Vanilla+

THE GLOBAL VOICE OF TELECOMS IT

MWC 2021

ISSN 1745-1736

THE VANILLAPLUS CEO GUIDE TO MWC2021

TALKING HEADS

iconectiv's Michael O'Brien explains how verification initiatives are restoring trust in telecoms

PLUS: Vodafone unveils strategic O-RAN vendors ■ Amdocs expands collaboration with Microsoft Azure for Operators ■ JieSai chooses TEOCO to predict 5G coverage in China ■ Mobileum launches RAID on BNET fraudsters ■ AWS and Spirent to deliver automated 5G testing ■ How to combat rich business messaging frauds ■ All you need to know for MWC's return to Barcelona ■ Beyond by Bearing Point CEO details how co-creation and co-innovation are driving CSP opportunities for business model re-invention ■ Latest News, Features and Interviews at www.vanillaplus.com

the trust factor

Your business customers are negatively impacted because consumers are ignoring calls and texts from phone numbers they do not recognize. Protect your network, your customers and your bottom line.

Enough is enough.
It is time to take back your network

Trusted Voice | Text | Messaging | Chatbots

Let iconectiv help you keep people connected, businesses running and commerce flowing.

sales@iconectiv.com 1 +732-699-6800

click for details

iconectiv.com

iconectiv

TALKING HEADS 8
Michael O'Brien, iconectiv

RICH BUSINESS MESSAGING 12

GSMA MWC™ Barcelona

EVENT PREVIEW 14

CONTENTS

IN THIS ISSUE

COVER SPONSOR
Your business and your customers need to access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services and its unmatched numbering intelligence helps you do just that. In fact, more than two billion people count on our platforms each day to keep their networks, devices and applications connected. Our cloud-based Software as a Service (SaaS) solutions span network and operations management, numbering, trusted communications and fraud prevention. For more information, visit **https://iconectiv.com**. Follow us on Twitter and LinkedIn.

VanillaPlus magazine is published as a digital edition 4 times a year. It is available free of charge to all readers worldwide, at the publisher's discretion. To subscribe **free of charge** go to: **www.VanillaPlus.com**, click the "Subscribe" tab on the Home Page and answer the questions shown. The Publisher reserves the right to alter or end this free offer at any time without notice. No guarantee is stated or implied. You can unsubscribe at any time by emailing **subscribe@vanillaplus.com** with UNSUBSCRIBE in the Subject line.

PRESTIGE MEDIA LTD.

© Prestige Media Ltd 2021

All rights reserved. No part of this publication may be copied, stored, published or in any way reproduced without the prior written consent of the Publisher

Attendance is optional, attention is mandatory

MWC2021, to be held in Barcelona, Spain on 28 June – 1 July 2021, will be a very different event to those that have gone before. Fewer visitors and exhibitors will change the character of the event but much of this will be made up for by new virtual elements to the show

For me, MWC has always been an agenda-setting event. In more than 20 years covering the telecoms industry I have never found such a condensed opportunity to learn new things, meet new people and gauge the direction of travel in the industry for the coming year. This year, though, it isn't February and we're already halfway through the year so many of the trends of 2021 are all well underway.

Inescapably, 2021 is unlike 2019. Travel and social contact are constrained although there is hope, as vaccines continue to roll-out, this will soon end. For those able to make it safely to Barcelona, GSMA and the local authorities have worked extremely hard to minimise risk and assure visitors and the local population of their safety. These efforts which encompass testing and social distancing are detailed by Antony Savvas on p14 and go a long way to build peace of mind for in-person attendees.

However, for those facing lengthy quarantine periods on their return from Spain, the show will be a no-go in-person this year. This includes me and breaks a run of attendance extending back for more than 15 years. I have felt strangely dislocated from the industry in late February over the last two years as my muscle memory insists I board a budget flight to Barcelona so it's great that at least some form of show is happening this year.

Some of this looks jarring. **Ericsson**'s Hall 2 super-stand – incidentally always the best place for lunch – is being occupied by **TelcoDR**, the telco cloud start-up led by former **Optiva** CEO Danielle Royston, who is showcasing innovation in the vast space that Ericsson has opted out of this year. On one hand it's excellent that something is being done to entertain visitors but missing industry giants – Ericsson is far from alone in not attending this year – from the exhibitor roster will inevitably detract from the show experience.

George Malim, managing editor

Even in its weakened state, MWC2021 will still be one of the largest assemblies of telecoms professionals in the world this year and the virtual elements should not be ignored. I'll certainly be listening in and selecting key speeches and virtual events to participate in. However, I'll be keen to attend a full-scale event again once the pandemic is further under control.

The power of MWC has been demonstrated in its absence and whether you're attending in-person or virtually this year, I hope you have a great experience.

Enjoy the magazine!

George Malim

EDITORIAL ADVISORS

Louis Hall, chief executive, Cerillion Technologies

Martin Morgan, VP Marketing at Openet an Amdocs company

Laurent Leboucher, VP Customer Relations Solutions, Orange

Chris Yeadon, director of Product Marketing, Ericsson

MANAGING EDITOR
George Malim
Tel: **+44 (0) 1225 319566**
george@vanillaplus.com

EDITORIAL DIRECTOR & PUBLISHER
Jeremy Cowan
Tel: **+44 (0) 1420 588638**
j.cowan@wkm-global.com

DIGITAL SERVICES DIRECTOR
Nathalie Millar
Tel: **+44 (0) 1732 808690**
n.millar@wkm-global.com

SALES CONSULTANT
Cherisse Jameson
Tel: **+44 (0) 1732 807410**
c.jameson@wkm-global.com

DESIGN
Jason Appleby
Ark Design Consultancy Ltd
Tel: **+44 (0) 1787 881623**

DISTRIBUTION
UK Postings Ltd
Tel: **+44 (0) 8456 444137**

PUBLISHED BY
Prestige Media Ltd.
Suite 138, 80 Churchill Square,
Kings Hill, West Malling,
Kent ME19 4YU, UK
Tel: **+44 (0) 1732 807410**

VanillaPlus magazine is published as a digital edition 4 times a year. It is available free of charge to all readers worldwide, at the publisher's discretion. To subscribe **free of charge** go to: **www.VanillaPlus.com**, click the "Subscribe" tab on the Home Page and answer the questions shown. The Publisher reserves the right to alter or end this free offer at any time without notice. No guarantee is stated or implied. You can unsubscribe at any time by emailing **subscribe@vanillaplus.com** with UNSUBSCRIBE in the Subject line.

All rights reserved. No part of this publication may be copied, stored, published or in any way reproduced without the prior written consent of the Publisher

PRESTIGE MEDIA LTD.

© Prestige Media Ltd 2021

Vodafone partners with Dell, NEC, Samsung and Wind River to build Open RAN

Vodafone has unveiled its strategic vendors for deployment of its open radio access network (O-RAN); **Dell, NEC**, **Samsung Electronics**, **Wind River**, **Capgemini Engineering** and **Keysight Technologies**. The communications service provider (CSP) claims its partners will jointly deliver the first commercial deployment of O-RAN in Europe.

With political and industrial policy support from the European Commission and the national governments of the EU, open RAN has the potential to bring more European companies into this emerging market. Vodafone and the other major EU telecoms signatories of the Open RAN MoU believe this will help build a European ecosystem around these novel network architectures and boost the EU's global technology leadership in digital infrastructure.

Vodafone's initial focus will be on the 2,500 sites in the UK that it committed to O-RAN in October 2020. It is one of the largest deployments in the world and will be built jointly with Dell, NEC, Samsung and Wind River. Vodafone also expects to use new radio equipment defined under the Evenstar programme, a joint initiative it contributes to. Capgemini Engineering and Keysight Technologies are providing support to ensure interoperability between all the components.

Starting this year, the vendors will work with Vodafone to extend 4G and 5G coverage to more rural places across the South West of England and most of Wales, moving into urban areas in a later phase. Vodafone is also working to launch O-RAN in other countries within both Europe and Africa, enabling the digital society to be accessible to all, with no one left behind.

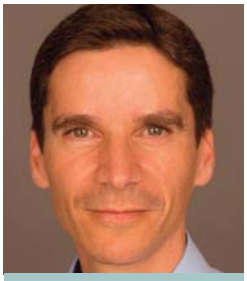
Johan Wibergh, Vodafone chief technology officer, said: "Open RAN provides huge advantages for customers. Our network will become highly programmable and automated meaning we can release new features simultaneously across multiple sites, add or direct capacity more quickly, resolve outages instantly and provide businesses with on-demand connectivity.

Trusted Connectivity Alliance enhances remote SIM provisioning specification

The **Trusted Connectivity Alliance (TCA)** has released version 3.0 of its eUICC Profile Package: Interoperable Format Technical Specification. This major update aligns the specification, which is used in every eSIM deployed in the field, with 3GPP Release 16 to fully support 5G and cellular vehicle-to-everything (C-V2X) functionality. The latest version of the specification also includes clarifications and guidance to further enhance eSIM interoperability.

The specification standardises the format used for remote loading of subscriptions onto eSIMs across deployed devices. This enables mobile network operators to load interoperable connectivity profiles in an eSIM, regardless of the SIM vendor.

"The publication of this specification marks a very significant step forward for the eSIM market," said Claus Dietze, chair of the TCA Board. "We are seeing robust eSIM growth, with our members reporting an 83% year-on-year increase to 309 million units in 2020, and sustaining this momentum requires approaches to enable secure, consistent and reliable remote eSIM provisioning."



Claus Dietze, TCA

TCA is also finalising an associated test specification which provides a globally standardised means of testing products to ensure the connectivity profile is correctly loaded. Other TCA initiatives to promote eSIM interoperability include coordination with GSMA to ensure that ongoing eSIM standardisation activity addresses the unique requirements of the IoT ecosystem in a simple, scalable way. This includes the development of lightweight subscription profiles that are optimised for constrained IoT devices.

NEWS IN BRIEF

Nokia opens new US O-RAN collaboration and testing centre

Nokia has opened its first open radio access network (O-RAN) Collaboration and Testing Centre at its US offices in Dallas, Texas. The centre is designed to support the development of partnerships among O-RAN vendors that will help with the verification, introduction and launch of O-RAN compliant solutions to market.

In particular, vendors will be able to execute Interoperability Tests (IOT) and end-to-end testing for O-RU/O-DU Open Fronthaul as well as xAPP testing for Nokia's near-real-time RAN Intelligent Controller (RIC). The project is the latest in Nokia's continued commitment to O-RAN, vRAN and Edge Cloud innovation. Nokia plans to open similar facilities at its other global offices around the world in the future.

MWC Los Angeles 2021 to return as a live event in October

GSMA has revealed details of MWCLA21, in partnership with **CTIA**, which will return live and in-person this October.

Taking place at the Los Angeles convention centre from 26-28 October, the theme of this year's event is connected impact. The programme will explore how the 5G era, IoT connectivity, telco cloud and disruptive innovation are shaping the future and continuing to transform lives.

"MWC Los Angeles is the must-attend tech industry event of the Americas and, we are very much looking forward to returning to California. MWCLA21 provides a platform for people to come together to push the industry and society forward," said John Hoffman, CEO of GSMA.

NEWS IN BRIEF

Fastweb moves to next-gen BSS with Netcracker

Fastweb, an Italian telecoms operator and part of the **Swisscom Group**, has renewed its contract to upgrade to **Netcracker** Digital BSS and extend its use of Netcracker Support & Maintenance. With 2.7 million wireline customers and 1.9 million mobile customers, Fastweb has developed a national fibre optic network infrastructure of 50,500km with more than four million kilometres of fibre reaching 22 million customers. This will be expanded with 5G fixed wireless access (FWA) technology, bringing the number of households and businesses reached to 16 million by 2025.

Netcracker Digital BSS helps transform operator environments into 5G-ready, cloud-native digital ecosystems that support new lines of business, cloud applications and virtualised services. When combined with Netcracker Support & Maintenance professional services, operators gain optimal business performance and outcomes while greatly reducing the risk of running and maintaining complex systems.

MTN Rwanda selects Whale Cloud digital BSS suite

MTN Rwanda has gone live with **Whale Cloud**'s digital BSS suite as part of its plans to revamp its business support system (BSS), allowing the CSP to accelerate its transformation journey with enhanced customer experience and increased revenue streams.
MTN Rwanda is a subsidiary of MTN Group, a mobile network operator across Africa.

As the need for new digital services continues to grow, MTN Rwanda is transforming its legacy systems to stay competitive. Whale Cloud has delivered full stack digital BSS solutions including Real-Time Billing (RTB) and Customer Relationship Management (CRM).

Capgemini and Orange create Bleu to meet cloud sovereignty requirements

Stephane Richard, Orange

Capgemini and **Orange** are to set up a new company named **Bleu** to provide a 'Cloud de Confiance' service that will meet sovereignty requirements of the French state, public administrations and critical infrastructure companies with privacy, security and resiliency needs. Bleu will aim to provide its customers with an independent, trusted cloud platform with a broad catalogue of digital solutions and collaborative tools. The partnership provides a significant step forward in accelerating France's digital transformation.

This project will combine the expertise of Capgemini and Orange two French global digital companies working with **Microsoft**, to create a French cloud service provider that satisfies the unique needs of a specific set of organisations. Bleu will offer its solutions to vital importance operators (OIVs) and essential service operators (OSEs), the French state, public agencies, hospitals and regional authorities whose sensitive data and workload require a 'Cloud de Confiance' platform tailored to their needs.

Bleu will offer Microsoft's secure cloud technology including the modern collaboration and productivity solutions of Microsoft 365 and the services available on the Microsoft Azure cloud platform, delivered via an independent environment, to ensure that customers benefit from the widest range of the latest technology innovations.

Stephane Richard, the chairman and CEO of Orange, commented: "This 'Cloud de Confiance' meets a growing need in the digital world. The French state recently highlighted this in defining its 'cloud au centre' policy and setting out the standards required regarding data protection and sovereignty. Orange, as a trusted partner for the digital transformation of businesses, operates, integrates and manages a range of trusted infrastructure services for its customers, whether they are public or private entities."

Amdocs expands strategic collaboration with Microsoft to boost CSPs' journeys to the cloud

Amdocs, a provider of software and services to communications and media companies, has announced the extension of its global business, technology and services collaboration with **Microsoft**, widening the availability of its portfolio on Microsoft Azure and the Azure for Operators (AFO) initiative. This expanded cooperation will accelerate the communications and media industry's journey to the cloud, enabling service providers to offer new and differentiated cloud services to drive growth, customer loyalty and value-add with fast and agile interactions, and a wide ecosystem of third-party partners.

The collaboration will enable service providers to accelerate their move to the cloud by using Amdocs' cloud-native BSS/OSS solutions and services and unique delivery accountability model while benefiting from the cloud capabilities of Azure to build, manage and deploy service provider applications at scale.

"As service providers embark on the most widespread transformation the communications and media industry has seen, Microsoft is playing a pivotal role in accelerating CSP journeys to the cloud," said Shuky Sheffer, the president and chief executive officer of Amdocs. "We are therefore delighted to become a Microsoft preferred Industry Priority Scenario (IPS) Partner. With Amdocs and Microsoft, service providers will be able to transform with cloud-native solutions and cloud services and deploy 5G networks in the cloud with Azure for Operators, automated by the Amdocs NEO service and network automation suite and monetised by Amdocs Charging."

BNET selects Mobileum to cut revenue leakage and boost customer experience

Mobileum, a global provider of analytics-based roaming and network services, telecoms security, risk management and testing and monitoring solutions, reports that **Bahrain's National Broadband Network** (BNE) has selected its Active Intelligence Platform for Risk Management. BNET will deploy the latest release of Mobileum's revenue assurance solution, RAID, enabling automation across key systems as part of its vision of creating a state-of-the-art digital communications infrastructure.

Launched in October 2019, BNET is an independent wholesale broadband provider, and a key part of the Kingdom of Bahrain's fifth National Telecommunication Plan to develop and enhance the telecoms sector. BNET provides next-generation fibre broadband connectivity solutions to all licensed telecoms operators in Bahrain.

Mobileum's Revenue Assurance solution will support BNET in the reduction of revenue leakage, relying on its next-generation automated control system to ensure that services are accurately billed and collected. Along with billing and payment assurance, the solution will also manage disputes and assure margins, contracts and inventory.

Rui Paiva, Mobileum

"By launching Mobileum's Revenue Assurance solution, BNET is well-positioned to respond to a rapidly evolving business landscape, getting strong visibility and control across the entire revenue chain," said Rui Paiva, chief of Mobileum's risk management business. "BNET will be able to map and correlate multiple business processes across ordering, billing, accounting and inventory systems, identify gaps where leakage occurs, protect margins and maximise monthly revenues."

JieSai selects TEOCO to predict 5G network coverage in China

TEOCO, a provider of analytics, assurance and optimisation solutions to more than 300 communication service providers (CSPs) worldwide, has been selected by **JieSai**, a Chinese design institute serving the country's mobile operators, to deploy ASSET Radio and ASSET Design, TEOCO's 5G radio network planning and design tools.

JieSai will use TEOCO's ASSET tools to deliver mobile radio network design, planning and modelling services for its operator customers, including **China Mobile**, **China Unicom** and **China Tower**. ASSET Radio and ASSET Design's planning and modelling features will help JieSai to better simulate 5G network coverage and performance, and support network parameter planning, including antenna location and positioning.

The deployment follows JieSai's use of ASSET for LTE network planning. Since using ASSET, the design institute has improved its planning efficiency, and increased mobile coverage and quality for its mobile operator customers significantly, it says.

"JieSai plays a critical role in helping Chinese mobile operators meet the demands of their customers through the delivery of network design and planning," said Cheng Min, the wireless chief engineer at JieSai. "It's very important that we have the right tools to accurately predict radio network coverage. Having seen the benefits of TEOCO's ASSET solution across LTE networks, we were confident of its capabilities for 5G and we're delighted to be working with TEOCO to deliver the best service to our operator customers."

Atul Jain, the founder and chief executive of TEOCO, added: "Our ASSET portfolio continues to play a critical role in the roll out of new networks, helping network planners around the world meet coverage, capacity and quality targets. As JieSai's operator customers continue to optimise their 5G roll outs and deployments, we are delighted to be providing the design institute with the right tools to ensure network coverage and maximise planning efficiency."

NEWS IN BRIEF

AWS and Spirent collaborate to deliver automated 5G network testing

Spirent Communications has announced a collaboration with **Amazon Web Services** (AWS) to bring automated 5G testing capabilities to communications service providers (CSPs) building 5G networks on AWS. Spirent's Landslide 5GC Automation Package is designed to help CSPs to rapidly deploy 5G networks on AWS, significantly reducing operational costs, time and resources compared to manual testing.

By combining AWS's continuous integration and continuous delivery (CI/CD) pipeline with Spirent's vendor-neutral 5G test capabilities, CSPs will be able to objectively, rapidly and continuously validate mobile network functions and services across a wide range of requirements, including compliance, capacity and performance dimensions. The combined solution is aimed at mobile carriers who want to accelerate delivery of 5G services on AWS.

CSG extends contract at Vietnamobile

CSG has announced a multi-year contract/relationship extension with **Vietnamobile** under which it will drive the CSP's customer billing, mediation and settlement operations to support accelerated growth and the introduction of new products and services.

"Our rapid transition to digital mobile services across Vietnam is fueling an explosive wave of customer growth and demand," said Christina Hui, the chief executive of Vietnamobile. "CSG has been our trusted technology provider for many years. We are excited to grow this relationship."

Verification initiatives hang up on fraudsters to restore trust in telecoms

Regulators, businesses and communications service providers (CSPs) face an uphill battle to mitigate telco and consumer fraud as well as illegal robocalls. Erosion of trust is damaging CSPs in the form of unanswered calls and fraudulent messaging but perhaps worse is the damage being done to CSPs and large brands as customers ignore their calls and turn away from telephony.

New technical approaches such as the robocall mitigation database in the US and other countries are starting to fightback but more effort is needed. Michael O'Brien, the chief product officer of iconectiv, tells George Malim, the managing editor of VanillaPlus, how verification, certification and legislation are coming together to combat damage to trust in networks. However, he emphasises it is implementation of solutions, not legislation that will enable trust to be rebuilt

George Malim: Why do you think consumer trust in telecoms services is being eroded?

Michael O'Brien: While some of the technologies that were created to enable the future of telecoms networks have been transformational, they also unintentionally exposed the network to spoofing and fraud. For instance, session initiation protocol (SIP) not only created flexibility and virtualisation of networks but also the ability to replace caller identification (ID) fields that are presented to the recipient – without being tied to the origination header that was used in a traditional switched network. That opened the door to means for deceiving people through spoofing methods, which has led to the level of caller distrust we are experiencing today.

Traditionally, telecommunications networks have been one of the most trusted methods of communication. Now, people don't want to answer phone calls because the volume of scam calls and attempted fraud has significantly altered public opinion about whether they can trust their caller ID. In fact, surveys show that more than 70% of people no longer answer their phone at all while 95% indicate that they would answer if they knew it was from a trusted source. It's not just communications service providers (CSPs) that are affected; this has also been damaging to organisations such as banks, insurers and medical providers that rely on voice to reach their customer base.

GM: What is the CSP's role in preserving global trust?

MO: The entire ecosystem, including service providers, is already working collaboratively to solve and close the technical loopholes that exist in order to re-establish trust. The same has happened with text messaging. When it evolved, spoofers sent fraudulent messages that encouraged people to engage in ways they otherwise may have not done, like reset a password for example. In the United States, short codes and toll-free texting emerged as a way to strengthen brand identity and combat fraudster's techniques, particularly as more high-impact use cases emerged, Now, the stakes are higher. This is a global issue with increased complexity involved in both voice and text, especially when considering cross-border communications and the need to reconcile regulations of multiple nations alongside differing policies and approaches of CSPs.

GM: The United States has recently rolled out the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) framework ▶

to help protect the integrity of Caller ID, how does this framework operate and what is iconectiv's role in it?

MO: If you look at what's happening in the US with STIR/SHAKEN and the anti-robocalling legislation, it starts with the establishment of a database where networks have to register to be verified. This robocalling mitigation database enables CSPs to check to see if the originating network is listed before allowing calls to be terminated.

In the US, this is achieved, by implementing a technology whereby a certificate gets passed from the originating network. This, in effect, is a header that states where the call has originated. As of 28 September 2021, CSPs in the US will be required to block a call from anywhere in the world if that call uses US numbering assets and the originating service provider is not listed in the robocall mitigation database. Of course, there are calls to the US originating from outside the country using a US phone number. Brands do this frequently. As of 28 September, ▶

Michael O'Brien
iconectiv

Brands can register their names with their numbers so that consumers know the call is coming from a trusted network as well as which brand is calling

2021, the originating network must be known as the call traverses networks and that originating service provider must be in the robocall mitigation database or face being blocked.

At iconectiv, we are sharing our expertise in enabling trusted, verified communications worldwide. Our experience with STIR/SHAKEN includes being the Secure Telephone Identity Policy Administrator (STI-PA) for the US Calling Number Verification Service, which is an integral part of the STIR/SHAKEN ecosystem. We're also chairing a new GSMA Working Group called Validating INtegrity of End-to-End Signaling (VINES). This group is developing solutions to prevent internetwork signalling fraud, which enables illegal robocalls, spoofing, toll bypass and consumer fraud, with the goal of helping service providers worldwide implement a set of specifications to mitigate fraud, as well as help restore customer trust in caller ID.

GM: It sounds like the US is taking a lead here but this is a global problem so how do you see frameworks like this being adopted globally?

MO: This roll-out in the US, was the first in the world. While the US doesn't face the national fragmentation of a region like Europe, we have more than 1,600 organisations registered with telephony licences. Some of these are very small, and this verification drives cost back into the network. So, we must ensure that even the smallest CSPs can participate. We're starting to see cross-border implementations of robocall mitigation, with the networks playing a pivotal role in building trust at the network layer and how to pass the digital handshake – done via the certificate – along the process

In contrast, there are many more cross-border issues in Europe that will require co-operation between different countries, but domestic implementations will be required first. In other parts of the world, Canada and Australia are not far behind the US in implementation. When cross-border issues are resolved, the next issue is strengthening trust from the brand to the consumer.

GM: How can network trust be extended to re-inforce trust in brands that contact consumers?

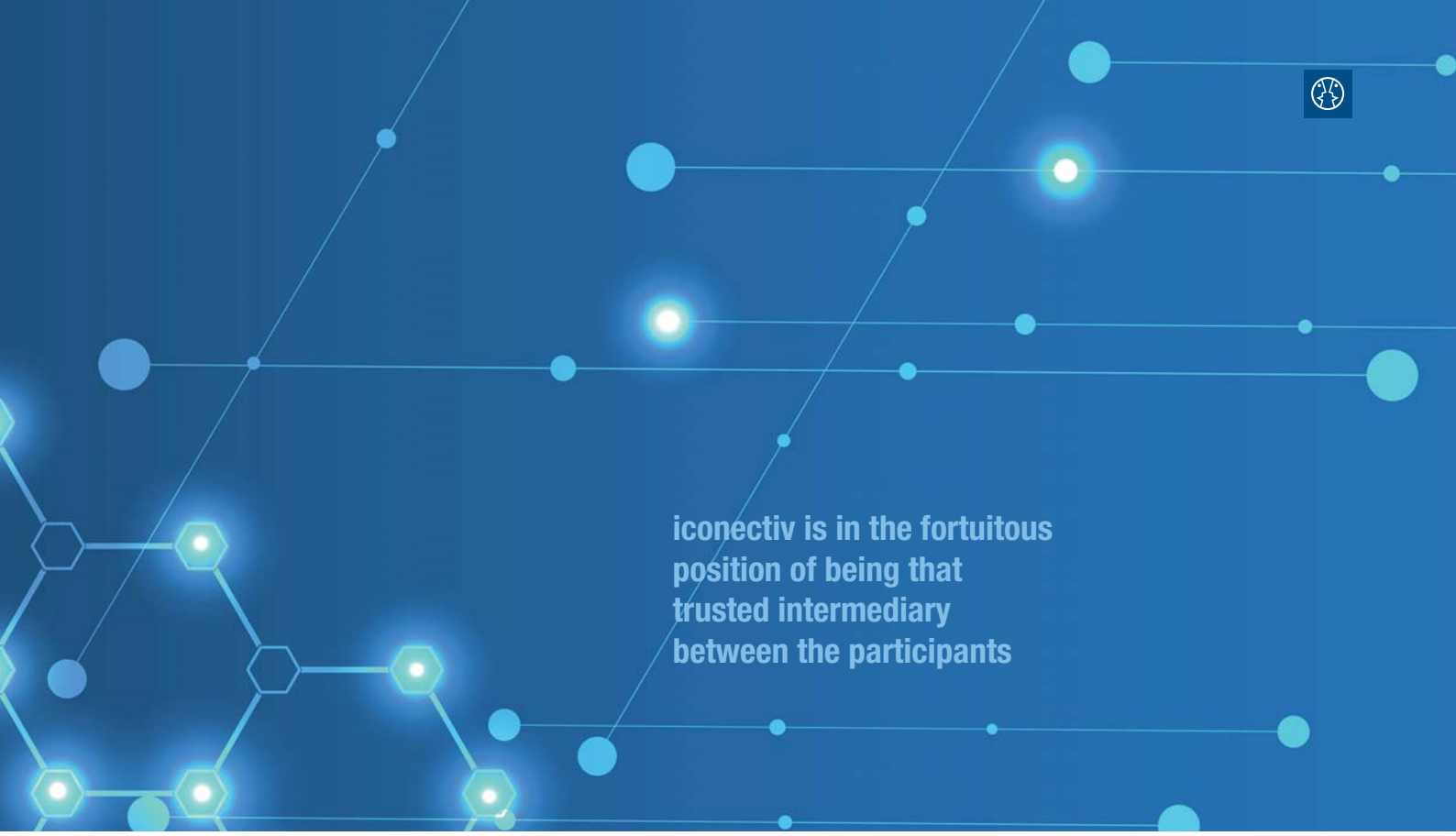
MO: Brands can register their names with their numbers so that consumers know the call is coming from a trusted network as well as which brand is calling. There is tremendous value in knowing a call has been verified, whether it is coming from a bank or a healthcare provider.

GM: We've discussed how trust can be strengthened in voice but what can be done in messaging?

MO: On the messaging side, and especially with the evolution and move toward rich communication services (RCS), there is a growing need to prevent spoofing and fraudulent messaging. Consumer engagement via short codes and toll-free texting, as stated, are an effective first step in traditional messaging because they enable a verified ID for a brand.

RCS has verification and even chatbot verification within it. This will be helpful, particularly when considering that companies like British Airways use chatbots for reservations. The stakes are much higher here, and verification is essential for these types of services.

Messaging, however, relies on an ecosystem of trust between CSPs to ensure that each is fairly remunerated. Identification of fraud has the potential to damage CSPs' reputations in this ecosystem. The CSPs care about protecting their ▶



integrity and the ability to identify and block fraudulent messages.

With the move to RCS, making sure aggregators are verifying the identity of the brands they charge for terminating messages is of great importance because there are significant implications associated with RCS having the ability to execute transactions for conversational commerce.

GM: What are the trends you're seeing in messaging as it relates to erosion of trust?

MO: It runs the gamut, attempts to take over accounts, identify theft, financial fraud. I also think companies are at continued risk with workers using their own phones to conduct business. CSPs are putting processes in place to monetise enterprise messaging more effectively – and charging for termination fees. Brands now must register. We cannot forget that spam is driven by the fact that there is no fee. The impact is tremendous. If sending unsolicited messaging is not free, it could potentially constrict the volume of spam sent.

GM: What steps can brands take to protect themselves and keep commerce flowing?

MO: With voice and messaging, brands should register their identity as a verified communicator so that their customers know they can be trusted. At the same time, brands should remain vigilant and proactively monitor threats. A good example is for a bank to register its brand but also continue to educate customers that it will never ask for a PIN, for example.

GM: I've heard discussions around the idea of self- attestation versus centralised-attestation. Can you talk a bit more about this and explain why it's important for communication providers to consider?

MO: Self-attestation is the idea that people will self-verify they are who they say they are, which may be fine for a consumer phone service where only one-month's revenue is at stake. For brands, however, self-attestation leaves vulnerabilities for incorrectly accepting a verification. The challenge is how to create trust between elements.

It's one thing for someone or some organisation to say, 'Trust me'. But as a call is handed off, the next person must have that same trust. With verified identity, which is part of the mechanism for centralised attestation, everyone can see directly who is verified without needing to trust a third party.

GM: How is iconectiv working across the telecoms industry to help preserve trust?

MO: iconectiv is in the fortuitous position of being that trusted intermediary between the participants. We manage the database of information about how networks interconnect, and we are continuing and extending that work to foster trust in the future.

As the Secure Telephony Identity Policy Administrator (STI-PA) in the US, iconectiv can recognise certified providers for STIR/SHAKEN. We also work with CTIA on a platform called Registered Caller, which allows brands to register their telephone numbers so that the Caller ID shows they are a trusted source.

We're also one of the first RCS verification authorities and we're working with GSMA in the VINES initiative. In general, we're working across the industry to secure cross-border trust in networks and educate people on what is being done. Legislation is a start but it's the implementation of solutions and collaboration across all industry players focused on the same initiatives that makes the difference.

www.iconectiv.com

How to create secure trust in rich business messaging

Unless service providers and brands get verification right – and soon – fraudsters will exploit rich business messaging (RBM) chatbots in the same way they do text messaging and other digital channels

The stakes for conversational commerce continue to rise. With the adoption of rich business messaging (RBM) chatbots, **Juniper Research** estimates online and physical retailers will save US$439m annually in customer service expenses and drive US$112bn in retail sales by 2023. Realising those savings and the increased sales, however, is dependent on one fundamental element: trust.

To establish and maintain consumer trust, the mobile ecosystem is counting on an industry-standard framework that authenticates and verifies the identity of each business that is using rich communication services (RCS) chatbots to engage consumers. That's no easy task considering that RBM is an open ecosystem for businesses of all types and sizes. As a result, huge volumes of business chatbots will be active on each service provider network at any given time.

Even with a framework in place, businesses and service providers have to decide on the best way to verify the identity of a business. Two main options have emerged: self-attestation or centralised attestation.

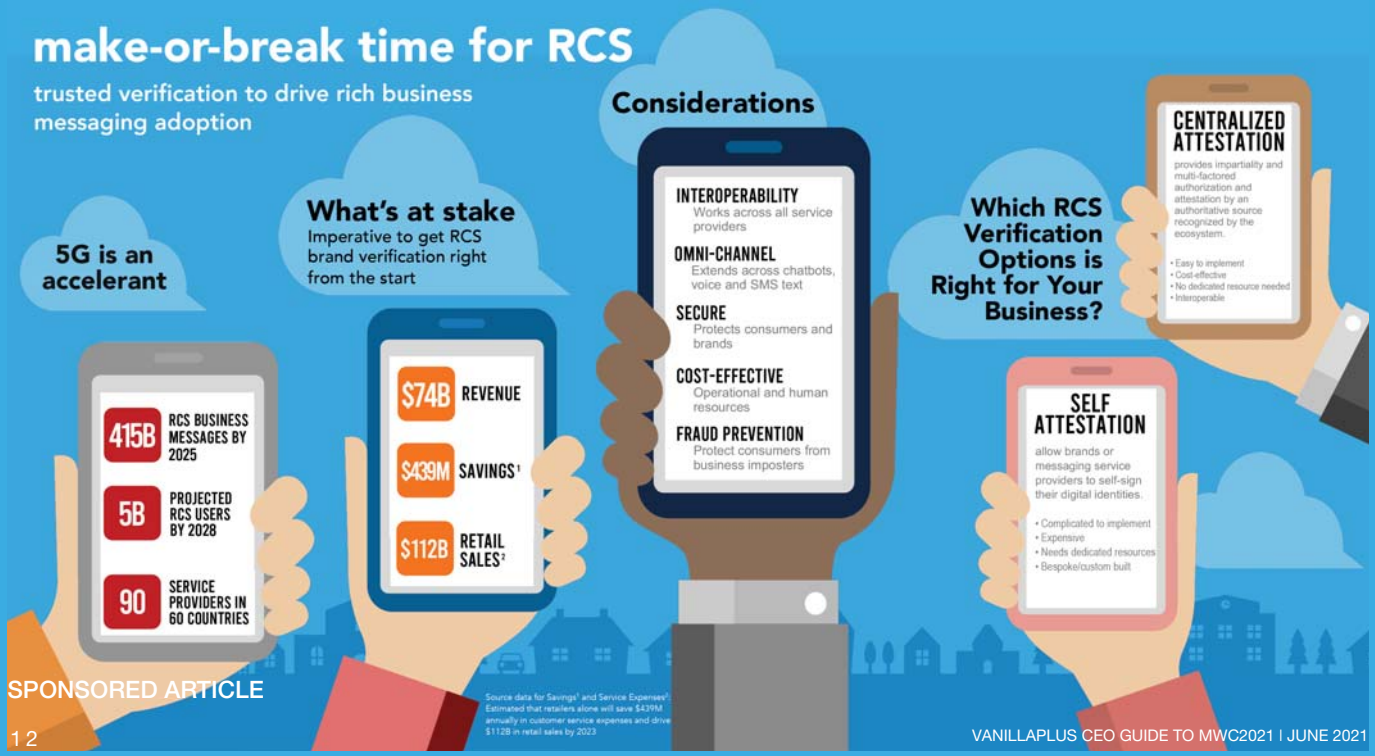
Verification 101

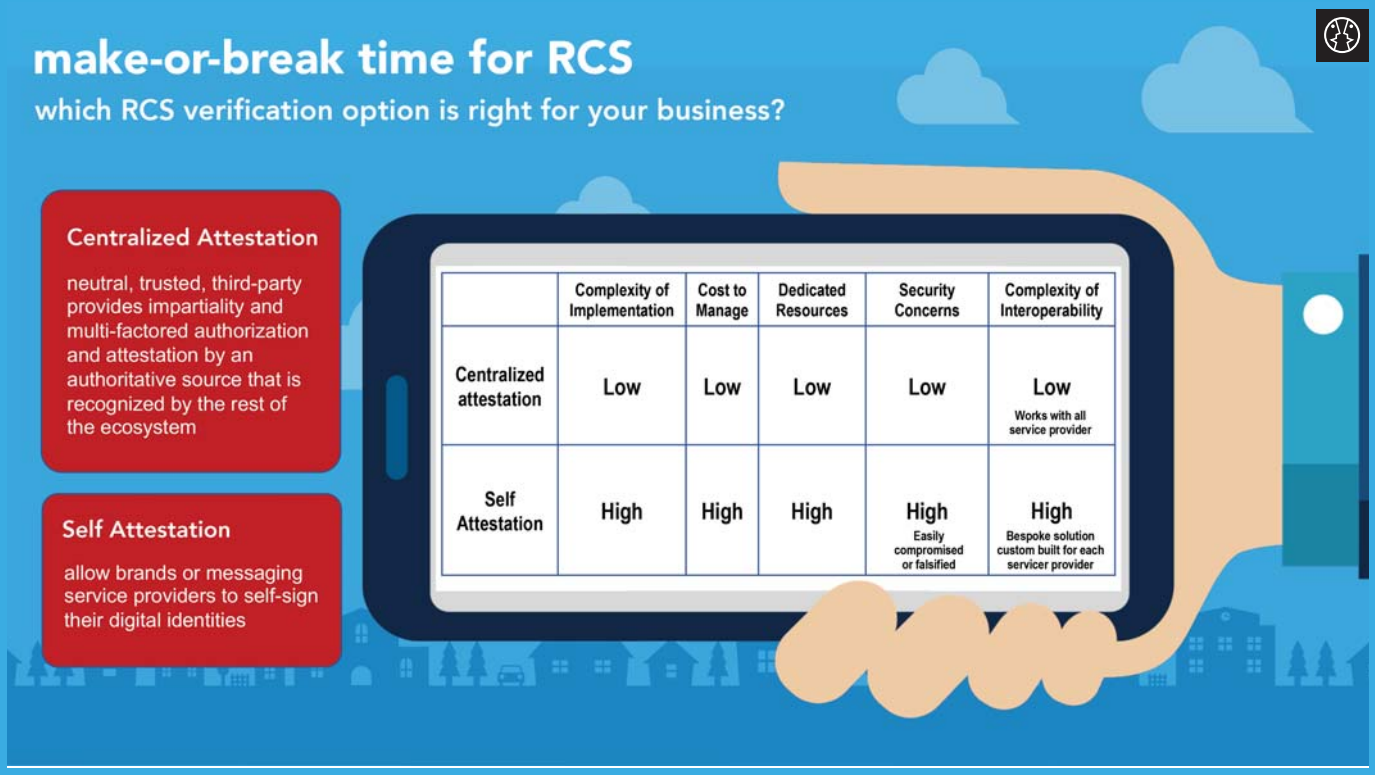
Digital signatures are used in a wide variety of e-commerce, banking, enterprise, government and other applications to verify the identities of people and companies accessing their systems. This proven approach is among the reasons why they're also an ideal way for service providers to verify the trustworthiness of business senders using their communications channels to engage consumers.

A digital signature uses a private key that's decoded against a matching public key, which is linked to a business or other organisation via a digital certificate. These key pairs require participants to invest in a robust public key infrastructure (PKI) policy to secure and scale that mechanism. To use digital signatures for RBM, service providers have two options: They can allow brands or messaging service providers to self-sign their digital identities, each under a unique certificate, or have a neutral, trusted third party sign these digital identities on their own certificate as an attestation of the business' authenticity. Each option has its pros and cons for wireless service providers.

The self-signing model appears to be faster and less expensive to implement but appearances can be deceiving. To accept self-signed certificates used to digitally sign chatbot identities, service providers must implement a system to verify that those businesses are operating under a robust and accepted certificate policy and root of trust before they rely upon those digital signatures. This creates an extraordinarily complex undertaking for the ecosystem, with each service provider potentially operating with a massive number of bespoke PKIs and tens of thousands of participating businesses.

Any initial savings quickly evaporate as RBM interactions scale up, making this bespoke PKI system increasingly expensive to maintain. The ROI is weak because no matter how much a service provider spends on supporting a diverse PKI environment, the system will provide only local verification. The rest of the ecosystem may not accept a self-signed certificate for the same reason no country will accept a traveller with a homemade passport: Neither is backed by an authoritative entity that has thoroughly vetted each user's identity. ▶





Finally, if the private key used for any one self-signer was compromised, it would enable a bad actor to sign a number of fraudulent chatbots. If the root certificate for the signer were compromised, hundreds of falsified certificates could be shared amongst bad actors. That could be a massive setback for consumer trust in RBM. Service providers will invest heavily to manage that vulnerability and are likely to need to pass that cost on to the business senders and their application provider partners.

Centralised attestation

An independent third-party verification authority provides impartiality and multi-factored authorisation and attestation by an authoritative source that is recognised by the rest of the ecosystem. A verification authority reduces fraud risk by providing a neutral set of eyes to validate a brand and its authorised chatbots. It provides the kind of comprehensive protection that each wireless service provider cannot necessarily achieve with internal checks and balances in a model with self-signing by business senders. For example, a verification authority has the resources necessary to identify fraudsters masquerading as brands that a service provider already works with.

With absent centralised verification, a service provider may inadvertently onboard some of those imposters, especially as RBM's popularity grows, leading to a growing number of nefarious new chatbot requests entering the ecosystem. A Verification Authority is much better suited to accommodate the necessary security, at scale.

GSMA's RCS Verified Sender initiative is an industry effort to ensure that RBM avoids the spoofing and other fraud types that afflict SMS. It establishes trust in business-to-consumer messaging by providing a framework that verifies the business sender's identity. RCS Verified Sender includes an independent Verification Authority that would be responsible for authenticating the identity of businesses. The Verification Authority would also verify the chatbots used by the business and would register the information in a system that shares the business's logos and other enhanced sender ID information with each participating platform provider.

This information would be digitally signed by the verification authority, which will help mitigate the risk of spoofing or impersonation of chatbots by fraudsters. Verified sender content could then be presented to the consumer with an icon, such as a trust mark, to further emphasise that the sender has been verified. The service provider would also deliver this information with the sender's business name and logo so recipients could feel more confident that the business is legitimate and that the content is authentic while, in parallel, business senders can rely on brand loyalty.

iconectiv TruReach Intel

iconectiv is helping lead the GSMA Verified Sender initiative. This role includes numerous contributions to GSMA industry specifications and related documents based on providing decades of expertise in helping service providers and businesses with tools for ensuring consumer trust in other forms of communications, including voice calls and application-to-person (A2P) SMS.

iconectiv TruReach Intel provides Verification Authority services, as well as a variety of additional tools to help the RBM ecosystem manage verification at scale. It's a neutral and secure service that helps distinguish those business messages that are coming from verified senders. Those messages can then be presented to consumers as legitimate and authenticated. The solution is very efficient for business senders connecting to numerous service providers.

Service providers can use this software as a service (SaaS) solution to allow businesses access to their networks where messages and chatbots from legitimate businesses can be authenticated and verified. TruReach Intel also supports voice calls and SMS, making it a comprehensive solution for building and maintaining consumer trust with omnichannel engagement.

Messaging application chatbot spoofing, SMS phishing (smishing), email spearfishing and illegal robocalling all show that consumer trust is hard to win and easily lost. History also shows that for every technology, fraudsters always find new loopholes to exploit. The most effective response is an industry-wide, collaborative and continually vigilant effort designed to make it as difficult as possible for fraud to occur.

As a new technology, RBM has a unique opportunity to build a technological and business-process foundation to minimise vulnerabilities from the outset. By utilising a centralised verification authority as the foundation for ensuring trust in RBM communications, the ecosystem can protect consumers, legitimate businesses and the RCS market opportunity.

www.iconectiv.com

MWC Barcelona returns as the industry's key sounding board

Mobile World Congress (MWC) in Barcelona returns on 28 June and runs until 1 July. This guide from communications journalist Antony Savvas outlines what attendees can expect on arrival, and remotely for those attending virtually for the first time

Tony Savvas

After last year's event was cancelled completely as a result of the pandemic, the telecoms industry will be all eyes on this year's effort. MWC in Barcelona is usually the biggest mobile industry conference and exhibition in the European calendar. In 2019, according to show organiser GSMA, there were 109,000 attendees. The figures will be well down this year – see below – but those backing a return to a new normal have to start somewhere.

The Spanish government is allowing MWC21 Barcelona registrants into the country to attend the show. This decision allows entry to those registrants who were previously denied entry – including those from China and the US – to do business at MWC21. After registration, event organiser GSMA will provide relevant information to the Spanish government for visa and border control purposes. ▶

Attendees can use their MWC Barcelona 2021 attendance confirmation when contacting their consulate or visa issuing authority.

Health and safety

The show health and safety plan covers everyone involved with the event, including staff, exhibitors, visitors, suppliers, partners and the local community. The plan includes frequent testing, contact tracing, touchless environments, re-vamped catering, occupancy monitoring and increased medical staff.

John Hoffman, CEO of the GSMA, said: “MWC21 Barcelona can go ahead safely in-person, with a digital online component for those unable to attend. It will remain the unique, unmissable experience that has made it the world's most important telecoms event.”

To get into the show attendees have to download the My MWC app. It is a digital badge that will activate once registration, a daily health self-declaration and three-day negative testing is completed. Some travellers will be required to show a negative Covid-19 test before being allowed to board planes to Spain. These test results can be uploaded to the show app. Participants arriving by train or car will be directed to MWC testing centres to validate their health status, with results uploaded to the show app.

All participants will be required to produce a valid negative rapid test [lateral flow test] to access the venue. The test must be repeated every 72 hours, with participants notified through the My MWC app of upcoming testing requirements – those not having an up-to-date negative test will not be allowed entry.

The price of a rapid test at the testing centres is €15. PCR tests for €85 are being offered to attendees that need one to return home, for instance.

At the venue temperature checks will be conducted at all access points. Entrances and exits have been doubled in size to ensure social distancing and to support one-way traffic flow through the venue.

Only contactless payments can be made at conference restaurants and the venue features a new fresh-air injection ventilation system to improve airflow. Attendees will be required to wear masks.

Virtual visitors

MWC21 Barcelona will be a hybrid event for the first time. Online, pass holders will be able to explore virtual exhibitions and network via video – before, during and after the show. Keynote speeches, conference sessions, partner ▶

All participants will be required to produce a valid negative rapid test to access the venue

GSMA estimates 35,000-plus people from Spain and around the world will attend

"With much of the world gradually emerging from the Covid-19 crisis, now is the moment to reflect on policies that support digital connectivity, innovation and, critically, economic recovery,"

programmes and summits will be live-streamed and available on-demand. The show portal enables attendees to interact with each other in real-time.

GSMA "estimates 35,000-plus people from Spain and around the world will attend" in person. "We expect thousands more to join us online," it added.

That compares with the 25,000 in-person and virtual attendees at the MWC Shanghai event this February, with most of the in-person attendees from China. The online portal at this event made up "approximately 30% of attendee turnout", said GSMA.

In Barcelona, GSMA says there will be "over 300 exhibitor stands, over 300 4YFN exhibitors [see below] and 300 sponsors both physically and virtually".

Highlights

The theme of this year's event is Connected Impact. The programme will explore how artificial intelligence (AI), 5G, big data and IoT will "shape the future and continue to transform lives". MWC21 includes leading keynote speakers, the Ministerial Programme, start-up innovation at 4YFN and the Diversity4Tech Summit.

There are more than 600 scheduled keynote and conference speakers. These include:

Julie Sweet, CEO of **Accenture**; Shuky Sheffer, CEO of **Amdocs**; Yang Jie, chairman of **China Mobile**; Arvind Krishna, CEO of **IBM**; Sarah Wilkinson, CEO of **NHS Digital**; Stéphane Richard, chief executive and chairman of **Orange**; Mathew Oommen, CEO of **Reliance Jio**; Anne Boden, CEO of **Starling Bank**; Danielle Royston, CEO of **TelcoDR**; Hans Vestberg, chairman and CEO of **Verizon**; Raffaele Annecchino, president and CEO of **Viacom Networks International** and Xu Ziyang, executive director and president at **ZTE**.

Around 70% of all speakers will be at the event itself, while the rest will be virtual.

Diversity

GSMA is partnering with Accenture to deliver the Diversity4Tech programme. It aims to "expand conversations to include the indisputable case for diversity and inclusion in business". The Summit includes talks, panels and awards to "create a unique opportunity to influence and accelerate the change needed", said Accenture.

Policy

The GSMA Ministerial Programme will convene policymakers to discuss digital inclusion, network resilience and maximising the potential of 5G, hosting dozens of delegations from around the world.

"With much of the world gradually emerging from the Covid-19 crisis, now is the moment to reflect on policies that support digital connectivity, innovation and, critically, economic recovery," said John Giusti, chief regulatory officer at GSMA.

"The Ministerial Programme always delivers timely, meaningful dialogue and debate – and we are glad to be back," said Giusti.

Start-ups

More than 300 international start-ups will exhibit their latest products within the Innovation Market and 150 speakers will share insights that aim to drive the ecosystem forward. In the 4YFN Discovery Area, 200 start-ups will pitch, hoping to attract the attention of leading venture capital firms.

New this year, the Investors Programme features a summit dedicated to knowledge-sharing among the investor community.

Sponsors and partners

Sponsors and partners include **Accenture**, **Airship**, **Amplitude Analytics**, **Citi**, **DAMM**, **Dell**, **Gazprom** ▶

Space Systems, **Huawei**, **Kaspersky Lab**, **NVIDIA**, **Orange**, **Red Hat**, **Shenzen Royole Technologies**, **Sony**, **STC**, **Tata Consultancy Services**, **TelcoDR**, **Thales DIS France** and **ZTE**.

Microsoft is the official video conferencing partner, providing its Teams platform to support virtual events.

Partner events are supported by the likes of **AECC**, **AWS, Braze**, **Cisco**, **Facebook**, **GTI**, **HERE**, **Huawei**, **IBM**, **iconectiv**, **Infineon**, **Intel**, **ITRI, Kigen**, **KORE**, **Lenovo**, **Marvell**, **Oracle**, **Orange**, **Palo Alto Networks, Red Hat**, **Samsung**, **ServiceNow**, **Snapchat**, **uCloudlink**, **Vodafone** and **Xilinx**.

One of the above companies sees the show as a key way to help address some of the data security problems the communications industry is facing. "The foundation for trusted communications and consumer engagement is eroding with the increase in illegal robocalls, smishing, wangiri and other fraud," said Richard Jacowleff, CEO of iconectiv.

"People simply want to be able to securely answer their phones again," said Jacowleff. "As industry stewards we need to make that happen, and not just to remedy the problems of today, but to fortify the communications infrastructure of tomorrow."

He said: "As the largest telecoms event in the world, MWC provides a global stage where iconectiv and its partners can showcase industry-backed solutions like STIR/SHAKEN, Verified Sender and Registered Caller – that are helping legitimate businesses and customers communicate with confidence."

Another company that will be taking part is **Beyond by BearingPoint**. Angus Ward, the chief executive, said: "At MWC Barcelona we look forward to reuniting with our industry peers. Despite the pandemic's disruption, the event is still the largest and most influential event in the mobile and telecoms calendar. We're keen to showcase the innovative work our team is doing and to involve ourselves in key industry conversations as the operator and vendor communities take advantage of technologies around the edge, IoT, AI and 5G."

Ward's company is presenting a keynote in Barcelona and he is moderating two sessions. He said: "We'll be aiming to address the need for CSPs to go beyond connectivity to capitalise on the rich revenue opportunities created by new technology. We'll be outlining the partnership imperative and underlining why partner ecosystems are so critical for the co-creation of attractive joint technology solutions."

"Ultimately, this brings CSPs and their ecosystem partners closer to their customers, helping them to generate revenue, drive efficiency and become more agile in the face of competition," added Ward.

And that's something everyone in the industry can get behind!

VanillaPlus and sister communications brand IoT Now are media partners for the event.

Angus Ward,
Beyond by BearingPoint

Co-creation and co-innovation drive CSP opportunities to re-invent their business models for the 5G era

With IoT established, the next shift facing communications service providers (CSPs) is the emergence of 5G into market reality. It's still early days but significant opportunities to re-invent telecoms business models and enter a new market of increased openness and collaboration are beginning to crystallise. Angus Ward, the chief executive of Beyond by BearingPoint, tells George Malim, the managing editor of VanillaPlus, that there are multiple dimensions to the opportunities presented by 5G, IoT and edge, but it won't necessarily be traditional CSPs that are best placed to capitalise on them or to extend into these adjacent markets. However, for those CSPs that can transform organisationally as well as technologically, new revenues will come with new models and new relationships across a far larger connectivity-enabled ecosystem

George Malim: 5G, IoT and Edge have been discussed for many years as enablers for CSPs to widen their offerings and generate new revenues by going beyond connectivity. Do you see this as a realistic prospect?

Angus Ward: It varies hugely. 5G is a new technology and how it plays out is what we're thinking about now. IoT is a more mature technology and has been around for a few years and therefore with edge, 5G is enabling the next lifecycle iteration. IoT is here as a market, you can assess it and understand who's doing what, it's very clear that there are opportunities to monetise using sensors, artificial intelligence (AI) and everything else at the edge. On the other hand, 5G is brand new so the business potential is less well defined today. ▶

The different markets and players also influence how each is being approached. If you look at the research published after March's telecoms industry analyst days, for example, there are some interesting insights. **Vodafone** Business mentioned IoT 54 times, cloud 45 times and security 49 times. That gives you a statement of intent if you compare that to **AT&T**, **T-Mobile** and **Verizon**. These CSPs' analyst days gave far less prominence to the new areas but were focused more on connectivity and talking strongly about 5G.

GM: CSP salespeople don't really have a track record of grasping every opportunity that comes their way. We've seen mobile content and messaging where they've been able to turn new opportunities into a significant business for themselves and others have taken advantage. So what's going to be different with 5G, IoT and edge in terms of how CSPs could play themselves into being more than just connectivity providers?

AW: The issue with what you just said is that those examples are very much B2C focused. This is where start-ups in Palo Alto massively scaled up using private equity cash and grew exponentially, which is quite different to the 5G and IoT B2B opportunity. With 5G, you're talking about enterprise or an SMB play and CIOs, who want to transform their operations, whether it's manufacturing, logistics or freight. They are worried about cyber security and ransomware attacks. They have very large mission critical operations with opportunities to accelerate, massively scale and take costs out. I had a conversation with the deputy CEO of Siemens last year, and he said approximately 60% of manufacturing processes were capable of being automated, which are not automated today. I think, what is different with 5G is it's the first generation of mobile technology where the benefits are primarily in the enterprise and SMB space. This massive scale with all the security concerns are better suited to large providers, such as CSPs and less suited to start-ups in college dorms.

GM: Do you think that the corporate relationships CSPs have are going to be a strength because if a CSP has been trusted to deliver the network for a manufacturing company, it's not that much of a leap to sell them a private 5G network, and then maybe adjacent services and offerings?

AW: The question is how quickly can you move into those adjacent markets? With Vodafone and IoT they've made acquisitions and are quite willing to commit capital and to aggregate solutions and revenues in IoT. I think the question then is how successful can they be? We are seeing this move towards technology communications by Vodafone with the carve out of its TechCo, BT with its DigiCo, the data services focus of **Telefónica** and **Telia**'s Division X, as great examples. These are journeys where CSPs are starting to navigate the organisational change required and learning how to join everything up so it's much easier for the customer to navigate and self-serve. The key thing is CSPs need to target being an aggregator and not a systems integrator, a path unsuited to many of them.

Historically, in all the B2C examples, you start off with the customer and a deep understanding of the problem they're trying to solve. They organise in a way that best suits their customer. So success here is really about the ability to get close to customers, understand their problems and be willing to co-create and co-innovate to develop a perfect solution that is easy to try, buy and consume out-of-the-box. Open innovation means bringing in partners who bring complementary capabilities, who can take the journey on that co-creation, to create that perfect solution for the customer. That's a very, very different way of looking at the world. CSPs have traditionally been organised in a way which best suits how they want to offer things to the market, to centralise control and minimise risk. This means selling horizontal products needing lengthy and costly integration by the customer to create a usable solution. It means CSPs don't get to understand customer needs.

The ability to rapidly innovate solutions for a customer means empowering teams and delegating responsibility to those people who are facing the customer to bring together whatever capabilities are necessary in order to solve the customer problem. Again, the aim is to be aggregator and not system integrator. This together with finding a different way to work with partners to find the win/win and not putting them through the mill of centralised and adversarial procurement are fundamental and a different way of organising. I think these are key challenges facing CSPs as they target adjacent offerings beyond connectivity.

GM: How big a shift is the concept of openness in telecoms? Open RAN and the multi-vendor world plus the need to offer open application programme interfaces (APIs) are alien to the traditionally closed telecoms environment so how far do you think CSPs will go when it comes to opening up?

AW: I think that what's happening within the telecoms industry is that while there's an opportunity in going beyond connectivity, there's also a threat. The traditional connectivity business is being unbundled in the same way as every traditional industry. If you think about payment services like **PayPal** or **Stripe**, they have attacked one part of the banking value chain. The switch from physical to virtual assets within the network allows pieces of the telecoms value chain to be targeted by software specialists who say: "We're going to be amazing at that one piece". ▶

The different markets and players also influence how each is being approached

The very best companies in digital run solution and business model innovation as two sides of the same coin

As the telecoms value chain beyond the pipe is more software-oriented so the question is whether, in the virtualisation of all those functions, will they go to the CSP to offer those functions or will some of the big webscale providers and tech companies take parts of their market? Dell's recent announcement that it is going into the open RAN space, with ecosystems and partnerships with the likes of Intel, saying that they will be a US-based open RAN provider illustrates this trend. All this innovation is great for the customer, but if it's not the CSP providing the customer with the overall solution, then the provider may choose to just buy the pipe.

I think this major trend to unbundle is rapidly extending into traditional telecoms services with sale of their towers business but also with all the virtual functions, security, and everything else. I've described the choice they now face as the Amazon versus AWS strategy. AWS sells components to solution providers who own the customer relationship and create the perfect solution whilst Amazon really wants to own the customer relationship and using its digital platform, bring in the right partner organisations to solve whatever problem the customer has. I think the paradigm here is really an existential question of whether CSPs serve customers and own the customer relationship. Or if they want to sell connectivity components to solution providers who will create the solutions on behalf of the customer via new solution providers which will choose the best virtual software components in order to provide the best possible solution?

The question is, who is the solution provider? It might be a systems integrator, network equipment manufacturer, one of the big IT wholesalers, a tech or an industry specialist. So, each one may want something different from the CSP and to a greater or lesser extent unbundle connectivity.

GM: How do you see the digital platform business model developing?

AW: The very best companies in digital run solution and business model innovation as two sides of the same coin. If you look at the really simple example of mobile messaging apps. They offer pretty much the same product as the CSPs in terms of voice and texts, but their market is growing by 10% CAGR because they're offering the service free of charge by monetising consumer

data. Conversely, CSPs are facing a flat or declining market for the same two services. The only difference is business model.

This is where digital business platforms come in. Traditional IT presupposes traditional business models and a linear supply chain. Linear means they have to be a systems integrator. Platforms are critically important to both solution and business model innovation because they supported any number of new business models and a multi-sided value chain where the roles of producer, provider and customer are flexible –such as in B2B2B2C models. The ability to co-innovate with an ecosystem is essential to create, offer, sell and monetise the perfect solution. A platform enables the much easier aggregator role – avoiding having to become a systems integrator – and bringing in end-to-end automation and repeatability with the ability for customers to self-serve, sets them up for commercial success in delivering multi-partner solutions.

I think platforms are the most powerful weapon to be successful in this new world of 5G and solutions. Many CSPs are using AppStores or BSS to resell widely available third-party products for a 5% margin. This is fundamentally different from using a platform to aggregate the orchestration and monetisation of multi-partner cloud-based solutions for a 40-55% margin. You are doing it for the entire ecosystem on a multi-country basis if required. It's very hard to educate yourself in this space because in software everyone claims they can do everything, but multi-partner platforms are fundamentally different.

GM: What is Beyond by BearingPoint's role here? How do you approach the market and what developments are you participating in?

AW: We saw this move to platform-based business models really early on, back in 2014 and for six or seven years we've really got inside how to make them work for CSPs. We understand business model change, we understand organisational change, we understand all the agile cooperation and co-innovation that are key to building successful partner ecosystems. We understand also what role CSPs want to play as an orchestrator. We have built up a lot of experience around how to do this, how to rapidly co-create and test new solutions with customers, the technology side and how to help large organisations navigate the pathway to success. It's not an easy change for CSPs but we have so many learnings of how to make it successful.

We also identified that their current IT is not fit for purpose and cannot support new business models and co-creation, as well as the sale and monetisation of new solutions with partners.

Therefore, we developed our Infonova Digital Business Platform and an advanced Digital Marketplace enabling CSPs, customers and any number of partners to take part in this new evolving ecosystem and experiment, co-create and deliver new solutions quicker and easier.

CSPs typically want to start the journey, which means starting off with the right partners. Launching new solutions in weeks. Earning new revenues really fast. People don't want to spend huge amounts of money and wait 12 months; they want to do something really quick and experiment. Using cloud native software-as-a-service (SaaS), open APIs and an agile approach to minimum viable product (MVP) with our Infonova Platform aggregating partner capabilities, this enables rapid delivery.

5G is something very new and exciting and it is just happening now. The open RAN conversations on applications and marketplaces are happening now. In IoT, you can go out there and see who's big and who's doing what and they've been doing it for three or four years and you can see their revenues.

CSPs have been heavily stovepiped and then broken into OpCo with minimal cross fertilisation. There is huge potential to cut costs across every dimension – function, business, product line and geography. The key thing is not to wait until 5G is rolled out in standalone mode but really to execute on your 5G product strategy now to build the solutions, ecosystems, in-house capabilities and organisational structures and ways of aggregating you need for success. We can help CSPs see the opportunity to start that journey now by overlaying our Infonova platform across the current fragmented internal and partner landscape with almost no impact on the day-to-day.

I think people are really starting to think about that and the problem of how to start to build their 5G solution portfolio with partners, whilst in 5G non-standalone mode. The challenge is how do you actually advance your portfolio now and start getting maturity in terms of your offerings for enterprises and SMBs now.

Beyond by BearingPoint addresses this challenge using our Infonova Digital Business Platform. We bring more experience and know-how than others. Quite simply because we are much broader than just the technology. In understanding that platforms and aggregation is a genuine paradigm shift, we were the first in the market to recognise this and to redefine our mission to help CSPs realise the enormous opportunity this presents. Particularly now in a 5G and connected solution world.

Angus Ward is speaking at MWC2021. He will be presenting at the Delivering Scalability Through Partnerships session at 1300-1400CEST on Monday 28 June and he will be session moderator of End-User Showcase to be held at 1200-1245CEST on Thursday 1 July.

I think platforms are the most powerful weapon to be successful in this new world of 5G and solutions

www.bearingpointbeyond.com

the trust factor

70% of global consumers say trusting a brand is more important today than in the past.

Your business and your customers need to access and exchange information simply, seamlessly and securely. This in no easy task considering that the misuse and abuse of communication networks is a global epidemic resulting in €1.5B lost annually due to fraudulent activities that are eroding that trust.

Trusted Voice | Text | Messaging | Chatbots

Let iconectiv help you keep people connected, businesses running and commerce flowing.

iconectiv sales@iconectiv.com 1 +732-699-6800 click for details iconectiv.com