Social Alarm systems: IP Signalling Protocols

BS8521-2:2020: Part 2: Specification for NOW-IP

Application Guidance

Developed by TSA Special Interest Group 10

Version: 1.0

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 second part of BS8521 which provided requirements for specialised group living environments.

This British Standard can be purchased from the BSi on the following link: https://knowledge.bsigroup.com/products/social-alarm-systems-ip-signalling-protocols-specification-for-now-ip/standard

This guidance has been produced by TSA Special Interest Group 10 (Digital Interoperability) and 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-/ The BS standard mandates that the communication conforms with the following protocols:

- RFC 3261 [N1] Session Initiation Protocol
- RFC 3428 [N2] for alarm transport
- RFC 3550 [N3] for media stream

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 grouped social alarms and ARC platforms of different manufacturers.

The focus is specifically placed upon key elements of the British Standard where there is room for interpretation and therefore, by providing guidance in those areas, will lead to a more consistent application of the specification. Where there are identified issues in the BS8521-2 standard, specifically:

- the standard for calls made from the Alarm Receiving Centre to the Scheme, and,
- clarification on the use of the word ‘local’ in respect of the Root Certification for encryption,

requests for clarification have been submitted to the relevant BSi committee (GW/001/012) and this guidance will be updated once the standard has been updated.

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

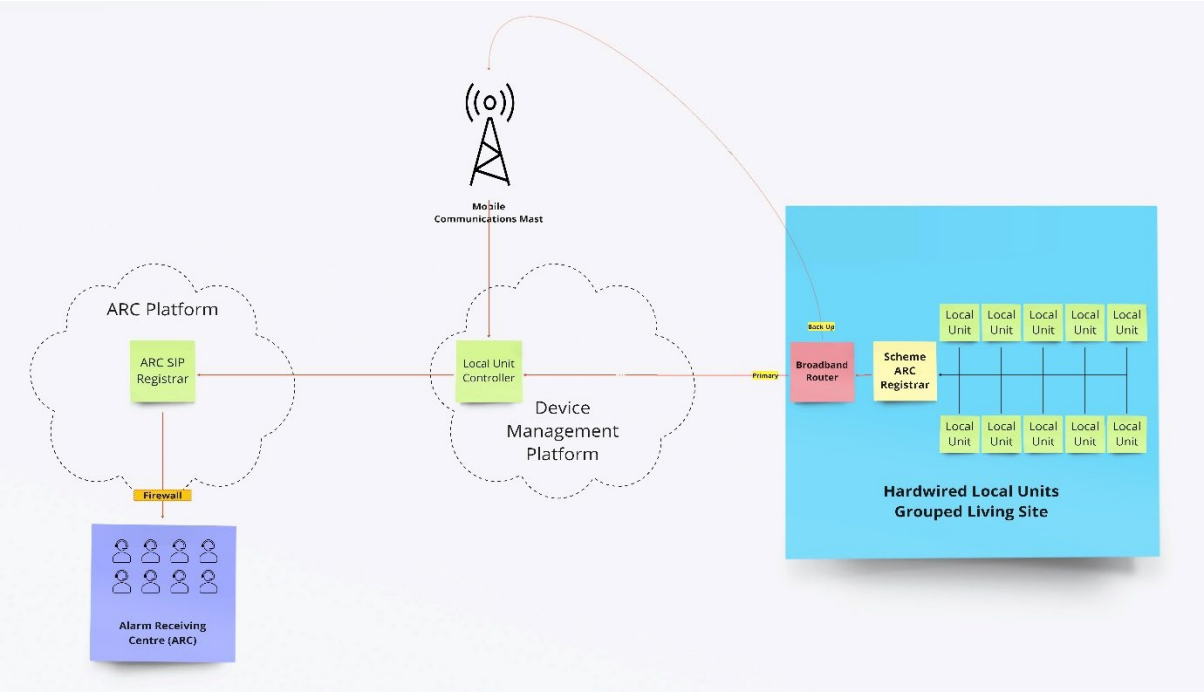
2. Overview

A grouped living digital social alarm can be implemented 2 different ways:

1. A fully end-to-end digital scheme solution that utilises wired or wireless interlinked scheme equipment within the scheme building, that is linked by a common transmission path to an Alarm Receiving Centre
2. A fully end-to-end digital dispersed solution within a scheme building where the dispersed units communicate with an Alarm Receiving Centre (either directly or via a Device Management Platform)

2.1. Fully End-to-End Digital Scheme Solution

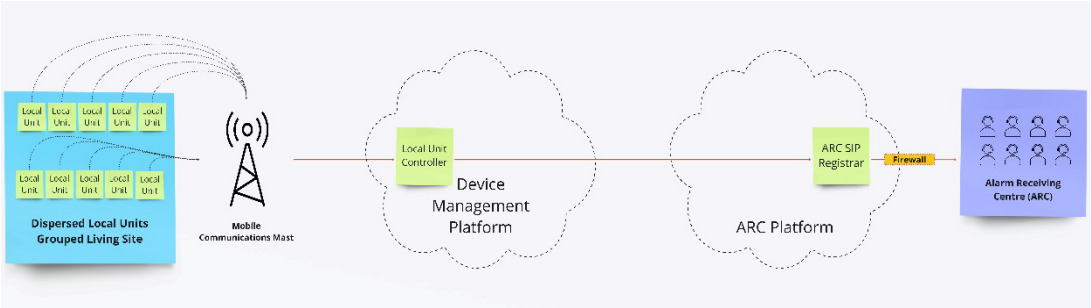
The natively digital grouped Local Unit Controller (LUC) and all the linked scheme Local Units (alarm devices in residences or communal areas) are registered with a local SIP registrar which is, in turn, connected to the Alarm Receiving Centre (ARC) Platform SIP registrar which means that only one SIP endpoint account needs to be set up for each scheme the ARC platform SIP registrar.



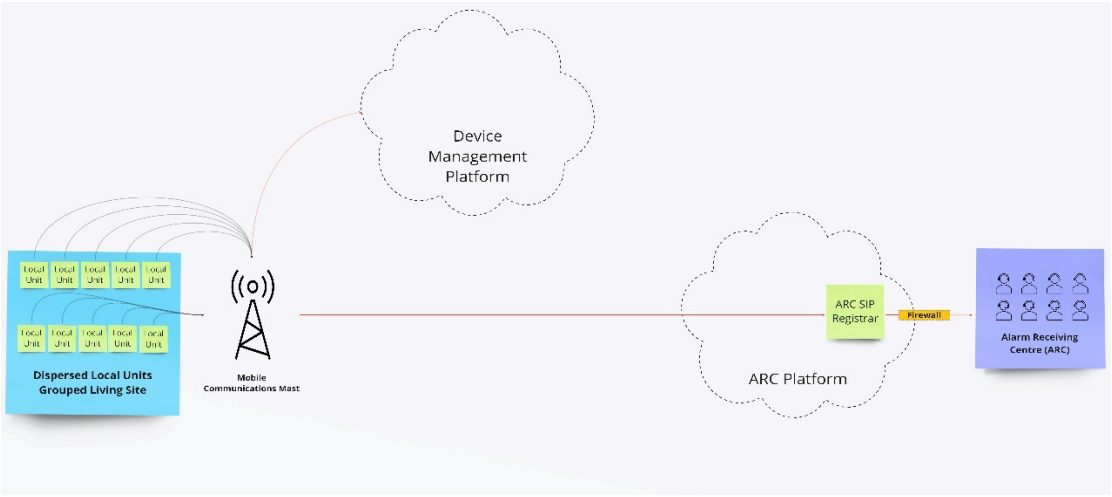
2.2. Fully End-to-End Digital Dispersed Scheme Solution

Dispersed units deployed in a scheme environment can be deployed in two ways:

a. The dispersed digital Local Units are grouped together under a Local Unit Controller (LUC) and that LUC is the SIP registrar for those dispersed Local Units. The LUC is registered with the ARC Platform SIP registrar which means that only one SIP endpoint account needs to be set up for each scheme the ARC platform SIP registrar.



b. The dispersed digital Local Units are registered directly with the Alarm Receiving Centre (ARC) platform SIP registrar which enables the ARC platform to have visibility of all of the scheme alarm devices connected to it. In this instance, each scheme Local Unit (alarm device) would require its own account (username / password etc…) on the ARC SIP registrar.



N.B. In practice, if dispersed units are deployed into a scheme environment, they are configured to communicate in TS50134-9 format rather than BS8521-2

3. Scheme Broadband / Cellular Connectivity and Resilience Guidance

Whilst there is no specific standard regarding scheme connectivity, the following recommendations are made which are based on best practice and conform with the requirements of the TEC resilience guidance (https://www.tsa-voice.org.uk/tec-guidance/the-end-to-end-resilience-of-technology-enabled-care-solutions/):

- Broadband as Primary or Secondary connectivity
- 4G VoLTE Cellular (single or dual roaming SIM) as Primary or Secondary Backup connectivity
- Break/Fix 1 hour maximum balanced across both connectivity paths
- Uptime target measured monthly balanced across all connectivity paths incorporating measures set in the TEC resilience guidance
- Uninterruptible Power Supply (UPS) connected to any controller equipment with minimum 8 hours power backup
    - Minimum 100 Mbps download / 30 Mbps Upload
    - Minimum 10 Mbps bandwidth per resident, if resident access required
    - Quality of Service enabled
    - RTP / SRTP voice stream enabled
    - Fixed IP addressing and Network Address Translation enabled
    - Minimum of 2 different cellular networks with over 30% signal strength
    - 4G VoLTE voice and data enabled
- End to End solution signed off by Technical Design Authority

4. Alarm Transmission Format

The following application guidance has been provided to assist organisations to follow industry best practice in terms of the configuration of digital grouped social alarm solutions using the common digital protocol BS8521-2

The messages sent by both the local controllers and/or local units to the ARC should consist of data from the data tables in the standard

- All non-voice communication between a local unit and an alarm receiving centre (ARC) shall be via SIP/SIMPLE instant messaging.
- The transfer of the alarm-related information shall be served by the MESSAGE method in accordance with RFC 3428 [N2].
- The information shall be carried in the body with the content-type “text/plain” with the restriction that the total length of the SIP message shall not exceed 1 300 bytes. The message body shall be based on an XML (extensible Markup Language) format.

The ARC shall use two SIP accounts (addresses) to handle SIP messages. One account shall be for IP alarm call handling and the other account shall be for IP alarm heartbeat message handling.

The IP alarm heartbeat should be agreed by the Commissioner/Buyer of the solution in conjunction with the suppliers of both the scheme equipment and ARC platform, but the minimum expectation is that the heartbeat should be sent by the device at least every 20 minutes with an alert sent to the monitoring provider if 3 consecutive heartbeats are missed.

5. Security Recommendations

Personal and sensitive data shall only be transmitted over a secure connection and Voice over Internet Protocol (VoIP) communication falls within that category and requires a secure connection.

That secure connection should be created using one of the following parameters as a minimum:

5.1. End-to-end Encryption

- The ARC shall present a valid ITU X509 certificate;
- The LUC shall verify the identity of the server certificate using a local Root CA certificate;
- The LUC to ARC SIP session shall be encrypted with TLS V1.2 or higher;
- The LUC to ARC SIP session shall use cryptographic algorithms AES-128 encryption minimum.

5.2. End-to-end Virtual Private Network (VPN)

- The VPN (or a combination of VPN and TLS) must run completely end to end from the scheme equipment 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

Ongoing management of the server certification should be agreed by the Commissioner/Buyer of the solution in conjunction with the suppliers of both the scheme equipment and ARC platform.

6. Sign off For Scheme / ARC Testing

Testing from the scheme to the ARC should be mandated by the Commissioner/Buyer prior to go-live of the scheme – it is the joint responsibility of the scheme equipment supplier and the ARC platform provider to ensure that adequate testing has taken place.

EXAMPLE SCHEME / ARC TESTING TEMPLATE	
Commissioning Organisation	
Lead Commissioner / Buyer	
On-Site Contact	
Equipment Supplier Contact	
ARC Platform / Monitoring Centre Contact	

Scheme Equipment	
Broadband / WAN Supplier	
SIM Network(s)	
ARC Platform / Version	
Protocol Version	
VPN Supplier (if applicable)	

Scheme ID	
Scheme Static IP Address	
Scheme Sub Net Mask	
Scheme IP Gateway	
Scheme Primary DNS	
Scheme Secondary DNS	

ARC Primary Domain	
ARC Secondary Domain	
ARC SIP Proxy Username	
ARC SIP Proxy Password	
ARC Primary SIP Username	
ARC Secondary SIP Username	
ARC Primary SIP Heartbeat Username	
ARC Secondary SIP Heartbeat Username	

		Handshake	Location	2 way Voice
Door Entry	Test 1			
	Test 2			
Door Contact Overall			Red/Amber/Green	
Smoke	Test 1			
	Test 2			
Smoke Overall			Red/Amber/Green	
Fire	Test 1			
	Test 2			
Fire Overall			Red/Amber/Green	
Personal Trigger	Test 1			
	Test 2			
Personal Trigger Overall			Red/Amber/Green	
Falls Trigger	Test 1			
	Test 2			
Falls Trigger Overall			Red/Amber/Green	
CO	Test 1			
	Test 2			
CO Overall			Red/Amber/Green	
Temp Extreme	Test 1			
	Test 2			
Temp Extreme Overall			Red/Amber/Green	
Mains Power	Test 1			
	Test 2			
Mains Power Overall			Red/Amber/Green	
Outbound Call from ARC	Test 1			
	Test 2			
Outbound Call from ARC			Red/Amber/Green	
Periodic Test	Test 1			
	Test 2			
Periodic Test Overall			Red/Amber/Green	
Heartbeat to the Heartbeat SIP Account	Test 1			
	Test 2			
Heartbeat Test Overall			Red/Amber/Green	
Failover Test	Test 1			
	Test 2			
Failover Test Overall			Red/Amber/Green	
Further devices as required	Test 1			
	Test 2			
Further devices as required			Red/Amber/Green	

Further Notes & Actions Required	

Sign Off	Signature	Date
Lead Commissioner / Buyer		
Equipment Supplier Contact		
ARC Platform / Monitoring Centre Contact		

7. Scheme Installer / Engineer / Maintainer Qualifications

It is recommended that any scheme equipment installers are suitably trained in the understanding of basic digital telephony standards as well as any specific training required on the scheme equipment itself.

In addition, there should be an allocated Project Engineer for each installation that has attained a higher level of training and experience in the following areas to support with the end to end connectivity between Scheme and ARC:

- Session Initiation Protocol (SIP)
- Internetworking
- The 7-layer model
- Troubleshooting TCP/IP using Wireshark
- IP Addressing
- IP configuration of Routers
- Analysis of TCP/IP packets
- Cyber Security
- Firewalls

Following successful implementation, all maintenance engineers should be trained to an equivalent standard to ensure ongoing issues are resolved as part of the maintenance contract.

8. Register of confirmed digital scheme connectivity using BS8521-2

As digital schemes are commissioned across the UK, a register will be kept of the known and verified interconnectivity between schemes, updated on a regular basis with any implementation notes. A summary of the current connectivity is shown below:

Equipment	Protocol	Appello Carenet	Chubb Care Control	Enovation Umo	Legrand Answerlink	Skyresponse	Tunstall PNC IP
Appello SLS	BS8521-2						
Appello Smart Connect	BS8521-2						
Chubb CareUnity CS	BS8521-2						
Everon Lyra	BS8521-2						
Legrand Care Advent XT2	BS8521-2						
Legrand Care Infinity	BS8521-2						

Key
Customer Verified
Under Testing
Not Connected

9. 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
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
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
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
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.
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
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
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