

The logo for 'secure chorus' is displayed in a lowercase, sans-serif font. The word 'secure' is followed by 'chorus', where the letter 'o' is replaced by a white keyhole icon. The background of the entire page is a dark blue gradient with a complex network of white lines and dots, resembling a data network or a constellation of stars.

secure chorus

WHITE PAPER

# General Data Protection Regulation (GDPR)

Open standards for secure processing of personal data  
within the security perimeters of an organisation and beyond

October 2017

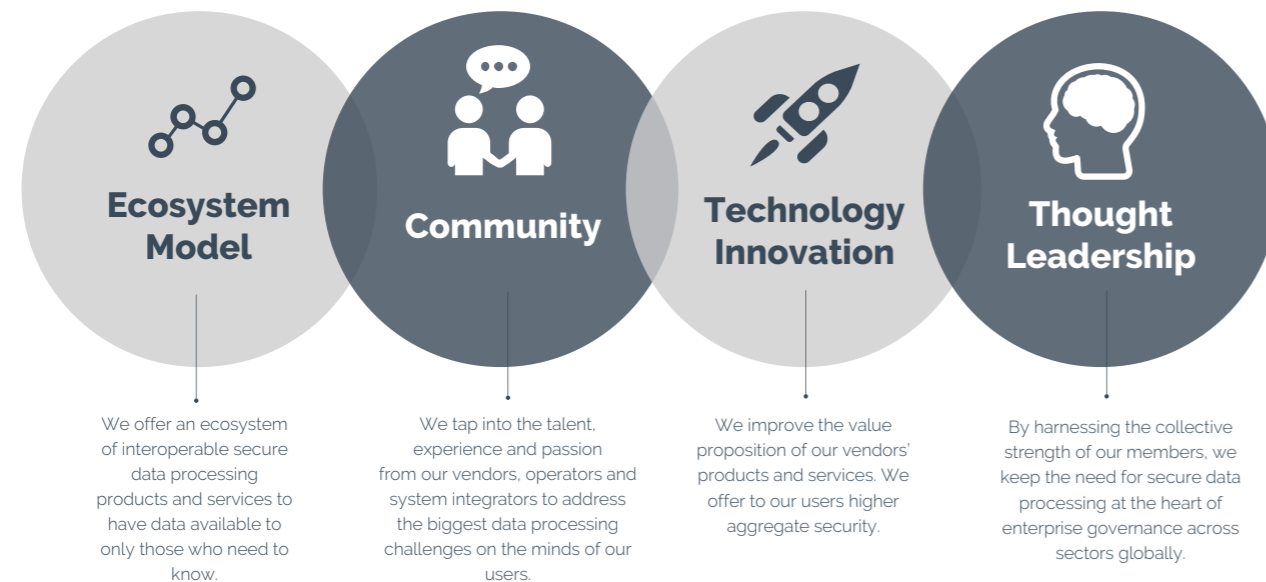
# Contents

1. About Secure Chorus	4
2. Introduction	6
3. An overview of the EU General Data Protection Regulation	8
3.1. GDPR and accountability	9
3.2. GDPR & data security requirements	10
3.3. GDPR & data access requirements	12
3.4. GDPR & record of data processing and notification of data breach	13
4. Secure Chorus: accelerating the path to compliance with GDPR	14
5. Secure Chorus cryptography standards	16
6. Secure Chorus' interoperability standards	17

This document is provided for information purposes only and should not be relied upon as giving advice or as a basis for making any decisions. We do not warrant that this document is error free and shall not be liable for any use of, or reliance upon, this document. No contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

# 1 About Secure Chorus

## An Independent, Not-For-Profit, Membership Organisation



We are a global forum comprising a diverse international membership focused on enabling secure communication products to communicate with each other, based on open standards and collaboration.

Secure Chorus membership is open to the secure communication industry supporting specific open communication and industry cryptography standards to connecting secure communication products through the development of open interoperability standards.

Our members also include enterprise and government users of Secure Chorus Compliant Products. We also welcome observers such as regulators, academic institutions, standards organisations and trade associations interested in contributing to the future of the secure communication industry.

We work together with our vendors to develop interoperability standards for secure communication to meet the requirements of a wide range of use cases. Uniquely, we go beyond the technology and seek to establish a mutually beneficial ecosystem model amongst our community of vendors and users.

### Our user members

Secure Chorus membership enables our user members to tap into the talent, experience and passion of our vendors, to address the biggest secure multimedia communication challenges on their mind. Purchasing Secure Chorus Compliant Products will result in lower costs, increased capability and higher aggregate security for users.

### Our vendor members

Secure Chorus membership enables vendors to form new partnerships and channels for their products, and have access to a larger client base.

### Our telecommunication operator and system integrator members

Secure Chorus membership opens many opportunities to offer enhanced services to facilitate interoperability between enterprises as well as between carriers. Operators and System Integrators also gain insights into key areas of innovation and the state of the art from our innovative start-ups and SMEs.

Secure Chorus' work, based on multi-stakeholder collaboration, has enabled the development of an ecosystem of products, which are all based on a set of open standards which provide specific features that are of great relevance for the transmission of personal data across enterprises. All products provide for end-to-end encryption; however, users are not locked-in by a specific vendor, users of different products can process personal data with one another securely. The technology can be centrally managed, giving the enterprise the ability to comply with any auditing requirements through a managed and logged process. Since the specifications are known and open, it is possible to assess if the technology meets information assurance requirements.



## 2 Introduction

The GDPR will take direct effect in EU Member States on 25 May 2018. Local data protection laws will fill remaining gaps. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The GDPR also applies to organisations outside the EU, whose processing activities relate to personal data of EU 'data subjects' (within the EU).

The GDPR marks a huge increase in regulatory risk. Fines of up to 4% of global annual turnover are expected for a wide range of breaches, akin to what has been seen in anti-trust cases. This means that organisations will need to give privacy compliance a higher priority.

Organisations across industries will need to assess their current approach to data protection, undertaking a gap analysis between that current approach and the requirements under the GDPR, and implementing any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

The standards developed by Secure Chorus enable the development of products which can support secure data processing within the security perimeter of an organisation and beyond, notwithstanding potential worldwide geographical scope.

Large companies organise their data management across different internal systems and interact with a complex external business ecosystem in order to process data.

Secure Chorus is developing standards which respond to a range of requirements under GDPR. Secure Chorus' standards provide for interoperability and end-to-end encryption. These two features combined, enable an organisation to process data securely within its security perimeter and beyond.

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.

In addition, Secure Chorus' KMS (Key Management Server) based approach allows domain managers to easily enable the processing of data between different user groups without bringing external user groups into the security perimeter of the organisation. Secure Chorus' standards use an identity based public key, removing the need for an expensive and complex supporting infrastructure for distributing credentials, allowing for scalable implementation.

Secure Chorus' standards support both real-time processing of data and deferred delivery of data. The standards are also agnostic to implementation and give organisations the complete freedom and flexibility to deploy platforms and infrastructure to meet their requirements.

Since Secure Chorus upholds open industry cryptography standards, it is possible for an organisation – and the regulatory bodies involved in ensuring GDPR compliance – to confirm if the technology meets information assurance requirements.





## 3 An Overview Of The EU General Data Protection Regulation

The GDPR is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private and public-sector organisations, to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally.

The aim of GDPR is to seek to ensure consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union.

Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States of the EU will be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation.

This Regulation also provides a margin of manoeuvre for Member States to specify their rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

The key GDPR requirements can be broadly defined as strengthening and setting out in detail:

- the rights of 'data subjects'
- the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring
- ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

We have outlined in the following pages some core concepts of the GDPR. This list should not be considered exhaustive but it is limited to what we consider relevant from a point of view of how Secure Chorus' standards can support compliance with several aspects of the GDPR.



### 3.1 GDPR And Accountability

The GDPR introduces the principle of accountability which requires the controllers to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR. Controllers are also required to review and update those measures where necessary through internal and external assessment. The measures the controllers ought to implement should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

#### **GDPR, CHAPTER I, "General Provisions", Article 4 "Definitions", sub (7)**

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;...

#### **GDPR, CHAPTER IV, "Controller and processor", Section 1 "General obligations", Article 24, "Responsibility of the controller"**

"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."

## 3.2 GDPR & Data Security Requirements

Data security plays a prominent role in the new General Data Protection Regulation (GDPR) reflecting its symbiotic relationship with cyber security.

The GDPR provides specific suggestions for what kinds of data processing security measures should be considered by organisations processing data:

- pseudonymisation and encryption of personal data;
- ongoing review of the confidentiality, integrity, availability and resilience of processing systems and services.
- introduction of capabilities to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- regular testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of the processing.

### Personal Data

The GDPR has expanded the scope of what constitutes “personal data”. The scope has explicitly been broadened to include any information “relating to” an individual.

#### GDPR, CHAPTER I, “General provisions”, Article 4, “Definitions”

“For the purposes of this Regulation:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

### Processing

The GDPR defines “processing” as anything that is done to, or with, personal data (including simply collecting, transmitting, storing or deleting those data). This definition is significant because it would suggest that GDPR applies wherever an organisation does any activity that involves or affects personal data.

#### GDPR, CHAPTER I, “General provisions”, Article 4, “Definitions”

“‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

### Data Security by design and by default

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance and the implementation of data protection by design and by default.

Data security by design and by default, under GDPR, means that data security becomes a fundamental requirement in the design and maintenance of any information systems and in the mode of operation for an organisation. In addition, the data controller will need to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

The controller however is given the flexibility to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of risks posed by the processing of personal data in the context of an organisation.

#### GDPR, CHAPTER IV, “Controller and processor”, Section 1, “General obligations”, “Data Security by design and by default” Article 25

(1) “...the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects”

(2) “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.”

### Security of Personal Data

The GDPR requires organisations to implement appropriate systems to provide end-to-end security of personal data across data-processing systems and services as well as the capability for the organisation to control the security of the system and perform regular testing of the effectiveness of the technologies used and all relevant business measures.

#### GDPR, CHAPTER IV, “Controller and processor”, Section 2, “Security of personal data”, Article 32, “Security of processing”

1. “...the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. “In assessing the appropriate levels of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”

### Encryption of personal data

The GDPR considers encryption as one of the core techniques to protect personal data.

#### GDPR, CHAPTER IV, “Controller and processor”, Section 2, “Security of personal data”, Article 32, “Security of processing”

“...the controller, and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate:

(a) The pseudonymisation and encryption of personal data;...”

### Lawfulness, Fairness and Transparency

The GDPR requires organisations to process personal data lawfully, and in a fair and transparent manner in relation to the data subject.

#### GDPR, CHAPTER II, Article 5, “Principles relating to processing of personal data”

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

### Data Minimisation

The GDPR recommends minimising the processing of personal data to the necessities of a specific activity.

#### GDPR, CHAPTER II, Article 5, “Principles relating to processing of personal data”

“Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);”

### Integrity and Confidentially

The GDPR requires that personal data is processed with appropriate security measures, including protection from unauthorised or unlawful processing, as well as against cyber-attacks.

#### GDPR, CHAPTER II, Article 5, “Principles relating to processing of personal data”

“(f) Personal data shall be:

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”



### 3.3 GDPR & Data Access Requirements

GDPR provides the data subject with the right to make a data access request regarding the personal data relating to them, that is held by an organisation.

Any organisation which collects personal data has an obligation to give the data subject full access to that data, for whatever reason the individual has decided to make the request.

Therefore, it is important for organisations to look at data processing security solutions which simultaneously provide for end-to-end encryption as well as handle requests to access requests, restrictions, rectification and erasure of personal data.

#### Transparency and Modalities

The GDPR requires Controllers to provide the data subject with any information relating to the processing of personal data of the data subject.

**GDPR, Chapter III, “Rights of the Data Subjects”, Section 1 “Transparency and Modalities”, Art 12 “Transparent information, communication and modalities for the exercise of the rights of the data subject”**

*“1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.”*

#### Right of access by the data subject

The GDPR gives the right to the data subject to request access to their personal data.

**GDPR, Chapter III, “Rights of the Data Subjects”, Section 2 “Information and access to personal data”, Art 13 “Right of access by the data subject”**

*“1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:”*

#### Right to rectification

The GDPR gives the right to the data subject to request rectification of their personal data.

**GDPR, Chapter III, “Rights of the Data Subjects “Section 3 “Rectification and erasure”, Article 16 “Right to rectification”**

*“The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.”*

#### Right to be forgotten

The GDPR gives the right to the data subject to request erasure of their personal data.

**GDPR, Chapter III, “Rights of the Data Subjects “Section 3 “Rectification and erasure Article 17 Right to erasure (‘right to be forgotten’)**

*“1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: ...”*



### 3.4 GDPR & Record of Data Processing & Notification of Data Breach

#### Records of processing activities

The GDPR requires maintaining a record of processing activities and provides a detailed list of the type of information to be recorded.

**GDPR CHAPTER IV, “Controller and processor”, Section 1 “General obligations” Art 30, “Records of processing activities”**

*“Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:...”*

#### Notification of a personal data breach to the supervisory authority

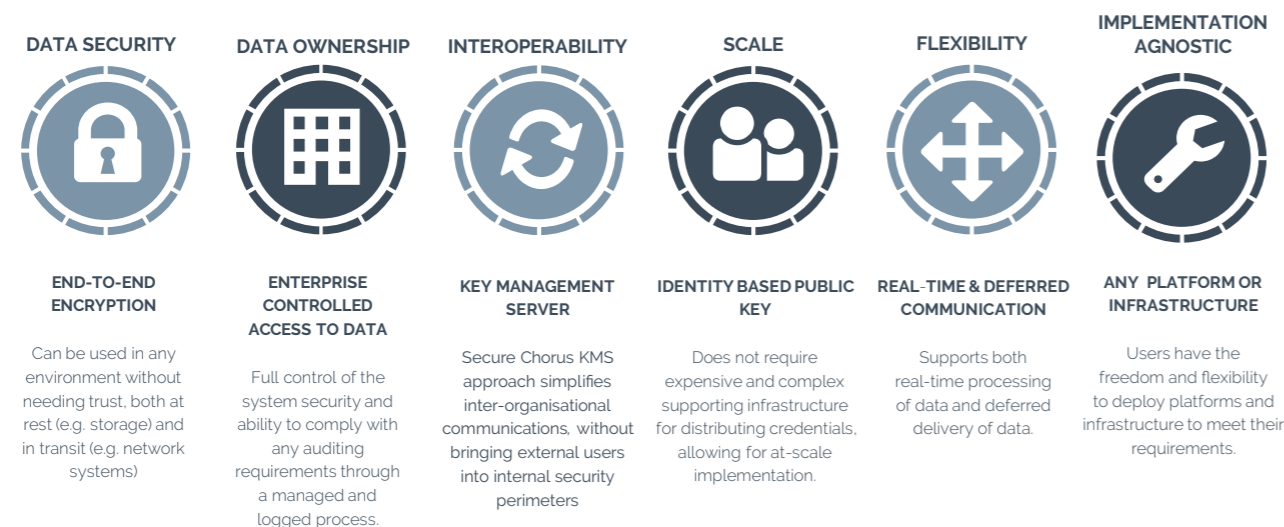
The GDPR mandates timely notifications in case of a breach.

**GDPR, CHAPTER IV, “Controller and processor”, Section 2 “Security of personal data”, Art 33 “Notification of a personal data breach to the supervisory authority”**

*“1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”*

# 4 Secure Chorus: Accelerating the Path To Compliance With GDPR

## Secure Chorus Compliant Products



The GDPR has a direct impact on organisations’ governance, systems and technologies in the private and public sector, in how they securely process personal data within the security perimeter of their organisation and beyond.

These changes will influence the choices organisations make when selecting cyber security solutions for the protection of personal data processing.

One challenge with GDPR is that there is no overarching standard. As such, businesses are challenged to define current compliance levels and come to conclusions themselves about the best way to achieve compliance.

As previously highlighted, personal data processing includes a broad set of activities (“processing”) performed by organisations and any third-party services providers which may process personal data on their behalf.

Under GDPR, Art 4 “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

It is clear therefore that as the meaning of “processing” includes the entire personal data lifecycle, a new model is required for the protection of data during any type of processing, whether such processing occurs within the security perimeters of an organisation or beyond.

This change in regulation raises questions on how an organisation can securely process personal data – its collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction – considering the involvement of a variety of actors such as the data subject and an organisation’s third-party services providers.

In a closed environment such as the security perimeter of an organisation, securing data may be less complex. In the interconnected environment which includes actors outside the security perimeters of an organisation, however, there are issues of interoperability, discovery, trusted cloud-based services, and routing, all of which are cemented by the need to ensure the actors processing the data are those who are authorised to do so.

Secure Chorus effectively address the challenges organisations are facing with personal data processing under GDPR in these complex multi-actor environments, by offering a new business model which is based on industry collaboration and open industry standards to enable secure data processing technologies to interoperate with each other.

This is important as it allows an organisation to process personal data within the security perimeter of the organisation and beyond, so long as all actors use Secure Chorus Compliant Products.

In addition, Secure Chorus’ KMS (Key Management Server) based approach allows domain managers to easily enable secure data processing between different user groups without bringing external users into the security perimeter of their organisation.

Secure Chorus Compliant Products can interoperate as they all use, at their core, the same open cryptography standard, which has been developed by the UK government’s National Technical Authority for Information and Assurance (CESG) - now the National Cyber Security Centre (NCSC) - and adopted by the wider global industry at 3GPP for relevant user cases such as emergency services.

GDPR regulation requires data security by design and by default, which means that data security becomes a fundamental requirement in the design and maintenance of information systems. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. The open cryptography standard used by Secure Chorus provides for end-to-end encryption, which enable all actors using compliant products to process personal data in any environment without needing trust in the environment, both at rest (e.g. storage) and in transit (e.g. network systems).

Since the specifications of the standards are known and open, it is possible for anyone to assess that the technology meets the desired security requirements. As such, vendors providing products compliant to the standards can help organisations overcome the challenge of defining current compliance levels from a cyber security perspective. The organisations using these products

can be confident that the technologies they adopted to protect data processing in their organisations are based open industry standards which are proven and tested.

There are other interesting aspects to Secure Chorus’ standards which allow the organisation to have full control on their security system. Products based on the standards can be centrally managed, giving an organisation the ability to comply with the GDPR clauses which gives the data subject the right to request the organisation that is processing his/her personal data to access, restrict, rectify and erase his/her personal data and this through a managed and logged process.

The GDPR also requires that an organisation record any processing of personal data, as well as notify the supervisory authority of any data breach, in certain circumstances. Security technologies that have a robust and clear approach to auditability and data access are key to fulfilling these requirements.

Secure Chorus’ standards support the use of identity-based public key cryptography, avoiding the need for any expensive and complex supporting infrastructure for distributing credentials, allowing for at-scale implementation.

The use of this keying method makes it easy and cost-effective to ensure keys are only distributed to the individuals who lawfully have access to the data, and avoids excessive costs in upgrading legacy systems to achieve compliance with GDPR across an organisation.



## 5 Secure Chorus' Cryptography Standards

The underpinning technologies behind Secure Chorus are at the cutting-edge of modern cryptographic standards. These standards are used in Secure Chorus for two primary purposes: ensuring that two parties exchanging data, whether persons or machines, are doing so with the individual or the machine they believe they are exchanging data with (authentication of identity) and ensuring no unauthorized person or machine can access the content of any data exchange (end-to-end encryption).

### 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 a standard to answer the security requirements from government to have a cryptographic method for validating an identity for government communications.

This standard 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, SAKAI and KASAHARA. Using these protocols for secure communications gave rise to MIKEY-SAKKE, defined by the IETF as RFC 6507 [1] and RFC 6509 [2].

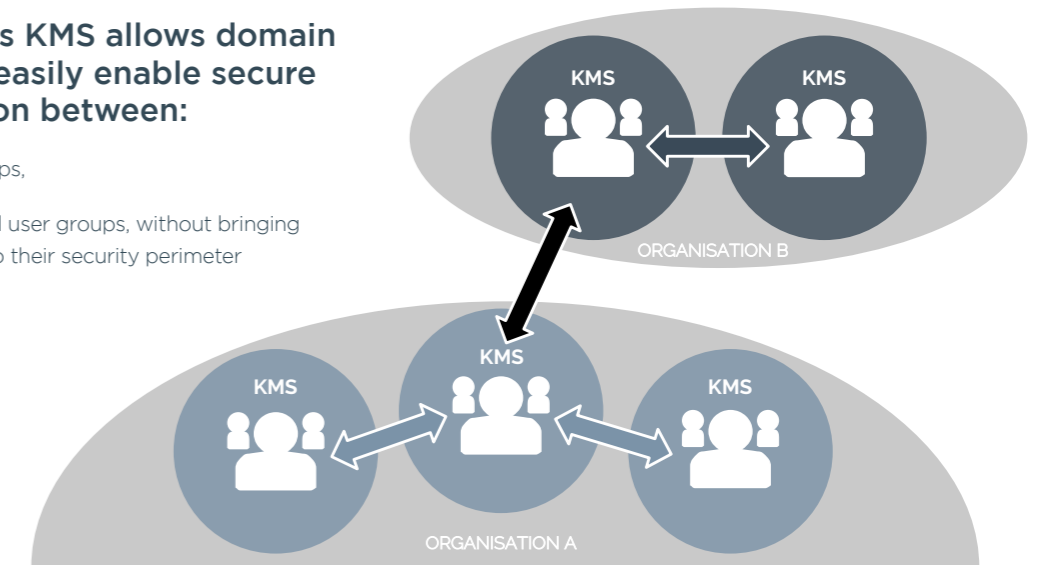
MIKEY-SAKKE builds upon a range of existing security technologies. It specifies the use of the widespread Secure Real-time Protocol (SRTP) [3] to securely transmit multimedia data. This is specifically used with the widespread Advanced Encryption Standard - 128 bit (AES-128) as defined by NIST FIPS 197 [4] in the Galois Counter Mode (AES/GCM) cipher mode of operation, as defined by NIST SP 800-38D [4].

MIKEY-SAKKE has been approved by 3GPP for use in Mission-Critical applications, such as emergency services communications [5]. 3GPP is the collaboration project which provides system specifications for cellular telecommunications network technologies.

More information on how MIKEY-SAKKE was developed by NCSC and the use-cases for the cryptographic technology can be found on the NCSC's website [6].

Secure Chorus KMS allows domain managers to easily enable secure communication between:

- 1 internal user groups,
- 2 internal & external user groups, without bringing external users into their security perimeter



### Key Management Servers

The system used in MIKEY-SAKKE means 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. Unlike other closed secure communication systems, the approach in Secure Chorus is specifically adapted for enterprise.

The existence of the KMS means that an organisation has control over its own security system, without having to give access to their data to unauthorised third parties. As an organisation's data becomes increasingly valuable and sensitive in today's world, an organisation's control over its own security system is critically important. With this control, different activities can be performed by the organisation such as data analytics, monitoring of cyber incidents and auditing activities. All while ensuring compliance with the relevant regulatory frameworks applicable to the organisation's sector.

The Key Management Server can be managed entirely by an organisation's own IT team. And it may be kept offline for maximal security. Ultimately, thanks to the properties of MIKEY-SAKKE, the organisation retains full control over their security system, and only those explicitly authorised by an organisation can access that organisation's data.

With a KMS approach, there is no need for complex key-exchange or handshaking between the originator and consumers of data. Instead a short packet of data ("I\_MESSAGE") is sent from the originator to the consumers, which encapsulates all the information required to decrypt a data stream or message, and a signature from the originator. Both parties can then be mutually authenticated following the processing of this single I\_MESSAGE, without the need for a return path from the consumer back to the originator. The overhead on the data channel is minimal to none, depending on the protocol used at the application layer. This high data-efficiency also makes the standard very attractive for IoT purposes.

A walkthrough on how the MIKEY-SAKKE and the KMS works, how keys are managed, and how the technology can be used to build secure multimedia services for data processing can be found on the NCSC's website [7].

## 6 Secure Chorus' Interoperability Standards

Secure Chorus develops standards which enable interoperable secure digital data processing between Secure Chorus Compliant Products.

Secure Chorus' interoperability standards build upon a foundation of a number of existing and industry-wide adopted standards not only in the field of cryptography – but also leveraging other existing telecommunication standards. Secure Chorus contains MIKEY-SAKKE as the encryption algorithm at its core, but defines other protocols and codecs which Secure Chorus products must support.

As a first step to make their secure communication products interoperable with one-another, Secure Chorus' members need to adopt these specific standards into their products.

Although Secure Chorus' approach can extend to all types of digital data, the foundation of Secure Chorus' interoperability standards specifically addresses and resolves the problem of achieving interoperability of two secure voice products, with the aim of achieving a seamless secure phone call. The NCSC's website [8] highlights how solutions with MIKEY-SAKKE at their core can address the evolving risks of communications, and further address the benefit of interoperability for products using Secure Chorus' standards.

The Secure Chorus standards specify a profile of the Session Initialisation Protocol (SIP) for supporting the communication between systems. SIP is a common Voice over IP (VoIP) protocol standardised by the IETF [9].

Secure Chorus' technology roadmap is developed by consensus amongst its members, generating a multi-layered time-based chart that enables the technology development to be aligned with market trends and drivers.

Current areas of collaboration include extending the VoIP standards beyond one-to-one communication to group calls, instant messaging, video calls, voicemail, document sharing and machine-to-machine communications. We are also studying other areas of innovation – we intend to develop post-quantum capability into Secure Chorus with a Post Quantum Identity Based Crypto Scheme. We will be seeking input from industry, academia and government to identify the right solution to address this critical challenge.

### Secure Chorus Open Standards

Our members collaborate to develop open INTEROPERABILITY STANDARDS that will allow their products to interoperate.



### Industry Open Standards

Based upon COMMUNICATION and CRYPTOGRAPHY STANDARDS documented by international standards bodies (IETF and 3GPP).

An open-source code library is available.

## References

- [1] IETF, "RFC 6507 - Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)," February 2012 [Online]. Available: <https://tools.ietf.org/html/rfc6507>.
- [2] IETF, "RFC 6509 - MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)," February 2012. [Online]. Available: <https://tools.ietf.org/html/rfc6509>.
- [3] IETF, "RFC 3711 - The Secure Real-time Transport Protocol (SRTP)," Mar 2004. [Online]. Available: <https://tools.ietf.org/html/rfc3711>.
- [4] NIST, "Information Technology Library," [Online]. Available: <https://www.nist.gov/itl>.
- [5] 3GPP, "Specification #: 22.179," 22 Sep 2017. [Online]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623>.
- [6] NCSC, "The development of MIKEY-SAKKE," 26 Jan 2016. [Online]. Available: <https://www.ncsc.gov.uk/articles/development-mikey-sakke>.
- [7] NCSC, "Using MIKEY-SAKKE: Building secure multimedia services," 28 Sep 2016. [Online]. Available: <https://www.ncsc.gov.uk/articles/using-mikey-sakke-building-secure-multimedia-services>.
- [8] NCSC, "Secure Voice at OFFICIAL," 8 Aug 2016. [Online]. Available: <https://www.ncsc.gov.uk/guidance/secure-voice-official>.
- [9] IETF, "RFC 3261 - SIP: Session Initiation Protocol," Jun 2002. [Online]. Available: <https://tools.ietf.org/html/rfc3261>.



# secure chorus

## CONTACT DETAILS:

One Canada Square,  
Canary Wharf,  
London E14 5AB

General Inquiries: [info@securechorus.org](mailto:info@securechorus.org)

Membership Inquiries: [membership@securechorus.org](mailto:membership@securechorus.org)

[www.securechorus.org](http://www.securechorus.org)



Secure Chorus Ltd, a not-for-profit private company limited by guarantee, under The Companies Act 2006 and the situation of its registered office is in England and Wales.

Copyright © Secure Chorus Limited 2017 - Present. All Rights Reserved.