Securing the Mobile Ecosystem

Key Principles for Network Security and Device Integrity

Safety, privacy and security across the mobile ecosystem

This document is an extract from the GSMA's main report 'Safety, privacy and security across the mobile ecosystem'. The report can be found at www.gsma.com/xxxx

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com
Follow the GSMA on Twitter: @GSMA

Digital services, underpinned by fast, high-performance networks, play an increasingly vital role in the way people live and businesses operate. Protection against threats to mobile networks and devices is, therefore, absolutely crucial.

This document highlights a number of factors that can affect the security and integrity of the mobile ecosystem, with considerations for business practice and regulation.

Protecting Mobile Network Security and Device Integrity

Industry players need to work together and coordinate with international law enforcement agencies and national security authorities to share threat intelligence to respond to malicious attacks on mobile networks and devices, as well as to identify perpetrators. This can be achieved through the engagement of existing security incident response teams and the establishment of new ones, if required, to cover any gaps. Regulations, where necessary, should be applied consistently across all providers within the value chain in a service- and technology-neutral manner, while preserving the multi-stakeholder model for internet governance and allowing it to evolve. With this in mind, the GSMA and its mobile operator members have agreed to the following principle:

Operators will take steps to protect the underlying infrastructure to ensure that we provide consumers with the most secure and reliable communication service possible, by:

- Taking steps to source network equipment that is securely designed, developed and supported and to secure the network infrastructure that we operate and control
- Promoting public-private partnership to minimise the risk of either hacking or use of the network for malicious means through global and coordinated approaches
- Being clear about what infrastructure operators are responsible for and where the boundaries with other infrastructure or services lie

Mobile network operators safeguard the confidentiality, integrity and availability of communications across the network by securing critical assets (hardware, software and data) and preventing unauthorised access or intrusion to any of the constituent nodes or links. Since the end-user mobile device is the primary access point to the network from a user's perspective, protecting the integrity of mobile devices is a critical requirement. By necessity, mobile networks are accessible to a very wide range of users, via a variety of devices and connection protocols. They must also interconnect with many other communications networks around the world (fixed, mobile, internet service providers and enterprise) in order to offer the anywhere-anytime functionality of modern networks. Protecting networks and devices is therefore highly complex in practice.

The rapid evolution of mobile communications over the past decade has led to not only convergence of mobile and fixed network connectivity but also the exposure of mobile networks to new interfaces outside a network operator's control. 5G is ushering in an era in which connectivity is more fluid and flexible, with 5G networks adapting to applications and performance tailored precisely to the needs of users. By 2030, most markets will have at least one 5G network and mobile 5G connections are expected to surpass five billion, accounting for more than half of total connections.[1] The mobile industry is enhancing network and service security through network function design as well as through deployment strategies. New authentication capabilities and enhanced subscriber identity protection are resulting in significant security improvements compared with legacy generations. However, 5G capabilities are likely to co-exist with previous generations of mobile infrastructure for some time, in which case, both existing and new infrastructure will need to be secured.

[1] GSMA report '5G in Context, Q4 2021 Data-driven insight into areas influential to the development of 5G' (March 2022)

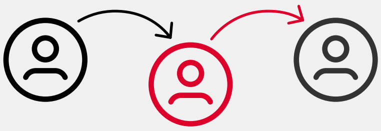
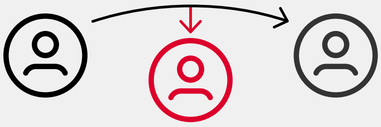
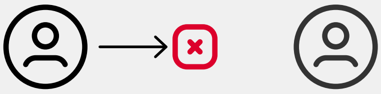
Different types of threats (Figure 1) have the potential to undermine the integrity of networks through unauthorised interception, impersonation or service interruption. The mobile industry has been responding to these threats primarily by strengthening security hygiene, encouraging transparent debate on the balance between convenience and security, and building ever more sophisticated security functionality into the technical standards and protocols as each new generation of mobile network has been developed and deployed.

This report addresses a number of security considerations that affect networks and devices and that have the potential to compromise the security required to keep customer communications safe and secure:

- Network security, including physical security and signalling, interconnect and operational security
- Mobile device security and integrity, including malware and software (both proprietary and open source code)
- 5G, IoT and future network developments, including cloud and virtualisation as well as supply chain

Each of these has important implications for government, industry and other stakeholders, outlined later in this document.

Figure 1
Protecting networks

SAFEGUARD OBJECTIVE	DESCRIPTION OF THREAT	EXAMPLE ATTACK
Integrity avoid data being altered	Unauthorised tampering	MAN-IN-THE-MIDDLE (MITM) 
Confidentiality keep data private	Unauthorised access	EAVESDROPPING 
Availability keep network and data available to genuine users	Destruction, theft, removal, or loss of data, or networks become unavailable	DENIAL OF SERVICE (DOS) 

Physical network infrastructure

The first step in securing mobile networks is the physical infrastructure itself, such as the cell sites, the backhaul network transmission and core network assets.

For example, there are key functions within a network, such as the register of authorised users, which need to be secured since they represent single points of vulnerability, whether exposed to malicious attack or technical failure. Mobile network operators and equipment vendors continue to develop and deploy new solutions to make these more robust, and have been largely successful to date, but this requires ongoing investment in the development and deployment of new functions and features.

The use of false mobile base stations, or IMSI (international mobile subscriber identity) catchers, is a vulnerability due to the absence of mutual authentication on 2G technologies and functionality that can automatically configure 3G and 4G devices to use the 2G network. False base stations trick mobile devices that are within range to connect to them rather than the real network to which the false base station operator can then relay the call. Such a "man in the middle" attack creates a range of exposures to interception, location tracking, denial of service, and fraud. Lawmakers are developing recommendations to protect against the unauthorised use of these devices. Mobile network operators can deploy standard network and security measures to help mitigate against this risk and the GSMA has developed guidance to assist operators.

In addition to telecoms infrastructure, there are a range of corporate IT services that enable broader business operations as well as software for supporting customers, including billing systems and enterprise client dashboard and control systems. Internal corporate systems include intranet, email, instant messaging and staff systems such as accounting and sales systems. These systems are accessed by a range of employee devices and used by the full range of staff functions including the system administrators for the operational network.

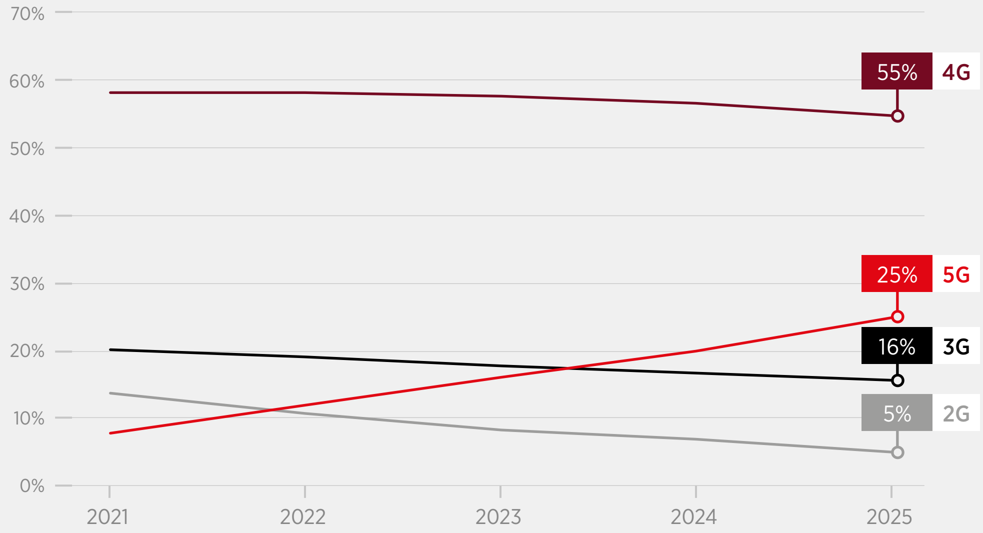
The technology used within mobile networks is regularly upgraded with the latest enhancements rolled out on a planned basis. The high levels of investment in new infrastructure on a periodic basis have gone a long way to ensuring that the network infrastructure is as robust as reasonably possible. Maintaining confidence in this ability to invest as legislation and regulation changes in response to evolving threats will be increasingly important for success.

Some legacy 2G and 3G networks make use of unsecure signalling protocols, which were developed many years ago when security needs were lower, and as a result are subject to fraud and security threats on a regular basis. The GSMA's Fraud and Security Group has undertaken significant work to provide advice to network operators on how to mitigate signalling security risks. Several of the known attacks have been mitigated with security enhancements introduced in 4G and 5G. Exploitation of vulnerabilities on 4G networks can be minimised by ensuring the security capabilities that are inherent in the standards are properly deployed and configured. However, due to the backward compatibility of 4G with 3G/2G they will not disappear until the legacy technology or backward compatibility ceases to exist.

5G includes security controls to address many of the threats faced in legacy 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection and additional security mechanisms. GSM Gateways (or "SIM Boxes") can also allow unauthorised third parties to interfere with the routing of calls to mobile networks and their customers, and this can raise safety and security concerns. Calling line identity (CLI) is generally not supported by GSM Gateways, and its absence has implications for services that rely on CLI (e.g. prepaid SIM account top up) as well as for network operators' lawful interception obligations to support law enforcement.

While mobile operators continue to mitigate the threats to their networks and their consumers, the same should be expected of operators of public wireless networks, such as public Wi-Fi Hotspots. The operators of these networks and customers should deploy appropriate safeguards, for example virtual private networks (VPNs) to help secure the wider communications ecosystem.

Figure 2
Percentage of Connections
5G will account for a quarter of total mobile connections by 2025, more than three times the figure for 2021
Percentage of connections (excluding licensed cellular IoT)



Source: GSMA Intelligence

Key implications for government, industry and other relevant stakeholders

While no security technology is guaranteed to be unbreakable, attacks on mobile networks and services are less common, as many would require considerable resources, including specialised equipment, computer processing power and technical expertise beyond the capability of most people or organisations. The barriers to compromising mobile security have been very high, and understanding of possible vulnerabilities has been greatly enhanced thereby enabling a prompt industry response to new security issues. However, the changing technology landscape and the emergence of new threats and sources of attack requires industry to take an even more proactive approach to protecting networks in future:

- It is important that the mobile industry ensures adequate mechanisms, tools and opportunities are in place to facilitate the sharing of threat and attack information and to ensure information is promptly disseminated in response to incidents. Such an initiative could include regulators or other government authorities such as national Computer Security Incident Response Teams (CSIRTs).
- Collective industry action is required to protect connected networks and consumers through consistency and consensus in the development of standards and the proportionate use of monitoring, detection and blocking capabilities.
- Securing mobile networks and services is complex, with multiple decisions to be taken by mobile network operators and their suppliers to implement the security standards properly and to deploy and configure a range of features. The GSMA offers advice and guidance to its members on how to achieve optimal security levels and continues to work on defining baseline security requirements to be committed to by all mobile network operators.
- The ongoing security challenge will expand with the evolution of 5G, but that also creates an opportunity to rethink security and how it can be provided.
- Regulations, where necessary, should be applied consistently across all providers within the value-chain in a service- and technology-neutral manner, while preserving the multi-stakeholder model for internet governance and allowing it to evolve.

Mobile device security and integrity

By the end of 2021, 5.3 billion people subscribed to mobile services, representing 67% of the global population.[2] Over the period to 2025, there will be an additional 400 million new mobile subscribers, taking the total number of subscribers to 5.7 billion (70% of the global population).[3] It is expected that there will be 5.2 billion 5G connections by the end of 2030.[4]

A mobile phone call or data transmission will traverse several networks and, in the case of data, will often take multiple paths as part of a single communication. As a result, a range of potential vulnerabilities has emerged, requiring all network operators and the broader mobile industry ecosystem to be vigilant and to respond to them. Malware attacks can cover a range of targets including mobile devices, device applications and infrastructure. However, with increasing broadband access and a range of malware attacks on devices, protection must be also considered against device-based network attacks (e.g., signalling 'storms,' Denial of Service (DoS) attacks, IoT compromises back into the network).

Perhaps the most serious threat is a premeditated and systematic large-scale attack designed to render a whole network inoperable, affecting all users. There is a risk that breaches of mobile devices (e.g., by malware from phishing emails) could be used as an entry point to spread to other connected devices and then exploited to attack IP-based networks. For example, the 21 October 2016 attack on a major controller of domain name system infrastructure, Dyn[5] originated from malware on a computer, which spread to other devices, creating a botnet, which was then used to carry out a DDoS (distributed denial of service) attack. On an even larger scale, a similar approach could be used to inundate an IP-based mobile network with traffic that causes it to be overwhelmed and become unusable. Preventing such an attack requires close cooperation between mobile network operators and national law enforcement agencies as part of an overarching security plan, since attacking mobile networks is only one such possible route of attack by hostile parties.

The GSMA plays a central role in coordinating activity and leading on initiatives such as the Network Equipment Security Assurance Scheme (NESAS)[6] which is a global security assurance framework that facilitates improvements in security levels across the mobile industry for network equipment vendors. The scheme reflects the security needs of the entire ecosystem, including governments, mobile network operators and regulators, as it has been defined by industry experts through GSMA and 3GPP.

Security threats can come in many guises. Allied to the device is the eUICC, or SIM as it is better known. SIM swap is a normal business process to issue and provision new SIMs for customers that require replacements. The emergence of SIM swap fraud is an example where a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one, has provided an opportunity for fraudsters to obtain and use the replacement SIM card to gain access to users' financial and wider service accounts. Mobile operators are implementing best practice to defend against such attacks. Phasing out legacy methods of authentication (such as usage of secret information and user-selected passwords that need to be spoken) is just part of the solution. Some mobile operators are now providing APIs for services such as banks to be able to connect to in order to establish whether a SIM swap has occurred recently.

[2] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf Mobile Economy Report 2022

[3] ibid

[4] 5G in Context, Q1 2022 Data-driven insight into areas influential to the development of 5G (May 2022)

[5] Dyn is a domain name system (DSN) provider for internet service providers, including Twitter, Amazon, AirBnB and Spotify. The organisation was able to restore their services after each attack while avoiding a system-wide outage, and mitigate against a third attack without consumer impact.

[6] https://www.gsma.com/security/nesas-network-equipment-vendors/

Alongside the opportunities for consumers and businesses to use such services is the risk that mismanagement of these devices can create vulnerabilities that have the potential to breach networks and impact a wider set of users. Security attacks threaten all forms of technologies, including mobile. Mobile devices are targeted for a variety of reasons. For example, as an attractive item for thieves (due to their relatively high value and small size), organised criminals often seek to change the IMEI number of a stolen mobile device in order to re-activate it after it has been reported stolen. Other criminals use malware to perform functions that have the potential to cause harm to users, typically via identity theft and related fraud.

The GSMA has helped develop protection mechanisms such as those described in the GSMA IoT Connection Efficiency Guidelines[7] to protect mobile networks from the mass deployment of inefficient, insecure or defective IoT devices. Furthermore, the GSMA encourages its members to deliver security critical device patches to vulnerable devices as quickly as reasonably possible.

Key implications for government, industry and other relevant stakeholders

Good security practice and policy by industry suppliers is essential. Programmes such as the GSMA Security Accreditation Scheme, which certifies SIM suppliers, ensures that a commitment to security levels is encouraged and can be evidenced. Security assurance of suppliers and their products has been performed by the GSMA for some time with the Security Accreditation Scheme for SIM suppliers and the Network Equipment Security Assurance Scheme (NESAS) for network infrastructure product vendors.

The GSMA also seeks to support internet service providers and app developers which operate on the network and need to be accountable for preventing their exploitation as a channel to breach the integrity of a mobile network.

The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements can play, as an alternative to embedding the security into the mobile device or an external digital card (microSD), because the SIM card has proven itself to be resilient to attack.

[7] https://www.gsma.com/newsroom/wp-content/uploads//TS.34-v8.pdf

5G, IoT and future network developments

5G gives the mobile industry an unprecedented opportunity to uplift network and service security levels. The GSMA regularly explores a range of security considerations including secure by design, 5G deployment models and 5G security activities. This analysis is collated into a GSMA 5G Cybersecurity Knowledge Base[8] to provide useful guidance on a range of 5G security risks and mitigation measures. The GSMA's 5G Security Task Force (5GSTF) is responsible for monitoring work on 5G security, within the GSMA and across the wider industry and the standards development community, with a view to ensuring all necessary enablers are in place to deliver secure and resilient operational networks. In particular, the task force focuses on potential gaps between standards and operational implementations and the resolution of those.

With the implementation of 5G comes the migration to cloud computing, resulting in security considerations that were once the responsibility of the network equipment vendor becoming increasingly that of the operator. Virtualised networks bring a range of opportunities and benefits, including network slicing, network scalability and greater flexibility of vendor choice. But they also introduce a range of potential security threats. The transition of operator network environments to the cloud creates significant changes to the security operations and management of these networks, as well as to the type and capabilities of security controls. Assets are no longer placed at a fixed location (physical box) with planned capacity and long lifecycles. Instead, the solution stack relationship changes dynamically, and with it, the network traffic of the physical and virtual switches. This increases the complexity of monitoring the compute, storage and network properties of each component as they are no longer statically bound. Furthermore, the lifespan of such entities gets shorter to serve a workload for a few minutes after which it is decommissioned. In case of compromise there is a need to track not only the alignments of virtual/physical assets, but also the relationship between assets as well as the historic allocations of these assets as they moved within the platform.

5G is needed to capture the huge opportunity presented by IoT. As the ecosystem grows, the mobile industry will be expected to support bespoke services across industry verticals, where data is exchanged and insightful decisions using AI are made. According to the latest GSMA Intelligence IoT market update[9] the total number of IoT connections will more than double by 2030, reaching 37.4 billion.[10] Consumer IoT connections will almost double between 2020 and 2030 to 13.8 billion.

IoT services present security challenges, not only due to the scale and breadth of the services, but also due to the critical functionality that they provide and the private information they leverage. These factors make IoT services high-value targets for potential attackers who wish to exploit these services, for example, to launch DDoS attacks or extract sensitive data. Additionally, there exists a relatively large legacy estate of older IoT devices with limited in-built security protections. The GSMA has produced IoT security guidelines and an associated security self-assessment scheme for a range of ecosystem players. The GSMA's IoT security guidelines,[11] provide a comprehensive guide to IoT service providers.

As the industry moves from the traditional approach of dedicated hardware to a cloud-orientated approach, the number of options for infrastructure grows. Typically, modern infrastructure options can be classified into one of four groups: Software as a Service (SaaS); Infrastructure as a Service (IaaS); Platform as a Service (PaaS); and on-site infrastructure.

[8] https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

[9] https://data.gsmaintelligence.com/research/research/research-2021/IoT-market-update-assessing-disruption-and-opportunities-forecasting-connections-to-2030

[10] GSMA Intelligence report 'IoT market update: assessing disruption and opportunities, forecasting connections to 2030' (December 2021)

[11] https://www.gsma.com/IoT/IoT-security/IoT-security-guidelines/

The move from the traditional approach of dedicated hardware to a cloud-orientated approach presents a range of opportunities and benefits such as network slicing, network scalability and greater flexibility of vendor choice. Cloud computing software can run on a range of non-proprietary platforms ranging from the entire product being hosted in the cloud, through to every element being owned and managed by the operator. The GSMA's Network Function Virtualisation Threats Analysis (FS.33)[12] provides a comprehensive overview of the threats related to network function virtualisation (NFV) and the underlying infrastructure and platforms hosting the NFV. It also includes extensive guidance on appropriate risk controls.

Virtualised infrastructure and more open interfaces deliver significant benefits but also make the 5G supply chain more complex and multi-party compared to 4G and earlier. This enables significant flexibility, scalability and potential cost savings but it is a more complicated supply chain. The need for increased resilience in network infrastructure has resulted in many regulators placing requirements on all operators to increase the levels of diversity, security and controls.

The GSMA encourages suppliers to participate in industry-recognised security assurance schemes, such as the GSMA Network Security Assurance Scheme (NESAS)[13] and encourages operators to source equipment from suppliers that participate in these schemes. The GSMA Supply Chain Toolbox outlines a number of services and guidelines to help operators and their suppliers to better understand security and to access best practice.

[12] https://www.gsma.com/security/resources/fs-33-network-function-virtualisation-nfv-threats-analysis/
[13] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Key implications for government, industry and other relevant stakeholders

The GSMA aims to play a significant role in helping to shape the strategic, commercial and regulatory development of IoT and the 5G ecosystem.

— GSMA recognises that it has a key role to play in gathering and prioritising 5G security requirements for standardisation. The GSMA and its members invite other subject matter experts and law enforcement agencies to engage to ensure all needs are clearly understood.

— Government should support the global nature of future network markets and the wide variety of devices which will connect to the internet in future, and work across jurisdictions to ensure consistency and clarity on regulation and network security obligations for all players involved in this complex and rapidly evolving area.

— The mobile industry will continue to engage with the wider ecosystem and foster appropriate investment, directly or via vendors and ecosystem partners, in securing networks and devices as technology develops, especially in relation to the transition to network function virtualisation and 5G.

The GSMA has also conducted a comprehensive threat analysis involving industry experts from across the ecosystem, regulators as well as public sources such as 3GPP, the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST). These threats have been mapped to appropriate and effective security controls, and this analysis has been collated into a 5G Cybersecurity Knowledge Base providing useful guidance on a range of 5G security risks and mitigation measures.

The 5G Cybersecurity Knowledge Base makes available the combined knowledge of the 5G ecosystem to increase trust in 5G networks and make the interconnected world as secure as possible. The GSMA constantly monitors the activities of hacker groups, as well as researchers, innovators and a range of industry stakeholders, to improve the security of networks from one generation to the next.

GSMA security initiatives

The GSMA leads a range of industry initiatives (see Figure 3) to make operators aware of the risks and mitigation options available to protect their networks and customers and its work is acknowledged by regulators around the world as being sufficient to eliminate the need to formally regulate on a range of security matters.

Figure 3
GSMA Fraud and Security Services

GSMA Coordinated Vulnerability Disclosure (CVD)
A way for researchers to disclose vulnerabilities that could impact the mobile ecosystem

GSMA Device Check™
Protect against the risk of handling stolen or fraudulent devices, with this instant look-up service

GSMA Device Registry
Deter device crime, by exchanging device status information across the global ecosystem

GSMA eUICC Security Assurance (eSA)
Instil confidence that eUICC chipsets have reached rigorous industry security standards

GSMA Network Equipment Security Assurance Scheme (NESAS)
Security assessment of vendors' product development/lifecycle processes and infrastructure products

GSMA Security Accreditation Scheme (SAS)
Security audit and certification of SIM/eSIM production and subscription management sites

Services for GSMA members only:

GSMA (FASG)
Share threat intelligence in a confidential forum and collaborate to maintain the security of operators' and their customers' assets

GSMA Telecommunications-Information Sharing and Analysis Center (T-ISAC)
Share timely and actionable information on cybersecurity threats in a trusted environment

Further Reading

Mobile Telecommunications Security Landscape 2022:
https://www.gsma.com/security/resources/gsma-security-landscape-report-2022/

GSMA Network Equipment Security Assurance Scheme (NESAS):
https://www.gsma.com/security/network-equipment-security-assurance-scheme/

GSMA Device Registry:
https://www.gsma.com/services/deviceregistry/

GSMA IoT Security:
https://www.gsma.com/iot/iot-security/

GSMA Report: Cybersecurity: A Governance Framework for Mobile Money Providers:
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/Cybersecurity-A-governance-framework-for-mobile-money-providers_WEB.pdf

GSMA Cybersecurity and Mobile Money:
Prioritising Consumer Trust and Awareness: GSMA | Cybersecurity and mobile money: prioritising consumer trust and awareness | Mobile for Development

GSMA Mobile Policy Handbook 2022:
https://www.gsma.com/publicpolicy/wp-content/uploads/2022/03/Mobile-Policy-Handbook-2022.pdf

GSMA Head Office
One Angel Lane
London, U.K.
EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601