TECHNOLOGY ENABLED CARE

tec

CYMRU

Telecare Services in Wales

Interoperability & Protocols

September 2022

Background

Mission 2 of the TEC Cymru Telecare Programme states *"For Welsh Telecare services to use common data standards and interoperable protocols allowing for greater opportunities for widespread TEC adoption, shifting the narrative of reactive care to proactive".*

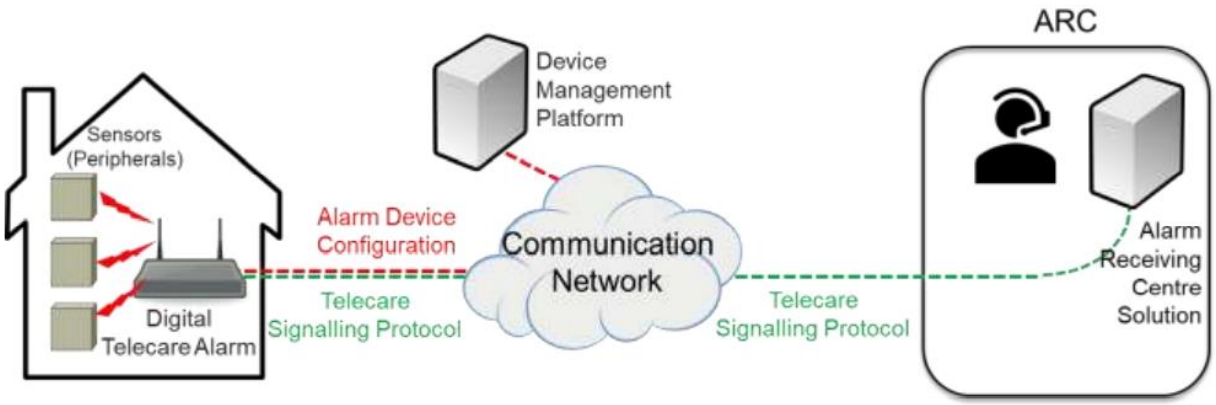
Technology Enabled Care products and solutions have the ability to successfully integrate elements of health and social care provided services. Telecare traditionally has operated using analogue connection nodes, typically PSTN and ISDN lines, operating on the traditional copper telecommunication exchanges. As we move towards the advent of 'all IP' and fibre, traditional telecare equipment will evolve into more mainstream technologies as the traditional analogue boxes are no longer supported.

Interoperability within the context of telecare, can be broken down into 4 component parts:

1. Telecare peripheral devices (how they communicate to the lifeline alarm)
2. Telecare ARC software (how the lifeline alarm communicates to the ARC)
3. Outbound data transfer (how the ARC 'talks' to third party databases)
4. Inbound data transfer (how the third party databases talk to the ARC)

Telecare Peripheral Devices

Problem/current state:
Telecare peripherals (pendants, smoke detectors etc.) are numerous. They are considered secondary pieces of technology that communicate with a central lifeline alarm, considered primary. Typically, this is done by radio signalling through a dedicated frequency for social alarms (Tunstall use 869 MHz/Tynetec use 169 MHz). This ensures that traffic is not interrupted, utilising a dedicated frequency/communication channel is vital for a 'life critical' service such as telecare. This however, is the first blocker in successful interoperability, with most of the peripherals on offer effectively 'locked' down to the supplier of the lifeline alarm.



With the impending transition to 'digital', the need for these peripherals to be 'backwards compatible' is also an issue. All suppliers bar one (Tynetec) currently ensure their new digital lifeline is compatible with their peripherals. Tynetec's digital lifeline alarm will only support their new range of 'digital' peripherals, which presents a problem to existing services with a large amount of peripherals in use. There are currently 4 local authorities in Wales who distribute Tynetec equipment. Some suppliers claim their peripheral devices can connect via Bluetooth, Zigbee and Z-Wave.

Solution:

The ideal solution would be for all suppliers of lifeline alarms to support other supplier's peripherals. This is easily achievable in an analogue context, however this has not been routinely done with suppliers keen to maintain a commercial advantage. It should be straight forward to implement in the near future, as some suppliers may shift their peripheral devices to an alternative method of communication to radio, by utilising IoT via a local gateway or Bluetooth.

Telecare ARC software

Problem/current state:

6 of the 7 ARC's in Wales are not digitally capable and operate in silo to one another. This is of particular frustration as all 6 are operated by Tunstall Healthcare. With 6 ARC's, Tunstall effectively are able to enter into local arrangements with local authority with no plans to join up the network of ARC's to provide consistent methods of data capture and reporting. As these ARC's all operate in an analogue setting, they will each need to be upgraded to digital in order to continue to support citizens with their telecare service. The majority of these ARC's in Wales, utilise proprietary signalling protocols (TT91/TT92/TTNEW) – The two T's stand for Tunstall and Tynetec. The two market leads effectively locking out competitors. These signalling protocols also limit other remote citizen/patient monitoring devices from utilising the lifeline alarm (telehealth) to communicate to a central location (ARC).

Solution:

When telecare services are planning on migrating their ARC platform to 'digital' TEC Cymru would strongly recommend that they state within their RFP document that the supplier of the ARC *"must configure their telecare solutions to use open protocols."* This approach means that the telecare solution can make use of equipment from a number of manufacturers, selecting equipment that offers the best features, or the best cost. Using open protocols also avoids the risk of supplier "lock in", where a telecare service using a proprietary protocol is forced to buy equipment from a single manufacturer because of the cost, effort and risk associated with moving the whole solution to an open protocol.

The open digital telecare protocols currently available are:

- SCAIP;
- TS50134-9 (CENELEC);
- NowIP.

Open Protocols

SCAIP

The Social Care Alarm over IP (SCAIP) protocol was developed in Sweden in 2014 to support the country's move to digital telecare. It is published by the Swedish Standards Institute as SS91100:2014. For several years SCAIP was the only open digital telecare protocol available for dispersed devices (primary lifeline alarms), and so it has been used widely for the digital telecare rollouts completed worldwide to date and is supported by a range of manufacturers' equipment.

The protocol defines the format for messages between the lifeline alarm and ARC. It defines two approaches to carrying voice traffic (calls): either as a separate dial-up phone call, or with voice carried over the digital connection as Voice over IP (VoIP).

A limitation of SCAIP is its lack of security. Telecare messages and potentially voice calls (where VoIP is used) are sent between the alarm unit and the alarm receiving centre unencrypted and so can be intercepted. While the protocol provides a degree of anonymisations by using device IDs, rather than personally identifiable information in messages, there is still scope for an unauthorised individual to access system information and potentially interfere with system operation. Where VoIP calls are used, the lack of encryption would allow eavesdropping on potentially sensitive conversations.

To ensure that digital telecare is deployed securely when SCAIP is used, the connection between the lifeline alarm and ARC must be secured using separate arrangements. Typically, SCAIP is deployed on devices that connect using the mobile telephone network. Where this is the case the mobile SIM provider can provide the required security, sending the signalling traffic to the ARC over a secure connection, rather than the Internet. If SCAIP is deployed on devices that use a fixed broadband connection (potentially a user's home internet service), then the connection must be encrypted using a dedicated security device, or by applying security on an existing network device in the home, such as an internet router. This setup is potentially complex to setup and manage and is one of the reasons that TEC Cymru would recommend Welsh telecare providers that digital telecare is deployed using mobile telephony for connectivity.

TS50134-9

The European Committee for Electro-technical Standardization (CENELEC) is one of the organisations responsible for developing European standards. It was responsible for developing a European standard for IP telecare devices, which resulted in the TS50134-9 standard being released. The standard is very similar to SCAIP (which was used as the starting point for the standard's development). TS50134-9 is also backwards compatible with SCAIP, meaning that devices using both protocols can be supported at the same time by an ARC. The main difference between TS50134-9 and SCAIP is security. TS50134-9 states that personal and sensitive data should only be transmitted over a secure connection.

A minimum security standard is defined of TLS V1.2 and AES-128 encryption. However, it is important that telecare services are aware that telecare equipment using TS50134-9 use different approaches to apply this security. Some devices do not encrypt data traffic themselves and assume that security is applied using other means (for example SIM security or a dedicated VPN device), whereas other telecare devices encrypt the data traffic themselves meaning that the connection is secured without the need for any other security arrangements being put in place. Where the device does not encrypt data traffic, the same security vulnerabilities exist as detailed for the SCAIP

protocol in the previous section. Telecare services must ensure that connections are secured using other means. The number of devices available in the marketplace that support the TS50134-9 protocol is more limited than for the SCAIP protocol. However, more manufacturers are planning to add support for the protocol in future product/software releases. Of the devices available that support TS50134-9, very few currently support encryption meaning that telecare services are likely to have to ensure that security is applied by other means.

NowIP

NowIP is a digital protocol originally developed by a number of telecare manufacturers for use in grouped schemes. NowIP is currently being adopted as a British Standard, and so is also known as BS8521-2 (not to be confused with BS8521, which is an analogue telecare standard).

NowIP assumes that the connection between the grouped scheme and ARC is secured using external arrangements (i.e. the security is not applied by the NowIP device itself). This, combined with the fact that NowIP sends voice calls with users as VoIP over the data connection, means that telecare services must ensure that appropriate arrangements are in place to secure the data connection.

Benefits

- Data is shared across the H&S spectrum allowing for greater person centred help and support;
- Greater efficiency in respect of data standards, access to real time data across multiple platforms;
- Promotes greater choice for citizens;
- Improves possibility of integration to wider digital health products and solutions (Apple watch, FitBit etc.);
- Suppliers no longer dictate to the marketplace on what to buy;
- Reduces cost for customers, as they don't need to update their peripheral devices;
- Enables service providers to continue to use existing telecare peripherals, whilst making the required move to digital connectivity;
- Reduces the environmental impact of throwing away devices just because they don't connect with the new device;
- Service users feel comfortable continuing with devices they already know works.

Proposal

TEC Cymru will recommend that telecare services use an open protocol instead of manufacturers' proprietary protocols wherever possible. It is recommended that telecare services use TS50134-9 for lifeline alarms, as this is the most recent standard and is a more robust version of SCAIP with added security/encryption measures. However, availability of equipment that uses this standard is limited, meaning that SCAIP can/will be used. TS50134- 9 is backwards compatible with SCAIP, meaning that any equipment using SCAIP should still be able to be used if telecare services move to TS50134-9 in the future.

Availability of equipment that offers the encrypted variant of TS50134-9 is extremely limited meaning that telecare services will need to ensure that appropriate security is applied to connections through other means. Where alarm devices use a mobile telephony connection, this security is likely to be provided by the SIM supplier, but this needs to be checked. Where a fixed

broadband connection is used for connectivity, connection security will need to be provided through other means, potentially using a dedicated or existing device to create a VPN.
Grouped schemes are currently limited to the use of the NowIP (BS8521-2) protocol. There is limited digital grouped scheme equipment available from the marketplace at present.

Aspect	Digital Telecare Protocols[1]		
	SCAIP	TS50134-9	NowIP (BS8521-2)
Defined by	Swedish Standards Institute (SWIS).	Progressed under European Committee for Electro-technical Standardisation (CENELEC), ratification by British Standards Institute (BSI).	NOW-IP project, intended to generate acceptance by Continua.
Applicable scenario	Communication between users and social services (LUC and ARC) - electronic messaging from LUC, data streaming channel, human-to-human channel.	As for SCAIP.	As for SCAIP plus an additional scenario is indicated: query / control / programming of local equipment by the ARC, such as door locks.
Grouped housing support	System configuration code for grouped equipment supported can identify a controlling unit and peripherals of that unit. It appears that a site controller that groups controlling units as part of a site cannot be identified.	As for SCAIP; development of the standard for better support of grouped housing is being considered as part of future new work item proposals.	System configuration code for grouped equipment supported includes things such as "Equipment Control Functions" and "Commands". Can identify the controller of a site/installation and a local unit within the installation.
Key base technologies	SIP MESSAGE or SIP + E.164 or SIP + RTP XML (SCAIP adaption) IP network.	As for SCAIP, plus TLS, and expands on details.	TLS SIP SIMPLE or SIP + RTP BS8521 data sequences IP network.
Information carried	Event messages, media streams (voice or multimedia sessions).	As for SCAIP; recognises that the alarm protocol and the media session may run over different network paths. Allows the media session to be on a non-IP connection.	As for SCAIP plus programming messages.
Summary of event messaging	Initiated by message from alarm sender. If the receiver returns the following message response of 'event was not received successfully' then the alarm sender will resend the message after short interval. Sender may also supply information update message at any time. Session is terminated when either receiver returns message to confirm that alarm handled or timeout is reached (send final reset message).	As for SCAIP.	Initiated by message from alarm sender. Receiver to respond with acknowledgement of the alarm. Sender to retry if session connection disrupted.
Summary of heartbeat messaging	Alarm sender sends heartbeat message. Receiver confirms open channel with response message.	As for SCAIP.	Alarm sender sends heartbeat message. Receiver can acknowledge or return command or programming message.

[1] TEC Scotland – Digital Playbook; Digital Telecare Protocols

Summary of media sessions	Begin with the basic event message protocol as above. If that session terminates with the receiver confirming readiness for the media session, then alarm sender can initiate that session. Session is terminated with request from either party. The session may carry DTMF audio tones to provide some control facilities for the receiver.	As for SCAIP plus support for a scenario (call back) where the sender requests a media session but that session is then initiated by the ARC.	Begin by ringing the receiver. Follow with basic event message protocol as above. Media stream starts when receiver OKs the invite. Session is terminated by the receiver.
Security	Left largely to considerations outside the standard. Points towards wrapping SCAIP into encryption provided by TLS. Requires authentication of alarm senders via HTTP. Authentication (not clear what that actually looks like when the person only holds a device with an alarm button).	Requires channel encryption via TLS (note that the minimum requirement is already outdated). Requires that the ARC is in possession of a valid certificate. Requires authentication of alarm senders via HTTP. Digest Note that this is framed in terms of capability to support ('shall'). It is left to the organisation to determine if the information requires this level of protection (for Personal and Sensitive data). This appears to open a path whereby a non-secured legacy device that complies with plain SCAIP can also be connected - if permitted.	Requires TLS, otherwise left to considerations outside the specification.
Other	Note that 'alarm' in this standard is a quite a flexible term. The codes from the dictionary show that this can also cover routine events such as door movement and light switches being operated.	Requires backwards compatibility to support products that comply with SCAIP.	