alarm user to ensure that the voice channel is operational.

3.6 Field Codes

The use of specific codes is central to the consistent application of the TS50134-9 protocol. A message request will provide information to the ARC such as the Device ID that is making the alarm call, the Device Type (DTY) code, for example, <dty>0012 for Bed Monitor or <dty>0033 for Flood Detector, as well as a Status Code (STY) to give further detail on the alarm raised such as <stc>0016 for battery low or <stc>0085 to advise of a mains power failure. These codes, sent in combination as part of the message request from the social alarm, provide the ARC with the required information in advance of the voice call being connected to the individual alarm user.

The specification provides a table of codes (embedded in the table below) and it is important that Supply Partners apply these codes consistently to allow consistency of alarm application and reporting regardless of the ARC platform or device that is connected – this is the essence of assuring interoperability.

Download the TS50134-9 Code Tables here

Any Supply Partner that is using or wishes to use any code number not specifically identified in the TS50134-9 tables should notify SIG10 to ensure that the code is consistently applied across all devices and ARCs.

As part of the implementation process, Service and Solution Providers should work together to ensure that different alerts are tested through to the ARC platform correctly, ensuring settings are as expected for voice and no-voice alerts.

4 Glossary of Terms

Term	TEC Explanation
APN	Access Point Name The gateway between a cellular network and the Internet used in digital alarm devices
ARC	Alarm Receiving Centre Receives alarm calls from alarm devices and handle those alerts appropriately
CP	Communication Provider For example: BT, Virgin, Sky, Talk Talk etc..
CRLF	Carriage Return Line Feed Two characters that indicate the end-of-line (end-of-paragraph) in Windows
AES-128	Advanced Encryption Standard 128 bit A 128-bit key used to encrypt and decrypt TS50134-9 messages
DMP	Device Management Platform Primarily used to configure and monitor digital alarms
DNS	Domain Name System A naming convention for turning domain names into IP addresses
DTY	Device Type A code that identifies the type of alarm alerting via TS50134-9 protocol
EN 50134-3	This European Standard applies to alarms and ARCs and governs the transmission of alarm calls and data
EN 50134-5	This European Standard specifies the minimum requirements for the performance, reliability, and security for transmission of alarm calls and data with regards to interconnections
EN 50136-1	This European Standard specifies the general requirements for alarm transmission systems
Ethernet	Connectivity using a digital cable between two digital devices (e.g. alarm and broadband router)
FTTP	Fibre To The Premises The internet / telephony route between the home/business and the local telephone exchange being routed entirely over optical fibre
Heartbeat	The signal sent by the digital alarm device to the Device Management Platform which provides a confirmation that the alarm device is still operational
ITU X509	International Telecommunication Union (ITU) X509 certificate

	The standard defining the format of public key certificates used as part of the encryption of alarm communications within the TS50134-9 protocol
Multi-SIM	Multiple Subscriber Identity Module cards A digital cellular alarm with two or more SIM cards within the alarm device
Multi-IMSI	Multiple International Mobile Subscriber Identities When a SIM card holds multiple IMSIs, it enables the alarm device to switch between mobile operators as necessary (e.g. during a carrier outage) and offers more reliability than a standard Roaming SIM
NAPTR	Name Authority Pointer NAPTR records are most commonly used for applications in Internet telephony, for example, in the mapping of servers and user addresses in the TS50134-9 alarm messaging
NAT	Network Address Translation A method of mapping multiple local private IP addresses to a public IP address before transferring alarm information to enhance the security of the solution
OTA	Over to Air The method used to provide remote updates to digital alarm devices (rather than on-site engineer updates)
Periodic Calls	The message sent by the digital device to the Alarm Receiving Centre which provides a confirmation that the device is still operational and contactable (generally set at one automated call per day, answered automatically)
RFC	Request For Comments Documentation from the Internet Engineering Task Force (IETF) that contains specifications about internet and computer networking used as the basis for alarm communication
Roaming SIM	Roaming Subscriber Identity Module cards Cellular network cards in digital alarms that can access multiple local cellular networks to enhance local connectivity for devices, albeit tied to a single overall mobile operator network
RTP	Real-time Transport Protocol A network language for transmitting alarm audio and/or video over IP networks.
SRTP	Secure Real-time Transport Protocol An encrypted network language for transmitting alarm audio and/or video over IP networks.
SCAIP	Social Care Alarm Internet Protocol

	The initial interoperable digital protocol developed by the Swedish Standards Institute to enable devices and ARCs from different manufacturers to communicate consistently
SIM	Subscriber Identity Module cards Cellular network card providing alarms with access to the mobile network(s)
SIP	Session Initiation Protocol A signaling language that enables the Voice Over Internet Protocol (VoIP) communication between alarm and ARC
SRV	Service record The specification of data in the Domain Name System (DNS) which defines the location (the hostname and port number) of specific servers for alarm communications
STY	Status Code Code contained within the TS50134-9 field code tables that identifies the status of the alarm device
TLS	Transport Layer Security A form of encryption to protect data in transit from being compromised by a 3rd party
TS50134-9	Technical Standard 50134 Part 9 Interoperable alarm protocol providing consistency of connection type between dispersed alarms and Alarm Platforms from different manufacturers
SIG10	TSA Special Interest Group 10 Group of industry stakeholders providing input, feedback and input to this document
TTL	Time To Live The amount of “hops” that am IP packet is set to exist inside a network before being discarded.
VoIP	Voice over Internet Protocol The description used when voice calls are transmitted entirely over the internet
VoLTE	Voice over Long-Term Evolution A technology specification that defines the standards and procedures for delivering voice communication and data over 4G LTE networks, a future development which will allow structured VoIP over cellular networks
VPN	Virtual Private Network Defines a private ‘tunnel’ to protect data in transit from being compromised by a 3rd party

Alarm systems - Social alarm systems - Application Guidance