secure chorus

WHITE PAPER

EMERGENCY SERVICES COMMUNICATIONS

Secure Chorus Compliant Products interoperability with Mission-Critical Push-to-Talk Products

November 2018

Table Contents

Disclaimer

Acknowledgements

The development of this white paper benefited significantly from the input and support provided by Dr Kit Kilgour. Secure Chorus Ltd would like to give special thanks to Dr Kit Kilgour for sharing his time and expertise with us. While the white paper has benefited greatly from his guidance, the views it contains are solely those of Secure Chorus Ltd and may not necessarily reflect the views of Dr Kit Kilgour.

1 List of Acronyms

3GPP	3rd Generation Partnership Project
4G	4th Generation cellular network technology
5G	5th Generation wireless systems
HTTPS	Hypertext Transfer Protocol (Secure)
IDPKC	Identity-Based Public Key Cryptography
KMS	Key Management Server
LTE	Long-Term Evolution
MCPTT	Mission-Critical Push-to-Talk
MIKEY	Multimedia Internet KEYing
RFC	Request For Comments
SAKKE	Sakai-Kasahara Key Encryption
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio

2 About Secure Chorus

Secure Chorus is a not-for-profit membership organisation serving as a platform for multi-stakeholder cooperation for the development of forward-looking strategies, common technology standards and tangible capabilities in the field of information security. Central to the Secure Chorus philosophy is that to effectively address data security requirements in enterprise, information security solutions need to be secure, regulatory compliant and interoperable.

Secure Chorus has brought together a community of inspiring organisations from across the globe, including governments, supranational organisations and private organisations, from large established global enterprises through to technology start-ups, academic institutions, regulators, trade associations and standards bodies.

.

3 Executive Summary

3 Executive Summary

Public safety is an essential function of any government as it ensures the protection of civil society, organisations and institutions against public safety incidents including, but not limited to, large events, pandemics, severe accidents, environmental disasters and terrorism attacks posing threats to public security and order.

Public safety agencies include emergency services and others in the fields of civil protection, including emergency medical services and healthcare, police, border guards, fire service, civil aviation, disaster prevention, armed forces and the security services.

In response to unplanned events, geopolitical crises, natural and man-made disasters, public safety organisations and other relevant stakeholders require reliable, secure and interoperable multimedia communication technologies to support their operational effectiveness and service delivery.

In particular, public safety agencies require multimedia communications to be secure and interoperable to ensure the smooth operations of intra- and inter-organisational and, at times, cross-jurisdictional coordination.

Terrestrial Trunked Radio (TETRA) has been widely adopted as the standard for such communication, along with Project 25 (P25) in the USA.

With commercial communication technology completely transformed since the development of TETRA, expectations of functionality and reliability for users of radio systems today are higher than ever. TETRA, designed for voice, remains extremely reliable, but has limited capacity to handle the vast demands for data bandwidth of media-rich communications that are an essential part of many modern user requirements.

Commercial mobile network operators are now rapidly migrating to IP-based networks and are preparing for the roll-out of 5G. The increased performance and added feature-set of next-generation consumer mobile networks, including device-to-device communication, means that many countries are examining the viability of using commercial mobile networks to provide increased capability and make the best possible use of radio frequencies to address the requirements of public safety multimedia communications.

In the past, the lack of harmonisation across the industry and the absence of interoperable solutions for public safety use-cases presented a barrier to the standardisation of commercial networks for public safety networks. Today, however, standardisation efforts for providing public safety networks over 4G are currently being undertaken at an international level, coordinated by the 3rd Generation Partnership Project (3GPP) – the standards body responsible for mobile communications – in their development of a family of standards for "Mission-Critical Push-to-Talk" (MCPTT), extended to include Mission Critical Data and Mission Critical Video.

The MIKEY-SAKKE protocol, which was standardised in the Internet Engineering Task Force (IETF), has been chosen by 3GPP for use in the MCPTT standards.

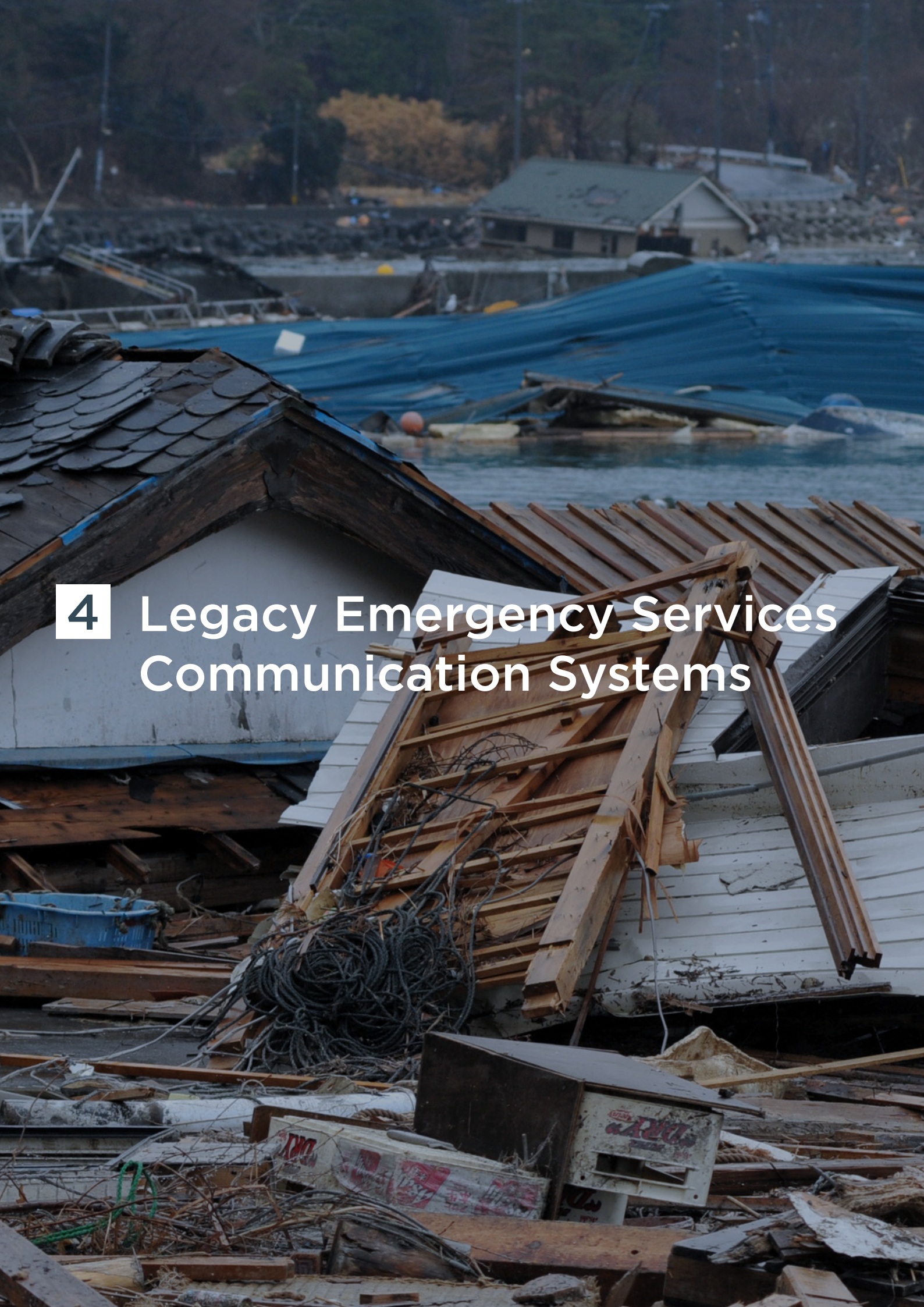
MIKEY-SAKKE is an open cryptography standard designed to enable secure, cross-platform multimedia communications. In this paper we will provide an overview of MIKEY-SAKKE and explain why its characteristics are well suited for secure and interoperable multimedia communication technology products for emergency services organisations. We will also highlight why its characteristics are well suited for other stakeholders that may have slightly different communication requirements, but may need to communicate securely with emergency services agencies from time to time.

While all solutions that adopt MIKEY-SAKKE as an underlying cryptography protocol have the potential to interoperate with one another, it is only with common interoperability standards, such as those defined by 3GPP for Mission-Critical Push-to-Talk, that products developed by different vendors will be able to reliably communicate with each other.

Whilst 3GPP has developed the MCPTT standards to create a common set of interoperability standards for use within public safety scenarios, one further key requirement for a secure multimedia communication ecosystem for the public safety community is that any stakeholder can communicate with any other stakeholder in that community securely. This must hold true even if one such stakeholder isn't a typical user of an MCPTT-approved product.

We will also further explain how Secure Chorus, through industry collaboration and common interoperability standards, has enabled the development of a growing ecosystem of interoperable and secure multimedia communication technology products that all have the MIKEY-SAKKE open cryptography standard at their core, and which have been developed for a wide range of use-cases and a variety of stakeholders.

We will further explain how such Secure Chorus Compliant Products can interoperate with the Push-to-Talk products developed specifically for public safety scenarios, facilitated by the fact that they all use the same open cryptography standard: MIKEY-SAKKE.



4 Legacy Emergency Services Communication Systems

5 Legacy Emergency Services Communication Systems

Public safety communications systems are typically based on an implementation of TETRA (terrestrial trunked radio) or P25. TETRA is a European Telecommunications Institute Standard (ETSI) first published in 1995, whilst P25 was developed in the USA by APCO – the Association of Public Safety Communications Officials at around the same time.

Although TETRA provides a multitude of essential functionality to its users in public safety, its extensibility to match the modern demands and requirements of its users is limited. P25 has a more limited feature set than TETRA.

The growth of 4G networks against the backdrop of TETRA's limited extensibility offers an opportunity today for new approaches leveraging commercial infrastructure.

When it was designed [1], TETRA was developed with a number of unique and innovative features of specific use to public safety applications that are still in use today:

Group calls with Push-to-Talk (PTT) capability – TETRA provides communication capability where a button can be used to switch between voice reception and voice transmission modes.

Control – TETRA provides advanced controls over who is able to transmit and who can only receive, at a given point in time (floor priority), as well as the ability to prioritise certain communications (pre-emption).

Distress communication – TETRA provides capability for transmitting an emergency distress signal.

Discreet Listening (DL) and recording – TETRA recording can occur continuously, while ensuring such recordings can be used for evidential purposes, and thus may have to be kept for a 'lifetime'.

Direct Mode (or Proximity Services "ProSe") – TETRA provides for device-to-device communication services when devices are in proximity to one-another and the radio network cannot be relied upon.

Location – TETRA provides capability for communicating the location of a user of a system, for example to a dispatcher.

Dedicated hardware – A range of TETRA-compatible devices are available, customised to the requirements of public safety use cases, including ruggedised handsets with dedicated control or emergency signal buttons.

Although TETRA is a recognised standard, and thus competition exists in the market, operators did not demand interoperability between systems from different vendors at purchase. They also preferred a single public safety supplier per country. Consequently, many of these systems do not interoperate with each other, meaning that customers are 'locked' into their supplier. Some progress is being made via the recent deployment of the standardised TETRA Inter-System Interface between countries in Northern Europe, but use is still limited.

Public safety users consider the functionality provided by TETRA to be essential functionality. Yet, in order to transform the way in which they work, they now need video and fast data transfer for documents, photos and data from other applications: features that most consumer users of mobile networks today take for granted.

TETRA requires its own dedicated radio frequency (spectrum), an increasingly scarce and costly commodity, with its own radio base stations and core network infrastructure. Fundamentally, TETRA was designed for voice and has very little capacity to handle data beyond message-based solutions: certainly not the vast amounts of data that modern applications demand.

Although attempts have been made to evolve TETRA and increase data throughput using TETRA Enhanced Data Service (TEDS) [2] there has been very little use of this new standard because of spectrum scarcity. While TETRA is still being rolled out around the world, early adopters are finding that the equipment deployed to provide their TETRA service is nearing the end of its life and so will need augmentation, renewal or replacement.

Given the constant evolution of commercial mobile network technology, along with the need to make the best possible use of radio frequencies, many countries are consequently looking at the viability of using commercial mobile networks where a guarantee of priority can be provided in an emergency.

5 Emergency Services Communication Over Public Mobile Networks

5 Emergency Services Communication Over Public Mobile Networks

Commercial network operators are now rapidly migrating to IP-based networks and preparing for the roll-out of 5G. The increased performance and added feature set of next-generation consumer mobile networks, including device-to-device communication, are very appealing to public safety use cases.

However, with lives potentially at stake, the requirement for reliability in communications is significantly higher in public safety networks compared with commercial mobile networks. Users of a public safety communication system must have the confidence that, by pressing a single button labelled "Push-to-Talk", they can reliably communicate with those they need to speak to.

The term "Mission-Critical Push-to-Talk" (MCPTT) refers to Push-to-Talk solutions that can support the requirements of public safety applications. The term is now commonly used to refer to a set of standards developed by the 3rd Generation Partnership Project (3GPP), the standards body responsible for mobile communications.

Although the recent roll-out of 4G commercial mobile networks has been in response to the evolving needs of consumers, the MCPTT standards allow public safety agencies to leverage this investment in commercial infrastructure, bringing about significant advantages without compromising the functionality expected by users of TETRA systems.

Such advantages include:

Mobile broadband data capacity – the data capacity of 4G networks is significantly higher than TETRA networks.

Single device – users only need to carry a single device for all voice and data-based applications, saving valuable personal space for other mission-essential equipment.

Smartphone systems – users who do not wish to be recognised as a member of a public safety agency can carry an ordinary smartphone that is running public safety software.

Cost savings/economies of scale – the use of commercial networks leverages the investment in infrastructure made for a large consumer base.

Cross-agency interoperability – with a common international standard offering interoperability, different agencies have the possibility to communicate with each other and collaborate in missions.

Ecosystem of interoperable solutions – A wide range of products and services can be built around the standards, presenting a shift from traditional expensive and inflexible system integration to standards-based interoperability, enabling commercial off-the-shelf applications from multiple suppliers as well as bespoke solutions that remain adaptable, repeatable and scalable.

The standards development efforts have happened in stages, as part of the release cycle of 3GPP's Long-term Evolution (LTE), the standards for 4G mobile telephony.

3GPP LTE Release 13 [3] saw the completion of the first set of specifications covering Mission-Critical services, in particular Push-to-Talk. It was frozen in March 2016.

LTE Release 14 [4] contained Mission-Critical enhancements beyond Push-to-Talk, such as Mission-Critical Video and Mission-Critical Data services. It was frozen in June 2017.

Release 15 [5] contains further Mission-Critical enhancements to data, video and voice usage, including interworking with LMR systems such as TETRA, P25 and Digital Mobile Radio (DMR), as well as laying the groundwork for future Mission-Critical railway needs. It was functionally frozen at the end of 2017 and is expected to be completed in late 2018.

Release 16 will continue to add new features including Discreet Listening (DL) and further enhanced railway capabilities, including interworking with legacy mission-critical railway systems such as GSM-R, with an expected completion in December 2019.

Products compliant with the 3GPP standards are available on Android, iOS and Windows, as well as on dedicated hardware solutions. The assumption is that services will run over a public 4G-radio network that offers priority to public safety users, although there is nothing to prevent the use of a private network.

The use of public 4G networks brings about a wide range of significant advantages to users of public safety communication systems, leveraging the investment in commercial solutions. The security of the data exchanged over public networks is, however, essential and was carefully considered in the standards.

6 Securing Data And Authenticating The Source Of Data In Public Safety Networks

6 Securing Data And Authenticating The Source Of Data In Public Safety Networks

The essential requirements of the public safety agencies going forward are for voice, data and video. For voice, the main features of the Mission-Critical Push-to-Talk (MCPTT) requirements are described in 3GPP TS 22.179 'Mission-critical Push-to-Talk' [6]. Similarly, there are corresponding requirements documents for data and video in 3GPP TS 22.282 [15] and 3GPP TS 22.281 [16] respectively.

The use of commercial networks potentially exposes public safety communications to an increase in the possible attack vectors, including:

- A call made or received by an attacker, in which the user divulges sensitive information without realising the person they are speaking to is not who they think they are.
- An attacker that gains privileged network access to an organisation's premises, retrieving all call and multimedia data exchanged on a network.
- An attacker compromising elements of the public mobile telephony infrastructure or using a fake base station in close physical proximity to its target, thus gaining access to all data and call content and metadata for all users on that base station.
- An attacker offering public telephony networks low-cost wholesale data routing, potentially having access to all data routed over their network.

It is essential, therefore, to ensure that data is protected end-to-end, and that data recipients can be confidant that the content has come from a genuine source.

To address this, the mobile communications standards body (3GPP) defining the 'Security of Mission Critical Service' [7] (4G) has mandated MIKEY-SAKKE as the cryptography standard to be used for the encryption of data, as well as for the provisioning of cryptographic keys.

There are also the 'Study on security enhancements for Mission Critical Push to Talk (MCPTT) over LTE' (TR 33.879) [8], and 'Study on mission critical security enhancements' (TR 33.880 [9]. These include an analysis of the threats to the service (voice, video and data), the security requirements to mitigate those threats and an evaluation of possible technical solutions designed to meet the security requirements of the service.

MIKEY-SAKKE [10] is a method of encrypting communication data with a unique key management approach, using Identity-based Public Key Cryptography (IDPKC).

The techniques pioneered in the MIKEY-SAKKE protocol have been designed to minimise the traffic overhead needed to exchange keys and establish a secure data transfer or voice call between users while largely removing the need for a public key infrastructure. It is very efficient while minimising infrastructure cost.

Origins of MIKEY-SAKKE

In 2012, the UK Government's National Technical Authority for Information and Assurance (CESG) – now The National Cyber Security Centre (NCSC) – defined MIKEY-SAKKE as an open cryptography standard, in answer to the UK Government's secure communication requirements at OFFICIAL, and to have a cryptographic method for validating an identity for government communications.

An introduction is provided in two NCSC documents:

1. Using MIKEY-SAKKE – Building secure multimedia services (Issue no: 1.0, April 2014), now superseded by an NCSC White paper dated 28 September 2016. [11]

1. A MIKEY-SAKKE/SRTP profile (Technical Specification No. 63, Issue No: 1.0, January 2013). [12]

These refer to all the relevant standards, reports and research papers needed to get a theoretical understading of MIKEY-SAKKE.

MIKEY-SAKKE was based upon an existing standard for elliptic curve signatures, the Elliptic Curve Digital Signature Algorithm (ECDSA) and an identity-based cryptographic protocol developed by two Japanese researchers, Ryuichi Sakai and Masao Kasahara. Combining these protocols for secure communications gave rise to MIKEY-SAKKE.

The Internet Engineering Task Force RFCs that describe the innovative aspects of MIKEY-SAKKE developed by the NCSC are:

6507 Elliptic Curve-based Certificateless Signatures for Identity-based encryption (ECCSI) [13]

6508 Sakai-Kasahara Key Encryption (SAKKE) [14]

6509 MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet Keying (MIKEY) [10]

What makes MIKEY-SAKKE ideally suited for multimedia communication technology products for use by public safety organisations?

Identity-based Public Key Cryptography (IDPKC) is a public -key cryptography method that allows for data to be encrypted for a user, based upon the knowledge of the identity of that user within a system. Users are identified by their name, role, phone number or any other identifier.

End-to-end encryption of multimedia data can be performed with widespread data encryption technologies, such as the Advanced Encryption Scheme (AES). In such an approach, all participating parties need to have access to the same AES keys, used for encrypting the data traffic between the parties ("traffic keys").

The central innovation in MIKEY-SAKKE is the idea that the initiator of communication may send a message, called a MIKEY message, to the recipient containing these traffic keys. The MIKEY message itself is encrypted using the recipient's identity. Only a legitimate intended recipient can decrypt this message, recovering the traffic keys. As the message is also signed using an electronic signature, the recipient is also able to verify the identity of the sender, all through a single message.

This idea extends to group calls and group data by sending a separate message to each member of the group, encrypted to their identity. As before, only the intended recipients are able to recover the traffic key and they can verify that it was sent by the initiator – the group management server.

Another design goal was the ability for a group of users to communicate with each other at an incident when they have no communication back to their control room. This is possible with MIKEY-SAKKE, where vehicle-mounted repeater equipment can provide everything needed for the group to communicate among themselves, or directly at short range, using LTE Proximity Services (ProSe). This effectively corresponds to TETRA's Direct Mode.

Key Management Servers

The architecture of MIKEY-SAKKE defines that each system in a network exchanging data is attached to a Key Management Server (KMS). The server distributes key information to the systems it manages on a periodical (monthly or yearly) basis.

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 KMSs can be enabled. In this way, secure communication is enabled beyond the boundaries of a given agency or organisation.

The existence of the KMS means that an agency has access to its own encrypted data, without giving access to unauthorised third parties. This key management system can also be kept off-line if required, while still allowing for lawful interception of emergency communications.

As MIKEY-SAKKE standards are publicly available, the validity of the algorithms can be independently verified. These modern standards permit flexible and dynamic security associations to be made without the costs associated with public key infrastructure and online certificate authorities, such as those using X.509 certificates used in HTTPS communication.

With MIKEY-SAKKE, user identifiers (such as phone number, name or role) are used as public keys. MIKEY-SAKKE effectively addresses the security requirements of public safety multimedia communication by providing data confidentiality and authentication of participants: all while enabling efficient key management and responding to the requirements of inter-organisational communication and lawful interception.

7 Secure Chorus: Interoperability Standards For Multimedia Communication Technologies Based On MIKEY-SAKKE

7 Secure Chorus: Interoperability Standards For Multimedia Communication Technologies Based On MIKEY-SAKKE

Secure Chorus, through industry collaboration and common interoperability standards, has enabled the development of a growing ecosystem of interoperable and secure multimedia communication technology products that all have MIKEY-SAKKE at their core.

The MCPTT-related standards developed by 3GPP address the specific requirements of public safety stakeholders, ensuring they continue to have the functionality they are accustomed to from their use of TETRA, while also leveraging the innovation in commercial mobile network technology.

In certain public safety scenarios, public safety 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.

Existing secure communication technology solutions, such as consumer-focused mobile applications, may offer a degree of security for these relevant stakeholders, but require that all users adopt the same solution. This means that initiators and recipients of the relevant information can only establish a secure channel if both parties use the same solution. More importantly, users of such solutions would not be able to communicate with users of public safety communication networks.

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 the MCPTT standards, Secure Chorus' interoperability standards have selected MIKEY-SAKKE as the underlying cryptography standard.

Unlike users of many consumer-focused mobile applications, users of different Secure Chorus Compliant Products are able to communicate 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 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.

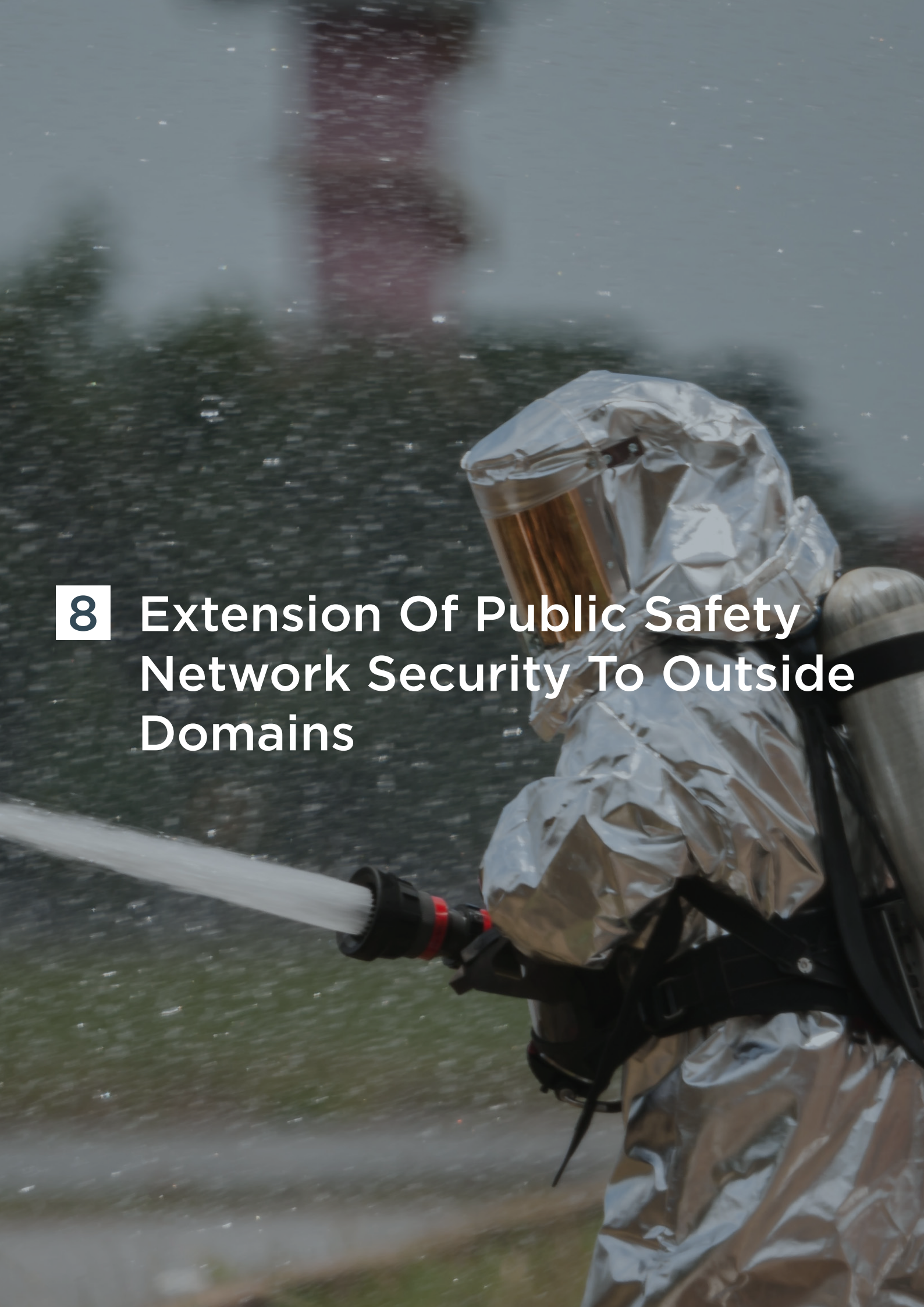
Multimedia communication technology products developed according to Secure Chorus' interoperability standards have other added benefits conferred by their inclusion of MIKEY-SAKKE. They are highly scalable, requiring no prior setup between users or distribution of user certificates. They are also highly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

As with the MCPTT standards, Secure Chorus' standards also allow these technologies to be centrally managed by an organisation, giving the domain manager full control of the security of the system as well as the ability to comply with any auditing requirements through a managed and logged process.

Since Secure Chorus upholds open industry cryptography standards, it is possible for an organisation – and the regulatory bodies that it is required to comply with – to assess if the technology meets Information Assurance (IA) requirements.

With a landscape of increasing regulation, including the EU General Data Protection Regulation (GDPR), mandating certain security and auditability requirements, solutions that leverage cutting-edge cryptographic innovation are needed now more than ever. Article 4 of the GDPR specifically includes public authorities in the definitions of data controllers and processors. There are other instances where specific terms are applied to public authorities to account for local laws and the effective operation of government. The only specific derogation relating to public authorities is where these are from non-EU countries and would otherwise be required to maintain a representative in the EU (Article 27 of the GDPR).

Public safety agencies are complex multi-actor environments and provide a good comparative model for enterprise and government secure communication applications. Secure Chorus has leveraged the innovation achieved in this industry and the unique features of MIKEY-SAKKE to deliver a growing ecosystem of interoperable products that answer the varied needs of a range of enterprise and government users. Through Secure Chorus, stakeholders now have the opportunity to choose solutions that not only enable communication with users of other multimedia communication solutions, but also create the opportunity for users to communicate with users of MCPTT-compliant public safety networks.



8 Extension Of Public Safety Network Security To Outside Domains

8 Extension Of Public Safety Network Security To Outside Domains

Secure Chorus, through industry collaboration and common interoperability standards, has enabled the development of a growing ecosystem of interoperable and secure multimedia communication technology products that all have MIKEY-SAKKE at their core.

The MCPTT-related standards developed by 3GPP address the specific requirements of public safety stakeholders, ensuring they continue to have the functionality they are accustomed to from their use of TETRA, while also leveraging the innovation in commercial mobile network technology.

In certain public safety scenarios, public safety 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.

Existing secure communication technology solutions, such as consumer-focused mobile applications, may offer a degree of security for these relevant stakeholders, but require that all users adopt the same solution. This means that initiators and recipients of the relevant information can only establish a secure channel if both parties use the same solution. More importantly, users of such solutions would not be able to communicate with users of public safety communication networks.

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 the MCPTT standards, Secure Chorus' interoperability standards have selected MIKEY-SAKKE as the underlying cryptography standard.

Unlike users of many consumer-focused mobile applications, users of different Secure Chorus Compliant Products are able to communicate 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 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 (such as voice), conference calls, and deferred delivery (such as messaging and voicemail).

9 Conclusion

9 Conclusion

Communication technology in public safety networks is undergoing rapid change. In many countries, Terrestrial Trunked Radio (TETRA), which has been widely adopted as the standard for communication by public safety agencies, is being augmented or replaced with an interoperable standard that leverages public mobile telephony networks – the Mission-Critical family of standards, developed by 3GPP.

Products are now available that provide public safety communication capability over public networks. These networks offer higher data capacity, additional functionality and more efficient use of radio spectrum without sacrificing key TETRA requirements.

When using public networks, the security of public safety networks is paramount. The responsible standardisation bodies have adopted MIKEY-SAKKE for this purpose, offering both data confidentiality and authentication of participants.

Secure Chorus leverages the key innovations developed in MIKEY-SAKKE – Secure Chorus' open cryptography standard of choice – to address modern needs for secure multimedia communications. Secure Chorus' interoperability standards allow for the creation of a marketplace of secure, regulatory compliant and interoperable solutions with essential functionality that suits the requirements of the day-to-day activities of a wide range of users.

Secure Chorus, through the work achieved by its members' collaboration, leverages the innovation that has enabled public safety communication solutions to interoperate over consumer networks, in order to transform the secure communication market from small islands of proprietary security into a vibrant security ecosystem. Because Secure Chorus has selected the same cryptography standard as in the 3GPP Mission-Critical family, there is now a much lower bar to providing assured interoperability with public safety networks. This provides enhanced capability for organisations that require communication with users of public safety networks.

Secure Chorus' technology roadmap is developed by consensus amongst its members, generating a multi-layered, time-based chart enabling technology development to be aligned with market trends and drivers, expanding the standards beyond secure voice calls to group calls, instant messaging, video calls, voicemail, document sharing and machine-to-machine communications.

Secure Chorus and its members are also studying other areas of innovation, including the development of post-quantum computing capability with the introduction of a Post Quantum Identity Based Crypto Scheme. Secure Chorus will be seeking input from industry, academia and government to identify the right solution to address this critical challenge.

10 References

[1] ETSI EN 300 392-2, "European Standard (Telecommunications series); Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)," 2001. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039202/.

[2] ETSI TS 100 392-2, "Technical Specification; Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)," 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/100300_100399/10039202.

[3] 3GPP, "Release 13," [Online]. Available: http://www.3gpp.org/release-13.

[4] 3GPP, "Release 14," [Online]. Available: http://www.3gpp.org/release-14.

[5] 3GPP, "Release 15," [Online]. Available: http://www.3gpp.org/release-15.

[6] 3GPP TS 22.179, "Technical Specification; Mission Critical Push To Talk (MCPTT); Stage 1," 2016. [Online]. Available: http://www.3gpp.org/DynaReport/22179.htm.

[7] 3GPP TS 33.180, "Technical Specification "Security of the mission critical service"," 2016. [Online]. Available: http://www.3gpp.org/DynaReport/33180.htm.

[8] 3GPP TR 33.879, "Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security enhancements for Mission Critical Push To Talk (MCPTT) over LTE (Release 13)," 2016.

[9] 3GPP TR 33.880, "Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on mission critical security enhancements," 2016.

[10] IETF, "RFC 6509 - MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)," February 2012. [Online]. Available: https://tools.ietf.org/html/rfc6509.

[11] NCSC, "Using MIKEY-SAKKE: Building secure multimedia services," 28 September 2016. [Online]. Available: https://www.ncsc.gov.uk/articles/using-mikey-sakke-building-secure-multimedia-services.

[12] CESG, "Technical Specification; A MIKEY-SAKKE / SRTP profile," 2013. [Online]. Available: https://www.ncsc.gov.uk/document/mikey-sakke-srtp-profile-technical-specification.

[13] IETF, "RFC 6507 - Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)," February 2012. [Online]. Available: https://tools.ietf.org/html/rfc6507.

[14] IETF, "RFC 6508 - Sakai-Kasahara Key Encryption (SAKKE)," February 2012. [Online]. Available: https://tools.ietf.org/html/rfc6508.

[15] 3GPP TS 22.282, "Technical Specification; Mission Critical Data services,". [Online]. Available: http://www.3gpp.org/DynaReport/22282.htm.

[16] 3GPP TS 22.281, "Mission Critical Video services". [Online]. Available: http://www.3gpp.org/DynaReport/22281.htm.

secure chorus

CONTACT DETAILS:

One Canada Square,
Canary Wharf,
London E14 5AB

General Inquiries: **info@securechorus.org**
Membership Inquiries: **membership@securechorus.org**

www.securechorus.org

@SecureChorus

/company/secure-chorus-ltd/

Design
www.springboardmarketing.co.uk