White Paper

HardenStance

5G Roaming Drives Security by Redesign

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

February 2022

Executive Summary

- GSMA has finished specifying the first three use cases for 5G SA roaming, affirming the choice of TLS for protecting 5G interconnection traffic rather than PRINS.
- Decisions on the role of 3rd party intermediaries in more complex 5G SA roaming use cases have been deferred. The trade-offs GSMA makes between security and efficiency here will determine what 'Security by Design' looks like for 5G roaming.
- As well as preparing a 'Great Leap Forward' with 5G SA, mobile operators and their customers expect to rely heavily on legacy 2G, 3G and 4G as well as 5G NSA for the next 5 - 10 years. Better security is required for these roaming services too.

Across hundreds of nation state jurisdictions all over the world, different politicians, regulators, citizens, businesses and interest groups strike very different balances between security, privacy, operational efficiency and scalability.

Individuals are Exposed to a Variety of Attackers

The fixed and mobile networks as well as the services, applications and data we use, and the devices we use to access them, are all vulnerable to being disrupted, corrupted, spied on, stolen or otherwise abused by third parties. These different parties comprise those that are authorised to act as they do as well as those that act illegally.

For the sake of simplicity, these different actors that either do, or potentially could, exploit telecom network vulnerabilities to harm us can be categorized as follows:

- Home nation states (law enforcement and intelligence agencies of the country or countries of which we are registered nationals and/or where we live) via their privileged access to telecom networks.
- Foreign nation states via their privileged access to telecom networks.
- Cyber criminals, online fraudsters and politically motivated hacktivists.
- An entire ecosystem of online businesses monitoring, aggregating, correlating and predicting our personal behaviours – much of it legal, much of it without our consent – according to what has been dubbed the modern "surveillance economy."
- Individuals, either known to us or not, who are personally motivated to harm us.

The Challenge of Optimal Trade-Offs with End-to-End Encryption

The telecom sector's challenge of reconciling national security and law enforcement with privacy and business efficiency objectives for 5G roaming is a small subset of the broader challenge societies face in determining how end-to-end encryption is used. In the years following the September 11th 2001 attacks, U.S. intelligence agencies invested in a huge programme of mass surveillance that was justified in terms of national security - protecting citizens from terrorism. The years following the 2011 'Snowden Revelations' that disclosed this activity have seen a marked reaction against this and in favour of greater protection of privacy against excessive surveillance by the state. This has shown itself in the rapid growth of application encryption, including by businesses and leading messaging providers, as well as in new data protection laws like the EU's General Data Protection Regulation (GDPR).

In western-leaning liberal democracies, the trade - offs between national security and law enforcement, privacy and efficiency remain highly contentious. Hopes for a better balance rest on a viable technological breakthrough somehow allowing law enforcement access to a subset of encrypted information without compromising user privacy indiscriminately - and without being attainable by unauthorized third parties. This is a huge challenge. The search for a solution that commands widespread support among key stakeholders, and with a high level of efficiency, is generally not expected to yield anything of great value in the near term. 3GPP and GSMA are similarly charged with finding the right balance in the unique environment of 5G roaming.

Across hundreds of nation state jurisdictions all over the world, different politicians, regulators, citizens, businesses and interest groups strike very different balances between national security and privacy in the way they allow online products and services to be created, deployed and consumed. Efficiency is a third critical consideration. It mandates that whatever the chosen trade-off between national security and privacy goals, they must be achievable by operating models that are efficient, affordable and secure.

In line with the conditions of their operating license, telecom operators occupy a unique and critical role in enforcing the chosen trade-off that is mandated by the state that licences them. Most commonly, telcos are required by law to protect the privacy of customer information in transit via network layer encryption. The only exception is where national security or law enforcement agencies determine that a specific individual's privacy must be compromised via Lawful Intercept (LI).

Authoritarian governments routinely require their telcos to help them spy on customers at home and while roaming abroad, as well as on visiting citizens from other countries.

Trade-Offs Between National Security and Privacy are Hotly Contested

As described at the bottom of page 2 this trade-off often does not remain settled for very long. Moreover it can differ enormously between regions and countries. Authoritarian governments routinely require their telcos to help them spy on customers at home and while roaming abroad, as well as on visiting citizens from other countries, including by exploiting vulnerabilities in mobile roaming signaling. They do that according to criteria that often far exceed more democratic countries' definitions of national security.

Some examples of how mobile networks are used by threat actors - including nation states - to spy on individuals are shown below:

- In July 2021 the Pegasus Project revealed abuse of smartphone spyware by several governments targeting political rivals, activists and journalists, in violation of their original licence terms. By highlighting the high profile NSO Group that develops the Pegasus spyware, the research nevertheless understated the scale of the ecosystem of many businesses selling and supporting the operation of such spyware products.
- Nation states also regularly exploit signaling vulnerabilities in 2G, 3G and 4G networks, for example to undertake reconnaissance on other telecom networks or track the location of target individuals at home as well as when roaming on foreign networks. Cyber criminals and individuals do this too. Where they don't have expertise in SS7 and Diameter themselves, they just hire grey market actors to design custom attacks for them as a service.

The Telecom Sector's Efforts to Secure Roaming with 5G SA

This White Paper assesses the telecom sector's efforts to enhance security in the global mobile roaming ecosystem in the context of these threats. It takes account of the nature of the mobile operator and mobile roaming business models. These are far more dependent on globally synchronized technical coordination and interoperability with peers than any other segment of the telecom sector, let alone the broader high tech sector. They are also characterised by the expectations of both mobile operators and consumers that each generation of mobile networks and devices should be in service for at least twenty five years rather than scrapped soon after the latest 'G' is rolled out.

In particular this White Paper assesses the following:

- The setback to the mobile industry's goal of enabling a 'great leap forward' in roaming security via the newest generation of 5G Standalone (5G SA) networks.
- The work of the GSMA's 5G Mobile Roaming Revisited (5GMRR) Task Force to get the detailed specification work on 5G SA roaming security back on track, albeit according to a less ambitious schedule than envisaged at the time of the completion of the first 5G specifications by 3GPP.

- The urgency of taking steps to add better security to the roaming infrastructure used for current 2G, 3G, 4G and 5G Non-Standalone (NSA) roaming. As can be extrapolated from the dedicated NSA and SA Variants of 5G' text box at the bottom of page 4, this current roaming infrastructure will continue carrying the majority of all mobile roaming traffic for the next 5 - 10 years.

Well-Known Vulnerabilities in the Legacy Roaming Model

While many other aspects of mobile security have kept pace with increased cyber threats, inherent vulnerabilities in the way mobile roaming relationships between operators are managed have remained largely unchanged for thirty years.

- 3GPP standards for 2G, 3G and 4G inherently trust a mobile operator's roaming partners. Even in 4G, signaling traffic between mobile operators on the S6a interface is still sent in the clear (unencrypted).
- Although many have, a lot of mobile operators have still not deployed GSMA-recommended signaling firewalls to counter the above vulnerability and block malicious messages such as those originating from 4G's S6a interface.

It's precisely the exchange of control plane messages between mobile operators in the clear that enables a large ecosystem of third party roaming intermediaries.

These well-known vulnerabilities in the interconnect regime are arguably the weakest security link in legacy 3GPP standards. They serve as a back door that allows cyber criminals and authoritarian governments from around the world to carry out cyber and physical world attacks on an operator's customers.

That said, while foregoing any encryption on the 4G's S6a interconnect interface is a major privacy and security flaw, the upside is that it has served telecom operators very well in terms of efficient business operations. Specifically, its precisely the exchange of control plane messages between mobile operators in the clear that has enabled a large ecosystem of third party roaming intermediaries to participate in the roaming infrastructure ecosystem over the last 30 years.

Mobile Roaming Intermediaries Strip Out a Lot of Cost and Complexity

As a result of being able to view and modify the control plane messages in roaming interactions between the world's 800 or so mobile operators, roaming intermediaries offer them one-to-many roaming relationships with one another that drive a lot of the operators' cost out of providing roaming services. It's thanks to these third parties that most mobile operators manage to have no more than a couple of dozen direct or bilateral roaming arrangements with their peers.

NSA and SA Variants of 5G and the Delayed Rollout of 5G Roaming

The current Non-Standalone (NSA) variant of 5G is commercially mature, the newer Stand Alone (SA) variant is not. The quite widely deployed 5G NSA, first launched in April 2019, uses 5G New Radio (5G NR) and re-uses the 4G core network. The newer 5G SA, featuring the new 5G Core (5GC), is still in its commercial infancy with hardly any networks launched as a commercial service.

5G roaming accounts for a small share of total roaming today. The limited 5G NSA roaming agreements in place reuse the existing 4G core and existing roaming infrastructure. The currently available NSA variant of 5G roaming is still in its infancy. Hence, whereas hundreds of operators support 2G, 3G and 4G roaming with hundreds of other operators, relatively few have a large number of 5G NSA roaming agreements with one another yet.

The first 5G SA roaming services are not expected until the end of 2022 at the earliest. As domestic roll-out of 5G SA networks is still only in its infancy, there is unlikely to be any requirement to start rolling out roaming agreements between 5G SA networks or between 5G SA and 4G networks at scale much before 2024.

The vast majority of roaming relationships – which together, account for a small share of total global roaming traffic – are realised through partnerships with one or more roaming intermediaries. Three types of roaming intermediary can be defined, albeit there is often some overlap between them with some providers playing in two or even all three market spaces.

- **IPX Carriers** – providers of premium IP routing, managed QoS interconnection services and other value added services such as signaling firewall filtering. These comprise the wholesale provider businesses of some of the larger telecom operators themselves as well as independent players.
- **Roaming Hubs** – one-to-many aggregators and connectivity providers that effectively serve as the equivalent of a network operator, albeit they are not licensed telecom operators. They manage core roaming functions between operators like testing, signaling, firewall filtering, service monitoring, incident management, billing and financial settlement
- **Roaming Value Added Service (RVAS) Providers** – providers of value added services like traffic steering and SMS campaign management.

The 'Great Leap Forward' Envisaged with 5G SA

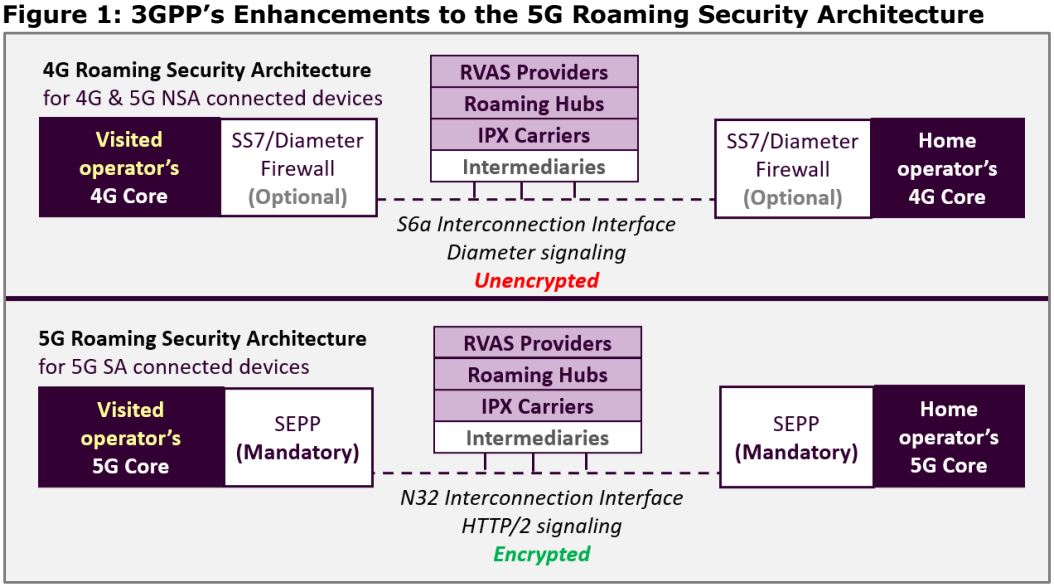
"Security by Design" was widely invoked within 3GPP and GSMA as the mantra according to which the security weaknesses in 4G would not be carried over into 5G.

In the run up to 5G standardization starting in 2016, the telecom sector – via 3GPP and GSMA – was clear that it wanted to make a great leap forward in mobile network security with the new 5G SA standards. "Security by Design" (instead of leaving an option to bolt on a signaling firewall, for example) was widely invoked by 3GPP and GSMA as the mantra by which the security weaknesses in 4G would not be carried over into 5G.

The work of writing the security specifications had to align with operator demand for the entire 5G standardization program to be accelerated. This demand to bring forward the specifications ahead of schedule was indeed met. This enabled South Korea's SK Telecom to launch the world's first 5G NSA service in April 2019 and T-Mobile USA to launch the world's first 5G SA network in August 2020 – both earlier than planned.

Several key fixes were specified for 5G SA standards in 3GPP Release 15 and Release 16. In 4G the International Mobile Subscriber Identity (IMSI) number is sent in the clear over the air where it can be captured by third party 'IMSI catchers'. In 5G SA the IMSI-equivalent is encrypted as a one-time temporary identifier. For the first time in mobile roaming scenarios, increased home control also enables a 5G SA-connected device to

Figure 1: 3GPP's Enhancements to the 5G Roaming Security Architecture



Source: HardenStance

inform its home network which visited network it is connecting to and empowers the home network to drop the session if it spots an authentication anomaly it doesn't like. **Figure 1** shows how security was also designed into other aspects of the 5G SA roaming specifications. As depicted in **Figure 1**, there are three main highlights of the new security features built into 3GPP's security specifications for 5G SA roaming:

- **The Security Edge Protection Proxy (SEPP)**: 5G's mandatory equivalent of the optional Diameter Edge Agent (DEA) and the Diameter Firewall, the SEPP is responsible for the authentication of the peer and integrity and confidentiality protection of outgoing HTTP/2 signalling messages over the N32 roaming interconnections. It also filters out malicious or anomalous incoming HTTP/2 signaling messages.

Due to the compressed time to market requirements for 5G SA that were imposed on 3GPP, it's not at all controversial to state that aspects of this security work were rushed.

- **Application Security on the N32 Interface:** In the case of the new N32 interface for forwarding packets between SEPPs, a new layer of application security includes security features that have never before been enabled for roaming interconnection. Among other things, this enables a receiving operator to validate where a given message has come from, validate the source, and validate that the message hasn't been modified. Deriving the value from this security feature is nevertheless dependent on operators agreeing to binding contracts between themselves that define what is, and what is not, allowed on the N32. This allows misbehaviour to be attributed to a particular entity, potentially resulting in penalties.
- **N32 encryption:** Rather than allow traffic to exit the SEPP into the interconnect environment in the clear as in 4G, 3GPP also mandated that 5G roaming traffic must be encrypted between SEPPs. 3GPP further specified that either or both of these specific encryption standards that must be used:
  - The widely used Transport Layer Security (TLS) standard for bilateral encrypting tunnels between mobile operator roaming partners end-to-end, where intermediary IPX carriers are not in the communications path.
  - PRotocol for N32 INternet Security (PRINS), a new 3GPP-specified application layer security protocol that allows a subset of signaling data to be exposed, inspected and modified where intermediary IPX carriers are in the path. PRINS combines the use of TLS for transport security and Java Web Encryption (JWE) plus Java Web Signature (JWS) for application layer security.

Due to the compressed time to market requirements for 5G SA that were imposed on 3GPP and GSMA, it's not at all controversial to state that aspects of this security work were rushed. This was largely responsible for issues being identified with PRINS after the first phase of specifications had been completed. Mobile operators and IPX carriers reported back that PRINS requirements are too complex and even create backdoors for fraud. Specific challenges deemed to be prohibitive from an operational standpoint include the following:

- The way terminating operators are required to verify modifications made by IPX carriers is far too complex.
- The way each operator is required to negotiate a protection policy contract with each roaming partner is too complex, especially for subsequent policy changes.
- The way, contrary to the goal of the application security embedded in the N32 interface, a sending operator is also not in control of what is modified, and by whom, with PRINS creates an opportunity for fraud and other abuses.

The Work of the GSMA's 5GMRR Task Force

To address these concerns the GSMA established the 5G Mobile Roaming Revisited (5GMRR) Task Force in the autumn of 2020. Comprised of experts from GSMA's Wholesale Agreements and Solutions Group (WAS), Network Group (NG) and Fraud and Security Group (FASG), its mission is to take the initial work of 3GPP on 5G roaming, undertake further research into the relevant issues relating to privacy, security and operational efficiency, and define secure, scalable, usable solutions for the N32 interface.

The 5GMRR Task Force broke its work down into three phases. The Phase 1 work, defining bilateral use cases, has recently concluded. The Phase 2 work, focused on use cases involving roaming hubs and adding refined Hosted SEPP solutions (sometimes referred to as SEPP outsourcing) is due to report its conclusions in April or May 2022. Phase 3, focused on RVAS providers, will report in October 2022. All the use cases that will be defined must be deployable by all mobile operators around the world. That means that the resource limitations of operators in developing countries have to be taken into account as much as the high-end capabilities of operators in advanced markets.

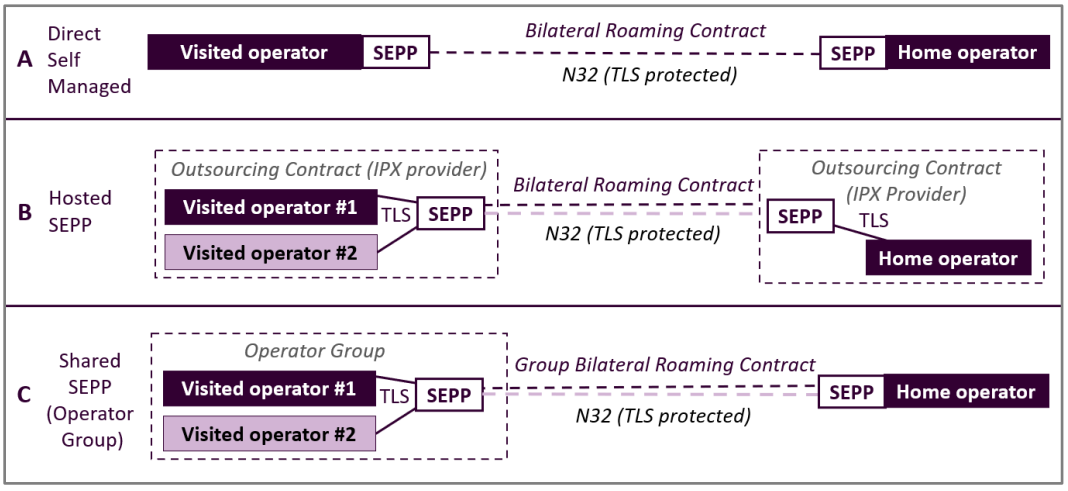
TLS is chosen in preference to PRINS as the encryption standard to be used on the N32 for all three Phase 1 use cases.

Phase 1 Specifies Three Bilateral Use Cases for 5G SA Roaming

As shown in **Figure 2** the 5GMRR Phase 1 documentation specifies the initial three bilateral use cases for 5G SA roaming. These share the following characteristics:

- They fulfil requirements for bilateral roaming use cases between operators that will be needed for the initial 1-3 years during which 5G SA roaming is initially rolled out, most likely in the 2023 – 2026 timeframe.
- TLS is chosen in preference to PRINS for all three Phase 1 use cases.
- Key decisions regarding roaming intermediaries are postponed to Phases 2 and 3:
  - Independent RVAS and Roaming Hub providers do not have any role of any kind specified for them in the Phase 1 recommendations, meaning they are unlikely to take part in the 5G SA roaming market much before 2025.
  - Whereas IPX carriers provide a variety of value added services as well as basic transport services for 2G, 3G and 4G roaming, for Phase 1 5G SA roaming their role is limited to offering SEPP hosting, IP routing and managed QoS services.
- The first three 5GMRR Phase 1 use cases are depicted in **Figure 2**. There are a lot of accompanying details, including cross-references to supporting GSMA guideline documents, but the use cases are simplified for the purposes of this paper.

Figure 2: The Three Phase 1 Use Cases For 5G SA Roaming



Source: HardenStance/GSMA 5GMRR Task Force

As depicted in **Figure 2**, the three use cases are as follows:

A. **Direct, Self-Managed:** In this model, both home and visited operators deploy and manages their own SEPPs and their own RVAS within their own network.

B. **Hosted or Outsourced SEPP:** In this model, operators outsource the operation of SEPP services to an IPX provider. TLS N32-c (control plane interface) connections are specified for establishing the N32-f (forwarding interface) connections between both SEPPs. The example in **Figure 2** shows the two visited operators being served by the same SEPP which requires the use of separate N32-f connections.

C. **Shared or Centralized Group-Level SEPP:** Applicable only to mobile operator groups with multiple affiliates, this model allows all of a mobile operator's affiliates to use shared SEPP resources as a single entry point rather than requiring each of them to deploy and manage their own SEPP within their own network.

The 5GMRR Group's Phase 2 and Phase 3 Specs Planned for 2022

The Phase 2 work (focusing on Roaming Hubs and Hosted SEPP refinements) and the Phase 3 work (focusing on RVAS) is underway and is due to be completed by April/May and October 2022 respectively. As it navigates the challenge of giving authorized third parties some limited visibility into encrypted traffic without substantially compromising privacy or operational efficiency, the challenges of the 5GMRR Task Force's work reflect the wider challenges of end-to-end encryption discussed at the bottom of page 1.

If the operational efficiencies achieved through roaming ecosystem intermediaries are to be carried over from 2G, 3G 4G and 5G NSA into 5G SA roaming as planned, the Phase 2 and Phase 3 work has to find some way to expose some amount of data to IPX carriers, RVAS providers and Roaming Hubs in a way that doesn't materially undermine the security and user privacy that is assured by the encryption.

Since they're operating at scale, roaming intermediaries are often better able to justify investing in more than the bare minimum security.

Operating at Scale Gives Intermediaries Certain Security Advantages

All real world operational aspects of the potential trade-offs between business efficiency and security have to be considered here. For example, many smaller operators tend to make greater use of roaming intermediaries than larger ones. Since they're operating at scale, roaming intermediaries are often better able to justify investing in more than the bare minimum security requirements in terms of people, technology and features than small operators having to do their own thing. If the 5GMRR Phase 2 and Phase 3 specifications do not create attractive market opportunities for intermediaries, there would be a negative impact from a security perspective here.

Clearly, the use of TLS exactly as it is – without either decrypting and re-encrypting or without modifying or adding to it in some way – cannot support the Phase 2 use cases. However, the majority of feedback from various mobile operators and IPX carriers is that PRINS in its current form cannot be used either. This suggests that the effort is most likely to focus on some modification, extension or addition to either or both of these two protocols as currently defined in the 3GPP standards.

While GSMA's members are universally agreed at the outset that one single approach using one single security standard must be specified per use case, the principle that only one of the two encryption standards must be specified for all use cases is not universally agreed. The Taskforce is at an early point in its Phase 2 and Phase 3 deliberations. At this early stage, very little is ruled in and very little is ruled out.

A Great Leap Forward for The Next Five Years

While achieving a 'great leap forward' in mobile network security with 5G SA was certainly a laudable aim at the outset, this White Paper has demonstrated that the point in time when most devices that are roaming are connected by a highly secure 5G SA interconnect environment is at least five, perhaps as much as ten, years away. In the meantime, if nothing else is done to improve mobile roaming security besides continuing

the 5GMRR Task Force's work, and then putting it into commercial practice, the vast majority of mobile users will continue to be vulnerable when roaming as outlined until some time in the 2026 – 2031 timeframe. Plainly, more can be done to secure the mobile roaming experience in the interim.

This paper has already referred to the necessary balance that has to be struck between national security, privacy and efficiency, as well as to the real world technical and commercial constraints imposed by the nature of the mobile operator and mobile roaming business models. As these trade-offs are deliberated, potential candidates for securing the legacy roaming ecosystem include the following:

- **SS7 and Diameter Firewalls:** Most obviously, and despite the GSMA having published detailed implementation guidelines many years ago, the majority of mobile operators still do not use SS7 or Diameter Firewalls to protect their 2G, 3G 4G and 5G NSA traffic. Decisions not to make these investments must be reviewed.

There may be potential to evolve the N32 interface so that 2G, 3G, 4G and 5G NSA as well as 5G SA traffic are sent encrypted over the N32.

- **Acceleration of 2G and 3G Network Shutdowns:** Freeing up spectrum and gaining operational efficiencies are currently the primary drivers for operators to shut down 2G and 3G networks and the momentum behind this is accelerating now. As operators and regulators deliberate over the timeframes for these shutdowns, security should get greater consideration as a driving force. Specifically, regulators and operators should consider the relationship between 2G and 3G shutdowns and the opportunity to accelerate 5G SA roll-outs. This can serve to bring forward the rate at which users and devices can be migrated onto 5G SA networks which are much safer to use in home networks as well as when roaming.
- **Diameter End-to-End Signaling (DESS) Phase 1:** Based on a GSMA standardisation effort concluded in 2019, DESS provides a backward compatible authentication and integrity protection capability for Diameter-based 4G roaming. This can be considered a prerequisite for SMS support via Diameter roaming interfaces as native Diameter lacks integrity protection, which makes SMS via Diameter vulnerable to fraud. Some operators are already working on implementing DESS Phase 1. When operational, this will provide additional protection for 5G SA customers via the reuse of Diameter for 5G NSA roaming.
- **Security audits of intermediaries.** There's no doubt at all that mobile operators are as much at risk from the malicious behaviour of other operators acting on behalf of their governments as they are from roaming intermediaries being hacked. However, that's not a reason to minimise or disregard this risk. In September 2021, Syniverse, one of the largest independent IPX carriers, reported in an SEC filing in September 2021 that log information allowing access to or from its Electronic Data Transfer (EDT) environment had been compromised for 235 of its customers. This arose from a breach during which attackers remained undetected in Syniverse's environment for five years.

  Through the GSMA's Network Equipment Security Assurance Scheme (NESAS), mobile operators are increasingly able to test the security of their network equipment vendors' software and undertake security audits of those vendors' development environments. As a future step, operators should consider undertaking security audits of roaming intermediaries as well.
- **Evolve the N32:** There may be potential to evolve the N32 interface so that 2G, 3G, 4G and 5G NSA as well as 5G SA traffic are protected over the N32 ■

** For this White Paper, HardenStance conducted detailed interviews with NetNumber, Orange and Deutsche Telekom subject matter experts, all of whom participated directly or indirectly in the 5G 5GMRR Taskforce. These interviews yielded a balanced set of*

perspectives around the background to the solutions released with 5GMRR Phase 1 as well as the challenges ahead as they relate to Phase 2 and Phase 3.

About the Sponsor and Co-Sponsors

The sponsor of this White Paper is NetNumber. The co-sponsors are Deutsche Telekom, and Orange.

About NetNumber

NetNumber, Inc. brings more than two decades of experience delivering core network signaling control platforms that power global telecom and enterprise networks. Our industry leading TITAN™ Centralized Signaling and Routing Control (CSRC) platform has been deployed by operators across the globe to simplify core networks in order to deliver new services and reduce operating costs.

TITAN.IUM™, the latest evolution for NetNumber, is an innovative, intergenerational framework for 5G that bridges legacy 2G, 3G and 4G technology to the new cloud-native era. TITAN.IUM enables our customers to migrate multiple generations of services, to a common, secure, simplified modern ecosystem. This means that the legacy applications can benefit from the technology of next generation of networks that are containerized, scalable and ultra-low latency. For more information visit www.netnumber.com

About Deutsche Telekom

Deutsche Telekom is one of the world's leading integrated telecommunications companies, with some 242 million mobile customers, 27 million fixed-network lines, and 22 million broadband lines.

The Group provides fixed network/broadband, mobile communications, Internet, and IPTV products and services for consumers, and information and communication technology (ICT) solutions for business and corporate customers. Deutsche Telekom is present in more than 50 countries. With a staff of some 226,300 (Dec 31, 2020) employees throughout the world, the Group generated revenue of 101 billion Euros in the 2020 financial year, about 66 percent of it outside Germany. For more information visit www.telekom.com

About Orange

Orange is one of the world’s leading telecommunications operators with sales of 42.3 billion Euros in 2020 and 137,000 employees worldwide at 30 September 2021, including 79,000 employees in France. The Group has a total customer base of 266 million customers worldwide at 30 September 2021, including 222 million mobile customers and 22 million fixed broadband customers. The Group is present in 26 countries. For more information visit www.orange.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The Cyber Threat Alliance, GSMA and ETSI. To learn more visit www.hardenstance.com