## Contents

1. Chairman’s Statement  
2. Annual Report FY 2017-2018  
3. Outlook for FY 2018-2019  
4. Description of Business  

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Chairman’s Statement</td>
<td>4</td>
</tr>
<tr>
<td>3. Outlook for FY 2018-2019</td>
<td>10</td>
</tr>
<tr>
<td>4. Description of Business</td>
<td>14</td>
</tr>
</tbody>
</table>
Chairman’s Statement
Chairman’s Statement

Secure Chorus is a not-for-profit membership organisation, operating at the nexus of public and private sectors, providing thought leadership and developing open standards for the long-term security of our global digitally-enabled economy.

With the ever-growing magnitude and complexity of our global digital economy, organisations are confronted by a much larger and increasingly multi-faceted security picture. Our vision is to provide a platform for public-private sector collaboration, to understand the challenges experienced by organisations across private and public sectors in the field of data protection and work with the cyber security industry to share knowledge, develop forward-looking strategies and innovative capabilities based on open technology standards.

We firmly believe that in order to effectively address data protection challenges, we must shift from providing capabilities that foster “islands” of secure communication to providing an ecosystem of interoperable capabilities to “build bridges”.

Moreover, we have realised that for organisations across sectors to be able to innovate and realize their digital potential it is important to develop security models that enable organisations to operate securely without losing agility and dynamism, and such security solutions must be affordable and easy to implement.

This is especially timely, as a number of proprietary standards have made their way into commercial products for enterprise. However, most of these proprietary standards only allow for the establishment of ‘islands’ of secure communication, where proprietary lock-in makes users dependent on a specific vendor and – unless they both use the same product – prevents two users from sharing information securely.

FY 2017-2018 has been a strong year of strategic execution for Secure Chorus, designing and rolling out our operating model. The operating model build-up phase of our 2-year programme is now complete. We have transitioned from a working group which was originally set up in 2012 into a stand-alone not-for-profit membership organisation providing a platform for increased global multi-stakeholder cooperation.

We have brought together inspiring organisations across the globe, including governments, supranational organisations and private organisations, from large established global enterprises through to innovative smaller technology start-ups, academic institutions and trade organisations. This is allowing us to rapidly scale our ecosystem of interoperable and secure information sharing technologies, services and infrastructure - and drive wide-spread access and adoption across the global digital economy.

It is satisfying that many of our achievements are the direct outcome of the collaborative efforts between the public and private sector over the course of the last 2 years, to establish Secure Chorus as a global community of thought leaders who believe passionately in the power of multi-stakeholder engagement and open standards to address the secure communication challenges of our global digital economy.

In particular, Secure Chorus has made great progress as an enabler of strategic conversations through the development of a Thought Leadership Platform. Such has been the interest in our Thought Leadership Platform, that over the past 12 months Secure Chorus has been invited to be part of strategic conversations with several important stakeholders including the UK National Cyber Security Centre, NATO, the European Council, Security Committee for Information Assurance, the Centre for Secure Information Technology Belfast, and the European Telecommunication Standards Institute and the Civil Aviation Authority.
In FY 2017-2018 we also launched several technology initiatives including the development of infrastructure and services to enable the successful development and testing of Secure Chorus Compliant Products and the development of a Hub infrastructure that will facilitate new user groups’ communication with existing users of Secure Chorus Compliant Products.

Another important initiative that was launched in FY 2017-2018 is the development of a Post-Quantum Identity Based Crypto Scheme to update Secure Chorus’ current cryptography standard of choice. The growth of quantum computer technology poses a threat to current cryptography algorithms. As the threat grows, the fundamental cryptography standards chosen by Secure Chorus will likely need to be updated to respond to the growing quantum computing threat.

Each one of these initiatives is an ambitious effort to contribute to the development of a safer global digital economy by building a global ecosystem of secure and interoperable technologies and services for enterprise.

I am proud to report that thanks to our unique approach, based on private and public-sector collaboration and open standards and our entrepreneurial outlook, we were able to attract many inspiring organisations across the globe which joined us to support our mission.

In FY 2017-2018 we welcomed on board the UK National Cyber Security Centre as our first government member, several major global telecommunication operators including Vodafone and O2, as well as a number of multinational defence, security, and aerospace organisations such as BAE Systems, Leonardo and Sepura.

We pride ourselves on being a start-up friendly organisation as membership for companies under £2M revenues is subscription fee free. We are very pleased that several nimble and dynamic technology companies including post-quantum cryptography leaders such as ISARA Corporation and ground-breaking secure communication software companies such as Cryptify, Armour Communications, SQR Systems, Galaxkey, and Serbus have joined us.

We also welcomed our first observers - two centres of academic excellence in the field of cyber security - CSIT and UCL as well as an important industry body, techUK.

Our Board of Directors is equipped with the skills and past performance to grow our organisation and lead our initiatives to meet the secure communication challenges of our global digital economy. More than that, our members and observers around the world are as committed as we are to work together to contribute to our Thought Leadership Platform as well as to develop cutting-edge innovation in the field of secure communication for enterprise.

Secure Chorus is well positioned for the future, and we will continue to support organisations across sectors and industries with their secure communication challenges through our Thought Leadership Platform. At the same time, we will continue to work on technology-focused initiatives in both technologies and services, democratising the market and ensuring our global digital economy will become a safe place to do business.

Elisabetta Zaccaria
Chairman
Annual Report FY 2017-2018
Secure Chorus FY April 1st, 2017 – March 31st, 2018 was marked by many exceptional milestones, from the transformation of Secure Chorus into a stand-alone not-for-profit membership organisation, to welcoming on board many inspiring organisations across the globe as members and observers, to launching several important initiatives.

The outcomes presented in this report are the result of our vision to create an organisation that serves as a platform for public-private sector collaboration, and to also provide education for the development of capabilities to solve the most challenging secure communication problems in our ever evolving and complex global digital economy.

The not-for-profit nature of our organisation coupled with our work through the Thought Leadership and Education & Training Platforms as well as our diverse range of technology-focused initiatives, have been the underlying force for developing Secure Chorus into an engine of innovation, addressing secure communication for our global digital economy.

Our strategy included 3 main pillars:

**Launch of our Thought Leadership Platform to foster public-private collaboration and the sharing of free knowledge in the field of secure communication, to increase awareness and offer thought leadership to enterprise**

In FY 2017-2018, we launched our Thought Leadership Platform, in collaboration with our members, to provide an environment for sharing free knowledge with the marketplace, in the field of secure communications.

This initiative had the goal of increasing awareness and understanding among business leader across the public and private sectors globally of the importance of protecting data and how to best address this challenge in practice.

We are proud to report that in FY 2017-2018, our Thought Leadership Platform advised supranational organisations, government and private industry across sectors on their secure communication challenges. This is thanks to the support provided by our member organisations which actively participated by sharing free knowledge.

**Development of interoperability standards based on our cryptography standard of choice to enable the industry to develop an ecosystem of Secure Chorus Compliant Products**

Prior to 2017 we developed two “Foundation Release” standards documents: the KMS Certificate Definition standard, and the One-to-One Communications standard. These documents provided guidelines for vendors of secure voice call solutions allowing them to build an interoperable product. This means end-users of their products can have one-to-one calls with end-users of any other Secure Chorus-Compliant Product.

In FY 2017-2018, we worked with our members to update our existing standards to include the missing components of the existing One-to-One Communications standard and the KMS Certificate standard. We also initiated conversation on standardising discovery and Hub technologies and developed our first draft for the Hub standard and discovery protocol.
Development of the infrastructure and services to support Secure Chorus Compliant Products

In FY 2017-2018 we kicked-off several technology-focused initiatives that will facilitate the global roll-out of Secure Chorus Compliant Products including the development of infrastructure and services to enable the successful development and testing of Secure Chorus Compliant Products as well as the development of a Hub infrastructure for Secure Chorus Compliant Products.

The Hub infrastructure will ensure new user groups can reach existing users of Secure Chorus Compliant Products with minimal setup or configuration, facilitating the growth of a truly global interoperability ecosystem where the opportunity for any user to reach any other user is not only possible, but easily enabled.
Outlook for FY 2018-2019
Outlook for FY 2018-2019

It is our view that in FY 2018-2019 cyber security and data security and privacy issues will continue to grow in significance across the public and private sectors globally. This growth will be driven by:

1. an unprecedented digitalisation across sectors;
2. an increasing need for data to be disseminated beyond the perimeter of an organisation;
3. an ever-increasing number of high profile data breaches reported that is leading organisations to be concerned about how data is managed; and
4. a strengthening of cyber security regulation and the implementation of the new EU General Data Protection Regulation (GDPR), a landmark moment in data protection.

We believe therefore that FY 2018-2019 will be a turning point for our organisation to become a world class thought leader in the in the field of data security as well as provide tangible capabilities to address the challenge of our global digital economy by providing an ecosystem of Secure Chorus Compliant Products, along with supporting infrastructure and services.

The Company’s strategy for FY 2018-2019 leverages the experience, access and influence built in FY 2017-2018. We will continue to deliver thought leadership and tangible capabilities through a diverse set of initiatives to make the global digital economy a safe and dynamic place.

Our effort will continue to focus on bringing together governments, supranational organisations, corporates, technology innovators, academic institutions and regulators who share our vision for data protection based on multistakeholder collaboration and open standards. We look to get all parties sitting at the same table to rapidly scale our ecosystem of interoperable and secure information sharing technologies, providing wide-spread access and achieving adoption across the global digital economy.

Secure Chorus’ FY 2018-2019 strategic focus areas:

1. Thought Leadership Platform
2. Education & Training Platform
3. Technology Capabilities
   a. Development of interoperability standards based on Secure Chorus’ cryptography standard of choice
   b. Development of infrastructure and services to support vendors and users of Secure Chorus Compliant Products, including:
      i. Infrastructure and services to enable the development of Secure Chorus Compliant Products;
      ii. Infrastructure and services to test Secure Chorus Compliant Products; and
      iii. Roll-out and management of a Hub infrastructure for vendors and users of Secure Chorus Compliant Products
   c. Development of Secure Chorus’ Post Quantum Identity-based Crypto Scheme
1. Thought Leadership Platform

We launched our Thought Leadership Platform in November 2017. In FY 2018-2019 we want to continue our work by focusing on three main objectives: a) Foster public-private sector collaboration to influence strategic conversations and act as a sounding board on policy making on the subject matter of data protection; b) Raise awareness among leaders across the public and private sector about data protection and, where they don’t have a data protection strategy, give them a dynamic and inspiring platform to meet with our members who are expert in this field, providing them the opportunity to learn and helping them to make strong strategic choices; and c) Promote our business model for data protection which is based on industry collaboration and open standards.

2. Education & Training Platform

In FY 2018-2019 we will launch our Education & Training Platform to enable our members to provide education in the field of data protection policy and regulation.

We will also launch a specific initiative focused on educating our vendor members on post-quantum cryptography.

The new emerging quantum technologies will require a next generation of data protection capabilities. In an effort to accelerate the development of the required post-quantum cryptography we have acknowledged the importance of education of our members in post-quantum cryptography.

3. Technology Capabilities

a. Development of interoperability standards based on Secure Chorus’ cryptography standard of choice

In FY 2018-2019 we will expand interoperable communications beyond one-to-one voice calls. Instant messaging, video calls, group calls, document sharing, voicemail and machine-to-machine secure communications are all candidates for the development of Secure Chorus standards.

b. Development of infrastructure and services to support vendors and users of Secure Chorus Compliant Products

i. Infrastructure and services to enable the development of Secure Chorus Compliant Products

In FY 2018 - 2019, we will undertake activities to ensure our members can easily and quickly develop Secure Chorus Compliant Products and can do so with confidence that their products will interoperate with the entire ecosystem.

We will develop an open-source reference codebase according to Secure Chorus’ standards with the aim of achieving a world-class reference codebase. We will facilitate the maintenance of the codebase and its usage, to better understand how the Company can support its members in deploying Secure Chorus Compliant Products in the marketplace.
We will investigate opportunities to develop and provide a Secure Chorus Hub software codebase, fostering a market of Hubs. We will maintain and monitor the usage of the codebase to ensure Secure Chorus can support the further development of the Hub marketplace.

**ii. Infrastructure and services to test Secure Chorus Compliant Products**

In FY 2018-2019, we will develop a Secure Chorus Compliant Product certification model for our members. This will include the setup and management of a testing infrastructure for our members. This infrastructure will ensure our members are able to test the interoperability of their products in an agile and practical manner.

**iii. Roll-out and management of a Hub infrastructure for vendors and users of Secure Chorus Compliant Products**

In FY 2018-2019, we will roll-out an infrastructure that will enable new users of Secure Chorus Compliant Products to quickly and cost-effectively enable their deployments to join the ecosystem. As part of the service we will also create a Secure Chorus certificate exchange platform.

We will capture the requirements from the user community to ensure the platforms are built to address current user requirements and engage the appropriate external support to ensure these platforms can be developed, launched and managed in a cost-effective and reliable way.

c. **Development of Secure Chorus’ Post-Quantum Identity-based Crypto Scheme**

The growth of quantum computer technology poses a threat to current cryptography algorithms. As the threat grows, the fundamental cryptography standards chosen by Secure Chorus will likely need to be updated to respond to the growing quantum computing threat. In FY 2018 - 2019 we will analyse the post-quantum challenges in secure communications and will work with our members and field experts alike to identify a long-term strategy for updating the standards to ensure the use of cryptography that is resilient to attack by quantum computing.
4 Description of Business
4 Description of Business

NOTE: The classes, eligibility criteria and rights of members are specified in detail in the Articles of Association and Membership Application Form of the Company. This section aims to offer a high-level overview only.

Company Ownership/Legal Entity

Not-for-profit Company Limited by Guarantee

Secure Chorus Ltd was incorporated on the 8th of September 2016, as 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.

The Company has developed bespoke Articles of Association and a Membership Application Form. These documents outline in full the legal framework of the company.

Members

Classes of Membership are as follows:

1. Launch Member
2. Government Member
3. Partner Member
4. Associate Member

Launch Member

Membership Criteria

The Launch Member status is limited to two companies incorporated under the Company’s Act 2006: Cyber Y Ltd and Roderick Hodgson Ltd.

Government Member

Membership Criteria

The Board of Directors of the Company may admit application for Government Membership, which is open to any supranational organization or national government able to:

I. have a 500 or more-user base utilising a Secure Chorus Compliant Product, service or infrastructure; or
II. provide assistance in the establishment and development an eco-system to support Secure Chorus Compliant Products enabling them to be sustainable and trusted by the market, such assistance may include:
   a. advice on the technical content of the Standards; and
   b. Standards authorship and development;
Partner Member

Membership Criteria

The Board of Directors of the Company may admit applications for Partner Membership, which is open to any company incorporated under the Companies Acts or any other body corporate which at the time of its application is

I. offering Secure Chorus Compliant Products, services and/or infrastructure; or
II. developing, manufacturing or selling Secure Chorus Compliant Products; or
III. having a 500 or more user base utilising a Secure Chorus Compliant Product, service or infrastructure; or
IV. providing assistance in the establishment and development an eco-system to support Secure Chorus Compliant Products enabling them to be sustainable and trusted by the market, such assistance may include:
   a. advice on the technical content of the Standards;
   b. Standards authorship and development;
   c. Client and gateway review services, including accreditation; or
   d. Inter-operability testing and measurement.

Associate Member

Membership Criteria

The Board of Directors of the Company may admit applications for Associate Membership, a company incorporated under the Companies Acts or any other body corporate that meets the following criteria:

I. committed to developing Secure Chorus Compliant Products, services and/or infrastructure within an Agreed Period; or
II. committed to developing, manufacturing or selling products related to Secure Chorus Compliant Products within an Agreed Period;
III. or committed to developing a 500 or more user base of a Secure Chorus Compliant Product, service or infrastructure within an Agreed Period;

Observer

Observer Criteria

The Board of Directors of the Company may admit applications for Observer: regulators, academic institutions, standards organisations or trade associations that are committed to assisting and/or promoting the Company within a period of 12 months.
Corporate Governance

The Company's corporate governance is aimed at facilitating effective, entrepreneurial and prudent management that can deliver the long-term success of the Company.

Corporate Governance Structure

The Company's corporate governance is structured as follows:

1. Board of Directors
2. Committees
   - Governments Committee
   - Corporates Committee
   - SMEs Committee
   - MEs Committee
   - Standards Committee
3. Advisory Groups
   - Regulatory Compliance Advisory Group

Board of Directors

The Company's Board of Directors has a strong presence of both executive and non-executive directors with the appropriate balance of skills, experience, independence and knowledge of the company to enable it to discharge its duties and responsibilities effectively.

The maximum number and minimum number respectively of the directors may be determined from time to time by Ordinary Resolution. Subject to and in default of any such determination the number of directors shall be no less than 2 throughout the Launch Period and no less than 3 following the Launch Period.

Committees

The Company has five membership committees, namely the Governments Committee, Corporates Committee, SMEs Committee, MEs Committee and the Standards Committee.

Each Membership Committee, except for the Governments Committee has the right to appoint its chairperson to the Board of the Company as non-executive director, after the Launch Period.

Governments Committee - means the membership committee consisting of Government Members which are either a supranational organisation or national government. The Company’s Board of Directors shall be entitled to be a member of the Government Committee.

Corporates Committee - means the membership committee consisting of Partner Members which are body corporates with a turnover of more than £50 million per financial year. The Company’s Board of Directors shall be entitled to be a member of the Corporates Committee.
**SMEs Committee** - means the small and medium enterprise membership committee consisting of Partner Members which are body corporates with a turnover of less than £50 million but more than £2 million per financial year. The Company’s Board of Directors shall be entitled to be a member of the SMEs Committee.

**MEs Committee** - means the microenterprises membership committee consisting of Partner Members which are body corporates with a turnover of less than £2 million per financial year. The Company’s Board of Directors shall be entitled to be a member of the MEs Committee.

**Standards Committee** - means the membership committee appointed in accordance with the Articles to advise the Board on the standards to be approved by the Board and issued by the Company from time to time. The Company’s Board of Directors, the Government Members and Partner Members shall be entitled to be members of the Standards Committee.

**Advisory Groups**

The Board can appoint other advisory groups to provide recommendations, guidance and advice to the Board on specific matters.
Board of Directors

Elisabetta Zaccaria, Chairman & Launch Director

Ms Zaccaria has oversight of the strategic direction, expansion and operation of Secure Chorus.

Elisabetta has over a decade of experience in the cyber security, risk management, information technology and communications sectors. She has been a Founder/CEO or C-level executive of several successful companies in the UK, US, MENA and APAC. She has achieved significant growth and returns for investors, by starting up or building businesses.

In 2015, she founded cyberY Ltd, a firm specialised in designing ecosystems to foster innovation in the cyber security sector. In February 2016, cyberY started a major ecosystem project, Secure Chorus.

cyberY was brought onto the project to grow Secure Chorus’ innovation capacity, sustainability and velocity. Secure Chorus Ltd was incorporated in September 2016 as a not-for-profit, membership organisation. cyberY is a co-founder of Secure Chorus Ltd and Elisabetta has taken on the roles of Chairman and Launch Director for a 2-year launch period of this project.

Prior to that Elisabetta was the Group Chief Strategy Officer & Chief Operating Officer of Global Strategies Group. She built the British stand-alone start-up into an international company, providing cyber security, systems development and integration, data management and analysis, reaching $600million in revenues in only 6 years. She left in 2012 after a career with the company and its predecessor organisations spanning nearly 9 years and including several acquisitions, an IPO (Nasdaq) and an exit to a private equity house. She also held various board director positions in several UK, US and EU companies.

Since 2012, Elisabetta has also been committed to volunteering her time, providing expert advice as Entrepreneur Mentor in Residence at London Business School, as well as through a number of technology accelerator and incubators programmes including CyLon and UCL Advances.

Elisabetta is a LBS alumnus, as well as receiving a Master Doctor of Law from Universita’ Degli Studii di Ferrara and an MA in International Relations from Hult International Business School. A keen linguist, she speaks English, Italian, Serbo-Croatian, Slovene, German and Spanish.

Roderick Hodgson, Launch Director

Mr Hodgson has oversight of the technical aspects of Secure Chorus including technical management, setting the technical strategy and representing the technology externally.

Mr Hodgson is a technologist, innovation strategist, and full-stack developer. Throughout his career he has defined, developed and delivered disruptive products in Video Streaming, Telecoms, Cyber Security, IoT and Big Data for different companies.

In 2016, he founded Roderick Hodgson Ltd, a consultancy firm specialised in assisting new companies in defining and developing their technology offering. In August 2016, Roderick Hodgson Ltd started a major ecosystem project, Secure Chorus.
Roderick Hodgson Ltd was brought onto the project to provide technical expert knowledge and to lead Secure Chorus’ technology roadmap. Roderick Hodgson Ltd is a co-founder of Secure Chorus Ltd and Roderick has taken on the roles of Launch Director for a 2-year launch period of this project.

Prior to setting up Roderick Hodgson Ltd, he served in several senior R&D roles where he worked on global research projects in the areas of video technology, broadcasting, and artificial intelligence, for companies including BBC R&D, SQR Systems Ltd and Toptal LLC. He has co-authored several papers and patents in the fields of broadcasting and artificial intelligence, spoken at conferences on IoT and secure communications, and contributed to a number of international standardisation efforts in both broadcasting and communications. In his spare time, he offers mentoring to ambitious technology start-ups.

Mr Hodgson has a B.Sc. (Hons.) in Artificial Intelligence and Computer Science from the University of Edinburgh. He speaks English and French.
Standards Committee

Elisabetta Zaccaria, Secure Chorus

Dr Andy Lilly, Armour Communications & Chair Standards Committee

Andy is the Co-Founder and CTO of Armour Communications, with a record of delivering challenging, leading-edge R&D solutions into global markets. Having lead high tech teams at both multi-national organisations and VC-funded start-ups, Andy has been instrumental in delivering secure communications systems and solutions into military, government and enterprise environments for nearly 30 years. Andy holds a PhD in radar modelling from UCL and a B.Eng. Hons. from the University of Surrey.

Mark Baggs, Telefonica

Mark is the Head of Recording for Telefonica O2. He is responsible for industrialising mobile recording within Telefonica’s O2 Business and the roll-out of other complimentary solutions such as conferencing (Just call Me and All Hands), secure voice, analytics, speech to text and integrating fixed solutions for our unified voice strategy. Prior to O2, Mark worked in Banking as an Associate Director for Royal Bank of Canada Capital Markets and Morgan Stanley running Infrastructure Services.

Dr Faith Bateman, BAE Systems Applied Intelligence

Faith is an Account Manager within the Defence Division of BAE Systems Applied Intelligence with a history in the defence and cyber security sectors. Faith has previously worked on number of projects involving advanced mobility, in particular secure communications and has a keen interest in this area. Faith has a PhD in Electronic and Electrical Engineering from the University of Southampton.

Micael Berg, Cryptify

Micael is the Chief Sales Officer of Cryptify. He is an entrepreneur and senior executive with over 19 years of experience in product development, sales and business development in the technology and telecommunications industry. He started his career at Ericsson developing products augmenting the mobile networks to also handle mobile broadband. Micael holds a M.Sc. in Electrical and Electronics Engineering from the Chalmers University of Technology.

Mike Brown, ISARA Corporation

Mike is the co-founder and CTO of ISARA Corporation focusing on the technical vision and direction of the company. Mike was most recently the VP of Security Product Management and Research at BlackBerry, where he co-founded the product security practice and was responsible for the vision and execution of security for all BlackBerry products. Mike has spoken at global security events and holds a Master of Mathematics from the University of Waterloo, focusing on cryptography.
Dr Kit Kilgour, Sepura plc

Kit is a Senior Specialist in the Product Strategy division of Sepura plc. Kit has over 20 years’ experience working in wireless communications. His standardisation experience includes a range of 3GPP working groups and the Small Cell Forum. He is currently working in 3GPP on the design of secure Mission Critical communications systems. Kit has a PhD in Mathematics from the University of Cambridge.

Gerald McQuaid, Vodafone

Gerald is responsible for national security and critical infrastructure protection area across Vodafone Group’s footprint. He is currently a chair of an ETSI Technical Committee, a member of a government advisory committee and a stakeholder of LEA Support in many markets. Previously a member of various EU Experts Groups and a frequent contributor to the EU’s Research Network on Critical Infrastructure Protection. Prior to Vodafone Gerry was responsible for deployment of LEA Support systems globally, as well as a first responder assisting the UN during major disasters. Gerald has a B Eng (Hons) Engineering, Electrical and Mechanical Engineering and a MSc in Security Management.

Simon Pryce, Leonardo MW

Simon is an Account Manager within the Security and Information Systems Division of Leonardo focused mainly on the company’s Secure Communications capabilities. This includes Leonardo’s MIKEY-SAKKE product, CERYX, and also the company’s Mission Critical Communications capabilities across its LTE, TETRA and Digital Mobile Radio portfolio ranges. Simon holds a BSc in Biology from the University of Nottingham.

Dr Nithin Thomas, SQR Systems

Nithin is the co-founder & CEO of SQR Systems, a company developing secure mobile and IoT communications for better control of data and privacy. He has delivered technology to regulated sectors, ranging from Defence and Intelligence to Financial Services. Nithin holds a PhD from University of Bristol and was granted a patent for optimisation of encrypted data for poorly connected networks.

Sebastian Wiles, Serbus

Seb’s career started in the military as a Communications Manager before he joined Three UK. In 2009 he and his business partner established Serbus Ltd, a very successful company focused on securing the remote worker. Serbus Secure is its leading product which gives users the freedom of today’s mobile technology, but in an enterprise managed and secure way.
Services

Government Member Benefits

- Organisation’s name included in the Secure Chorus’ Register of Members
- Entitled to send representatives to attend and vote at general meetings of Secure Chorus
- Vote on appointment of Directors of Secure Chorus’ board
- Vote on appointment of chairperson of Secure Chorus’ Governments Committee and Standards Committee
- Eligible to join Secure Chorus’ Governments Committee and Standards Committee and any advisory groups
- Right to be part of the Secure Chorus Thought Leadership Platform
- Right to influence the development and use Secure Chorus’ technical standards.
- Right to use any Secure Chorus infrastructure and services for Secure Chorus Compliant Products
- Right to participate in Secure Chorus’ Plugfests for interoperability testing
- Right to attend and participate in Secure Chorus member-only meetings

Partner Member Benefits

- Organisation’s name included in Secure Chorus’ Register of Members
- Entitled to send representatives to attend and vote at general meetings of Secure Chorus
- Vote on appointment of Directors of Secure Chorus’ board
- Vote on appointment of chairperson of Secure Chorus’ Standards Committee, SMEs or MEs Committee, depending on Partner Member’s annual revenue
- Eligible to serve on Secure Chorus’ board of directors as non-executive director
- Eligible to join Secure Chorus’ advisory groups and Standards Committee, SMEs or MEs Committee, depending on Partner Member’s annual revenue
- Right to be part of the Secure Chorus Thought Leadership Platform
- Right to influence the development and use Secure Chorus’ technical standards.
- Right to use any Secure Chorus infrastructure and services for Secure Chorus Compliant Products
- Right to participate in Secure Chorus’ Plugfests for cross vendor interoperability testing
- Right to attend and participate in Secure Chorus member-only meetings
- Priority placement at Secure Chorus’ events, shows and advertising
- Opportunity to keynote at Secure Chorus’ events
- Company logo highlighted on Secure Chorus’ website
- Public acknowledgement at Secure Chorus’ events such as corporate logo displays
- Access to speaking opportunities at industry events
- Demonstrate Secure Chorus Compliant Products at meetings, tradeshow booths, and other Secure Chorus events
- Right to use Secure Chorus marketing material internally and externally
- Free Secure Chorus marketing kits: signs, brochures, etc.
**Associate Member Benefit**

- Organisation’s name included in the Company’s Register of Members
- Entitled to send representatives to attend general meetings of Secure Chorus
- Right to be part of the Secure Chorus Thought Leadership Platform
- Right to use Secure Chorus’ technical standards
- Right to use any Secure Chorus infrastructure and services for Secure Chorus Compliant Products
- Right to participate in Secure Chorus’ Plugfests for cross vendor interoperability testing
- Right to be part of the Secure Chorus Thought Leadership Platform
- Right to attend and participate in Secure Chorus member-only meetings
- Prioritised placement at Secure Chorus’ events, shows and advertising
- Opportunity to keynote at Secure Chorus’ events
- Company logo highlighted on Secure Chorus’ website
- Public acknowledgement at Secure Chorus’ events such as corporate logo displays
- Access to speaking opportunities at industry events
- Demonstrate Secure Chorus Compliant Products at meetings, tradeshow booths, and other Secure Chorus events
- Right to use Secure Chorus marketing material internally and externally
- Free Secure Chorus marketing kits: signs, brochures, etc.

**Observers Benefits**

- Right to use Secure Chorus’ technical standards
- Right to use any Secure Chorus infrastructure and services for Secure Chorus Compliant Products
- Right to participate in Secure Chorus’ Plugfests for cross vendor interoperability testing
- Right to be part of the Secure Chorus Thought Leadership Platform
- Right to attend and participate in Secure Chorus member-only meetings
- Prioritised placement at Secure Chorus’ events, shows and advertising
- Opportunity to keynote at Secure Chorus’ events
- Company logo highlighted on Secure Chorus’ website
- Public acknowledgement at Secure Chorus’ events such as corporate logo displays
- Access to speaking opportunities at industry events
- Demonstrate Secure Chorus Compliant Products at meetings, tradeshow booths, and other Secure Chorus events
- Right to use Secure Chorus marketing material internally and externally
- Free Secure Chorus marketing kits: signs, brochures, etc.
## Subscription Fee

<table>
<thead>
<tr>
<th>Membership Type</th>
<th>Worldwide Turnover</th>
<th>Membership Fee/Annum (excludes VAT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supranational or National Government</td>
<td>N/A</td>
<td>£20,000</td>
</tr>
<tr>
<td>Partner Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Enterprise</td>
<td>Turnover above £50 million</td>
<td>£10,000</td>
</tr>
<tr>
<td>Small - Medium Enterprise (SME)</td>
<td>Turnover below £50 million</td>
<td>£5,000</td>
</tr>
<tr>
<td>Micro - Enterprise (ME)</td>
<td>Turnover below £2 million</td>
<td>Free</td>
</tr>
<tr>
<td>Associate Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Enterprise</td>
<td>Turnover above £50 million</td>
<td>£7,000</td>
</tr>
<tr>
<td>Small - Medium Enterprise (SME)</td>
<td>Turnover below £50 million</td>
<td>£3,000</td>
</tr>
<tr>
<td>Micro - Enterprise (ME)</td>
<td>Turnover below £2 million</td>
<td>Free</td>
</tr>
<tr>
<td>Observer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic institution, standards organisation or trade association</td>
<td>N/A</td>
<td>£2,000</td>
</tr>
</tbody>
</table>

The subscription fee will not be charged by the Company to its members and observers joining in 2017 and 2018.

We created this free membership and observer status to build momentum and help early potential members and observers overcome any hesitancy they may have about registering.

We also believe that members and observers which are not paying a fee are valuable assets. They help us test our membership model and become test cases for the Company’s services.
Intellectual Property Rights Model

The Company has a mandatory intellectual property rights policy which is set out in the Membership Application Form of the Company, and therefore applies to the Company and all of its members/observers.

Introduction

The objects for which the Company is established are the development and publishing of MIKEY-SAKKE protocol based interoperability standards. In the pursuance of its activities, the Company may refer to or make use of patents and IP protected by IPR legislation. Diligent conduct in respect of these rights is essential to the Company’s functioning, good reputation, authority, sustainability and the achievement of its core objectives.

Scope

The aim of the IPR policy is to ensure the Company and its members/observers are aware of their responsibilities and obligations in relation to IPR, in order to minimise risk of infringement of patents and IP, and to ensure members /observers are committed to fair licencing terms of any patents related to the standards (field patents).

The Company IPR Policy applies to all activities undertaken by the Company and its members/observers, regarding the development, convergence and adoption of MIKEY-SAKKE based interoperability standards for the secure communications industry.

Summary of the IPR Policy

Declaration of Field Patents

“Field Patents” means any Patent(s) owned by a member / observer, or an Affiliate of a member or observer, which would be infringed by the manufacture, sale, supply, lease, repair, use, importation, keeping, or otherwise disposal of any product that operates in accordance with any optional or mandatory part of a Standard such that it is not possible on technical (but not commercial) grounds to operate in accordance with any Standard without infringing that Patent. In the event that the technical solution prescribed in the Standard infringes different Patents depending upon how that Standard is implemented all such patents shall be considered to be Field Patents.

On becoming a member/observer, each shall provide the Company with a written declaration identifying its patents that are or may reasonably become field patents.

Thereafter, each member/observer shall use reasonable endeavours to provide the Company with a declaration identifying when a standard or any other deliverable may require the use of any field patent owned by that member/observer. Such declaration must be provided in a timely manner, and in particular if a member or observer is submitting a proposal for a Deliverable (including a Standard), such proposal should identify Field Patents, or potential Field Patents, for which a Declaration must be provided within 48 hours of submission.
The above obligations do not require that members/observers carry out searches for any Field Patents.

Members/observers are also not compelled to contribute any specific patents to any deliverable, but should they choose to do so, and should the relevant patents become field patents, then there is an obligation to make a declaration, which must be submitted to the Company within 14 days of such Patents becoming Field Patents, or within 14 days of that Member or Observer identifying a Patent as a potential Field Patent, whichever is the sooner.

If a member/observer fails to make a declaration, they will be deemed to have provided the undertaking relating to the field patents that should have been the subject of such declaration, as defined below.

Licencing of Field Patents

Where a member/observer becomes aware that it owns a patent that is, or may become, a field patent it must provide an irrevocable undertaking on the relevant declaration form that they are prepared to grant a non-exclusive licence of all of their field patents to manufacture (and have manufactured), sell, offer for sale, import, use or keep any product or service or method which operates in accordance with, or conforms to the Standard only in so far as it is necessary for the product, service or method to comply with the Standard:

• on FRAND Terms; and
• to any person or entity wishing to make use of the deliverable(s).

Such undertaking must bind all successors in title and affiliates, save where specific affiliates are noted on the Declaration as not being bound by the undertaking.

Any Undertaking that a member or observer provides can be made conditional upon a reciprocal Undertaking from any prospective licensee in respect of their Field Patents.

The member/observer may refuse to provide an Undertaking to licence only if the patents are:

• not based on any Activity;
• developed independently of any other member/observer;
• not developed with the intention to be part of a deliverable; and
• declared on a declaration form.

If any member/observer refuses to provide an undertaking, or if the Company does not accept (acting reasonably) the reasons that the member/observer has provided in the declaration form for refusing to provide the undertaking, then that member/observer will lose their rights to participate in the relevant activity and develop any deliverable arising from it.

If, prior to the publication of a deliverable (including a standard) a member/observer refuses to give the Undertaking in respect of certain field patents then the Company shall review the deliverable and identify alternative technology that does not infringe that patent. The above loss of rights to participate will continue to apply if alternative technology is identified unless the Company, at its sole discretion, determines otherwise.

If any field patent is not identified prior to the publication of a deliverable, the member/observer that owns the field patent undertakes to provide a declaration that includes an undertaking in respect of that patent within 14 days of the Member or Observer recognising that they have a field patent.
If a Third-Party field patent is identified prior to the publication of a deliverable, the member/observer that identified the Third-Party field patent will ask the third-party owner if it is prepared to give an undertaking. If the third-party refuses to do so, then the Company shall review the deliverable and identify alternative technology that does not infringe that Third-Party field patent.

If the Third-Party field patent is identified after the publication of a deliverable the member or observer that identified the Third-Party Field Patent will ask the third-party owner if it is prepared to give an undertaking. If the third-party refuses to do so, then the Company shall withdraw the Deliverable (including revoking the Standard) and review the Deliverable to identify alternative technology that does not infringe that Third-Party Field Patent. If no alternative technology is identified, the Deliverable shall remain withdrawn until such time as either an Undertaking is provided in respect of the Third-Party Field Patent, or alternative technology is identified.

The Company shall form an advisory group prior to 31 March 2019 to attempt to agree a policy and/or guidelines as to what FRAND Terms are for a licence under any Field Patent (the “FRAND Guidelines”). Should the committee reach agreement as to appropriate FRAND Guidelines, the FRAND Guidelines shall be presented to the members at an extraordinary general meeting for approval by a special resolution.

Deliverables

All copyright, other than any original contribution Intellectual Property that is contributed by a Member or Observer, in any Deliverable shall be owned by the Company.

The Company shall make copies of all issued Deliverables available to members free of charge.

If Deliverables are marked by the Company (at its sole discretion) as “members only”:

- Members may make copies of the Deliverables for their own use, but may not distribute copies to third parties, or communicate their content to anyone who is not a Member without the Company’s prior written approval; and
- Observers may not be provided with a copy of the Deliverable without the Company’s prior written approval.
- If an Observer is provided with a copy of the Deliverable the Observer may make copies of the Deliverables for its own use, but may not distribute copies to third parties, or communicate their content to anyone who is not a Member without the Company’s prior written approval.
- If Deliverables are not marked by the Company (at its sole discretion) as “members only” members or the Company may make copies of the Deliverables available to the public free of charge.

Intellectual Property and Field IP

All trademarks owned by the Company can be used by members/observers only while they remain members /observers and on the basis, that such use is in accordance with the Company’s brand guidelines which are located on the Company’s website at www.securechorus.org as may be updated from time to time. Any goodwill that accrues as a result of such use shall accrue automatically and exclusively to the Company. members/observers shall not make any statements on behalf of the Company without the Company’s prior written approval.
It is the Member/Observer’s responsibility to determine whether any IP that is contributed to an activity requires the prior consent of another party to be used by the Company and other members/observers, and if so, to obtain that consent.

By contributing IP to an activity, the member/observer warrants that, so far as that member/observer is aware, that IP does not infringe a third party’s IP.

By contributing IP to an activity, the member/observer grants the Company an irrevocable, sub-licensable, non-exclusive, royalty-free worldwide licence to use or reproduce the IP or carry out any activity that would but for this licence infringe the field IP, in connection with a deliverable or the implementation of a deliverable.

For the avoidance of doubt, ownership of any original contribution of field IP is not assigned to the Company.

Confidentiality

Except as expressly provided below, all Activity shall be non-confidential, and all documents submitted in connection with an Activity by a member or observer, or Affiliate of a member or observer shall be treated as non-confidential.

Information will be treated as confidential (“Confidential Information”) in the following circumstances:

- the confidential information is in written form, and the confidential information is clearly identified; and
- the information is identified as confidential in writing; and
- the confidential information, together with a request that it is treated as confidential has first been submitted to the Company, who has accepted that the information is confidential.

Confidential Information may be disclosed to any members/observers provided that the member/observer to whom the Confidential Information is disclosed is informed of the confidential nature of the Confidential Information before disclosure.

In the event that Confidential Information is to be discussed, referred to or otherwise used during an Activity, the Activity (or part thereof) shall be confidential only in so far as it is strictly necessary to maintain the confidentiality in the Confidential Information.

Any information that is treated as confidential pursuant to clause 11.2 that is incorporated into a Deliverable will be deemed to be non-confidential from the date upon which that Deliverable is issued.

Warranties

The Company makes no representations or give any warranties as to non-infringement of third party IP or Patents in relation to this IPR Policy.

The Company makes no representation or warranty as to the validity of any claim of any Field Patent, or as to the essentiality to a Standard of any claim of a Field Patent.
The Member or Observer agrees not to assert its Field IP or Field Patents against the Company in respect of any promotion or publication of Deliverables (including Standards) by the Company, during the period of its membership or afterwards.

If any Member or Observer breaches its obligations under this IPR Policy, the Company reserves the right to take any actions available to the Company under its procedures or at law, in order to protect the interests of the Company or of any other Member or Observer, including but not limited to excluding the defaulting Member or Observer from any Activities or terminating its membership.

The Company is not responsible for determining whether any proposed licensing terms are on FRAND Terms.

To the fullest extent permitted by law, the Company shall not be liable to the Member or Observer for any costs, expenses, loss or damage (whether direct, indirect or consequential, and whether economic or other) arising from the Member or Observer’s exercise of the rights granted to it under this IPR Policy.

Subject to the above, the total liability of the Company under or in connection with the IPR Policy (whether arising in contract, tort, negligence, breach of statutory duty or otherwise) shall not exceed the sum of the annual fee paid by the Member or Observer.
Secure Chorus Compliant Products

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 secure communication in enterprise. All products provide for end-to-end encryption; however, users are not locked-in by a specific vendor, therefore it is possible for users of different products to communicate 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.

Secure Chorus Compliant Products address several important communication requirements for the enterprise and the public sector:

**Data security:** end-to-end encryption enables users to communicate in a variety of environments, both at rest (e.g. storage) and in transit (e.g. network systems). However, users are not locked-in by a specific vendor.

**Data ownership:** the technology can be centrally managed, giving a 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.

**Interoperability:** Secure Chorus’ KMS (Key Management Server) based approach allows domain managers to easily enable secure communication between different user groups without bringing external users into their security perimeter.

**Scale:** all products use an identity based public key, requiring no expensive and complex supporting infrastructure for distributing credentials, allowing for at-scale implementation.

**Flexibility:** supporting both real-time communications (such as one-one and multi-party calls) and deferred delivery (such as messaging and voicemail).

**Implementation agnostic:** users have the complete freedom and flexibility to deploy platforms and infrastructure to meet their requirements.
Location

The Company's location and offices are as follows:

• Registered office address: Cannon Place, 78 Cannon Street, London, EC4N 6AF
• Trading office address: Level39 One Canada Square, Canary Wharf, London E14 5AB.