Picture credit: Getty

STAYING CONNECTED

Roderick Hodgson *on the importance of keeping the lines of communication open for emergency services with key decision makers in major incidents*

In cases of emergency response to incidents, first-responders need to communicate efficiently and securely with a large number of stakeholders. This communication extends not only to a variety of emergency services organisations, but also to others such as government officials.

The most widely used dedicated radio system for emergency services communications is the Terrestrial Trunked Radio (TETRA) standard, which remains reliable for its original purpose of voice communication. However, the way emergency services organisations work today means there is an increasing requirement for video and fast data transfer for documents, photography and data from other applications. While these are product features most users of commercial mobile infrastructure take for granted, TETRA's limited capacity cannot support the data bandwidth requirements of such communications.

Although TETRA is a recognised standard, operators have to date not demanded interoperability between systems from different vendors at purchase. They have also preferred a single emergency services communication supplier per country. As a result, emergency services agencies that have adopted TETRA have found themselves locked-in to a single supplier, limiting their ability to upgrade to different technologies. It has also placed limits on their ability to communicate with colleagues in neighbouring countries or organisations.

Features including the TETRA Enhanced Data Service and the TETRA Inter-System Interface (to build interoperability gateways between systems) have been added to TETRA to improve its services, but have seen limited uptake to date.

When TETRA was first standardised in 1995, commercial mobile infrastructure looked very different to how it does today. The third generation of wireless mobile telecommunications technology (3G) had not yet made its way into the consumer market. Since then, commercial mobile infrastructure has undergone a complete transformation, with the universal take up of 4G. Commercial mobile operators are now rapidly migrating to IP-based systems and are preparing for the roll-out of the next-generation consumer mobile technology, 5G. This investment in commercial mobile infrastructure is bringing increased performance and additional features to the user market.

Many countries are evaluating the use of this commercial mobile infrastructure to provide the necessary bandwidth and to deliver the much-needed additional capabilities to the emergency services. The 3rd Generation Partnership Project (3GPP) has developed a set of new standards for MCPTT that have been extended to include Mission-Critical Data and Mission-Critical Video. These standards have addressed a wider range of emergency services' requirements,

Emergency services require features more commonly found on domestic smartphones

IT IS ESSENTIAL TO USE PRODUCTS THAT SECURE DATA END-TO-END DURING AN EMERGENCY SITUATION

ensuring emergency services stakeholders continue to have the functionality they are accustomed to with TETRA, while leveraging recent innovation in commercial mobile infrastructure, bringing about significant advantages.

These include: increased data capacity, allowing users to efficiently share multimedia data such as pictures and videos; a single device for all voice and data-based applications, saving valuable personal space for other mission-essential equipment; the use of smartphone technology, allowing plain-clothed officers more discretion; cross-agency interoperability, enabling agencies to communicate with other colleagues; and an ecosystem of interoperable emergency services-focused products, shifting away from expensive and inflexible solutions towards off-the-shelf products that tap into economies of scale.

However, the adoption of commercial networks also exposes communications to a number of possible attack vectors common to other users of such commercial networks. For instance, commercial network users run the risk of disclosing sensitive information to potential attackers by failing to accurately confirm the identity of the person they are speaking with. Users may also be exchanging data through an internet service to which attackers have previously gained privileged network access, allowing them to retrieve multimedia data exchanged on a network.

The use of commercial mobile networks by emergency services could encourage attackers to target the commercial mobile infrastructure itself, or to set up a fake base station in close physical proximity to emergency services users during a major incident. This could allow an attacker to gain access to all data and call content, as well as metadata for all users on that base station. Attackers could further compromise the public mobile telephony network by offering public low-cost wholesale data routing during a major incident, potentially gaining access to all data routed over their network.

As a result, it is essential for stakeholders that have to interact during an emergency situation to use products that secure data end-to-end, rather than relying on the security provided by commercial mobile networks, which may not be sufficient in certain incident response scenarios. To address this, 3GPP has defined the Security of Mission-Critical Service, mandating the open cryptography standard Mikey-Sakke.

SECURE DATA TRANSFER

Mikey-Sakke is a cryptography standard with a unique key management approach – Identity-Based Public Key Cryptography (IDPKC). Techniques pioneered in the Mikey-Sakke protocol were designed to minimise the traffic overhead needed to exchange keys and to establish a secure data transfer between users, while largely removing the need for a public key infrastructure. Beyond its efficiency, it also has the advantage of helping to minimise infrastructure cost.

2012 saw the UK Government's National Technical Authority for Information and Assurance (CESG) – now the National Cyber Security Centre (NCSC) – define Mikey-Sakke as a protocol to answer the security requirements of the UK Government for an identity-validating cryptographic method in Government communications, at UK Official classification levels.

This protocol was based on an existing standard for elliptic curve signatures – the Elliptic Curve Digital Signature Algorithm (ECDSA) – and an identity-based cryptographic protocol developed by Japanese researchers Ryuichi Sakai and Masao Kasahara. This gave rise to Mikey-Sakke, which was made an open standard by the Internet Engineering Task Force (IETF), an organisation that develops and promotes voluntary internet standards.

Mikey-Sakke is configured so that each user is attached to a Key Management Server (KMS). This server distributes key information to the users it manages on a regular (typically monthly) basis. The existence of the KMS means that organisations have control over their own security system, without giving access to their data to unauthorised third parties. The KMS can also be managed entirely by an organisation's IT team and can be kept offline for maximum security. This means that organisations can retain full control over their security system, while only those explicitly authorised by an organisation can access that organisation's data.

Any participant in a communication session can validate the origin of the messages it receives by validating the signature against the public key material of the KMS controlling that system. This means communication between users controlled by different KMS can be enabled. In this way, secure communication is enabled beyond the boundaries of a given agency or organisation. Enabling communication in this way is especially important for major incidents in cross-border mission-critical scenarios, where a diverse set of stakeholders from different countries and organisations may need to be involved.

SECURE COMMUNICATION

While the standards developed by 3GPP ensure interoperability between users of MCPTT systems, in major incident scenarios, emergency services organisations may also need to communicate securely with other relevant stakeholders. For example, Government representatives that may not be users of MCPTT solutions on a day-to-day basis, favouring instead mobile applications that answer their individual communication requirements.

These commonly available mobile applications may offer a degree of security, however are typically not able to communicate with users of MCPTT, leading to operational inefficiency. One of the solutions for users not using MCPTT on a day-to-day basis is to adopt technologies that include Mikey-Sakke and are capable of communicating with each other in a secure way.

Secure Chorus, in collaboration with its industry members, is developing interoperability standards that respond to an extensive set of enterprise and Government requirements. As with MCPTT, its interoperability standards have selected Mikey-Sakke as the underlying cryptography standard.

Unlike users of many consumer-focused mobile applications, users of products that include Mikey-Sakke and Secure Chorus' interoperability standards are able to communicate securely with one another. This ensures secure data communication and processing within the security perimeter of an organisation and beyond, including potential worldwide geographical scope.

Unlike the MCPTT standards, Secure Chorus' interoperability standards were written to enable the development of a wide variety of products for capability suited to a broad range of modern use cases across industries. Facilitated by the fact that Secure Chorus' interoperability uses the same cryptography

EMERGENCY SERVICES HAVE AN INCREASING REQUIREMENT FOR VIDEO AND FAST DATA TRANSFER

standards as the MCPTT standards and is auditable, there is now a much lower bar to providing assured interoperability between Mission-Critical public safety networks and solutions that have adopted Secure Chorus' interoperability standards, with potential gains for all. User groups therefore have the opportunity to securely communicate with public safety network users, should they have this requirement.

Multimedia communication technology products developed according to Secure Chorus' interoperability standards have other added benefits conferred by their inclusion of Mikey-Sakke. They are highly scalable, requiring no prior setup between users or distribution of user certificates. They are also highly flexible, supporting real-time communications (voice), conference calls, and deferred delivery (messaging and voicemail) ●

Roderick Hodgson, Director – Secure Chorus, is a technologist and innovation strategist with oversight of all technology aspects of Secure Chorus, including technical management, setting technical strategy and representing the technology externally. Throughout his career he has defined, developed and delivered disruptive products in video streaming, telecoms, cyber security, IoT and Big Data for many organisations.

Services that use TETRA have found themselves locked-in to a single supplier

Picture credit: Getty