Security Assurance and Certification

- *Playing the long game*

June 2023

GSMA

This is an information paper of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

Executive Summary

Welcome to this information paper, which examines how today's actions engaging in industry security assurance certification schemes, international standards and developing industry security best practice guidance delivers an enduring long-term benefit. Changes in geopolitical dynamics and the increasing classification of mobile infrastructure as critical national infrastructure have intensified focus on the security posture and resilience of network equipment and the providers of it.

This information paper firstly describes how a holistic and efficient security strategy may be composed of multiple layers. The combination of security controls taken from each layer build to deliver a bespoke security solution for each operator. The underlying approach of adopting international standards, implementing industry security best practice and supporting industry assurance and certification schemes can act together to provide a baseline security on which to build a complete security strategy.

The mobile industry has long aimed to deliver robust security enablers to protect its networks, customers and services. This security approach is delivered through a lifecycle approach starting even before a service goes live. This information paper describes an example network *product* lifecycle and a complementary network operator *service* lifecycle. These are used to illustrate how early interventions in the security lifecycle can deliver efficient and enduring security returns and outcomes.

Furthermore, under the Cyber Security Act (CSA) and draft Cyber Resilience Act (CRA), the EU is intending to introduce network, device and, potentially, service cyber security certification. The EU is looking to existing industry schemes (where they exist) as the start point for any EU wide scheme. Where industry schemes don't exist or where there are significant gaps, the EU will look to develop its own scheme or use EU common criteria (EU CC) to meet EU certification requirements. In both cases, imposed regional or national schemes are likely to have considerably more impact on the industry and prove less flexible to technology changes than if industry can propose the reuse of that which it is already using. While the EU has first mover advantage most other countries or regions are considering similar proposals.

The GSMA continues to build security resilience by providing a range of advice, guidelines, recommendations, working group activities, discussion fora and threat mitigations; some of which are outlined later in the report.

Given the long in-life equipment usage stage, there is considerable benefit for industry involvement in:

- Reaping a longer-term security benefit by actively supporting the development of international standards
- Applying and developing industry-developed security best practices through active engagement in GSMA's working groups
- Developing coherent vendor arrangements that avoid fragmentation through actively supporting and specifying the use of industry schemes such as GSMA's Network Equipment Security Assurance Scheme (NESAS) scheme
- Strengthening the collective operational security response through threat intelligence sharing by joining and contributing to GSMA's T-ISAC scheme and security vulnerability sharing through GSMA's CVD scheme.

The relative ease of engagement in these areas means that playing the 'long game' for security can deliver high impact engagements with long-term residual value.

Introduction

Mobile services are being enhanced through increased deployment of 5G infrastructure[1], to support new industry vertical applications and to support a shift towards more flexible working. 5G, like previous generations of mobile network designs, has benefitted from near-global recognition of the standardisation activity at 3GPP. This standardisation has enabled the market to develop products and services that will inter-work, enabling the potential for global market supply chains.

Changes in geopolitical dynamics and the increasing classification of mobile infrastructure as critical national infrastructure have increased focus on the security posture and resilience of network equipment and the providers of it. There has been an increasing trend towards national responses to supply chain threats including restricting certain vendors and implementing new defensive regulations and security requirements. These market interventions act to limit the supplier options from which Mobile Network Operators (MNOs) can select (this reduction in supply competition can result in higher costs). It is recognised that there are various longer-term national and regional initiatives that aim to broaden existing vendor arrangements via open networking and wider innovations.

The mobile industry has long aimed to deliver robust security arrangements to protect its assets, customers and services. This security objective is delivered through a lifecycle approach starting even before a service goes live. The foundations of security are built through architectural design choices, choosing to adopt solutions utilising internationally recognised standards and shortlisting vendor solutions that already have a strong baseline security level built-in.

Product vendors seek to deploy their solutions in a global market to maximise efficiencies and the market opportunity. A common way of demonstrating product security is to build products that are assessed under globally recognised product security assurance schemes (such as GMSA's Network Equipment Security Accreditation Scheme (NESAS)). These, in turn, can help avert fragmentation of regulatory security requirements by providing a globally recognised robust security baseline that all stakeholders can adopt. In turn, mobile network operators seek to access the widest pool of viable global vendors to maximise competition in supply and access the most innovative products.

The availability of equipment developed to internationally recognised technical standards enables access to the best value global supply market. It also enables the successful inter-working of multi-vendor choices.

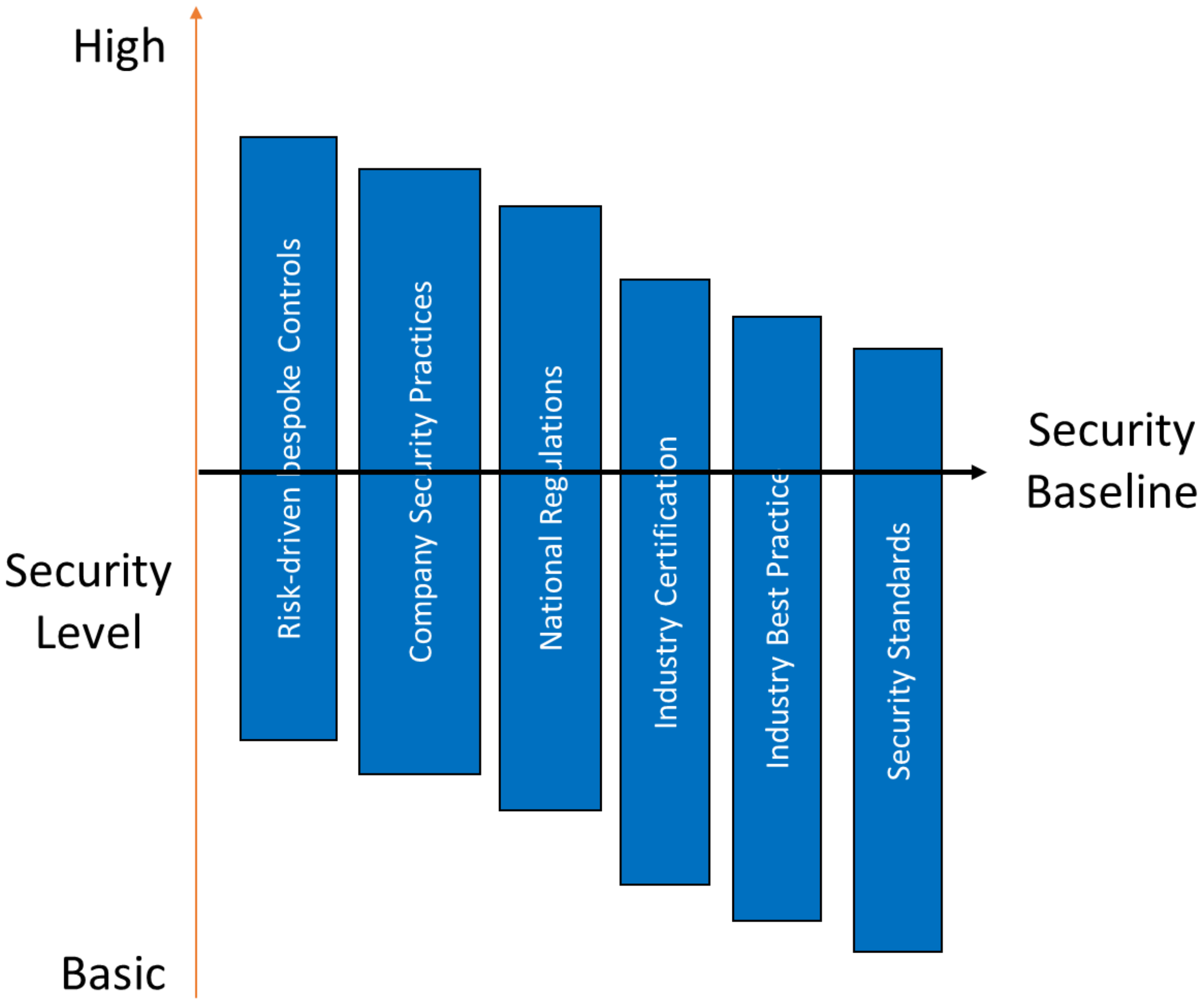
Mobile network equipment and services are developed and operated in the long-term within the aforementioned environment. Efficient utilisation of capital and operating expenditure means that intervention to make the operating environment favourable can have long-term returns for operational networks, regulators and consumers. This security 'long game' justifies engagement in the earlier stages of equipment and service definition and assurance.

[1] GSMA report '5G in Context, Q4 2022 Data-driven insight into areas influential to the development of 5G' (at 31st Dec 2022) identified 223 operators in 87 markets had launched mobile 5G with 1 billion connections (12% adoption)

A Layered & Efficient Security Strategy

A holistic and efficient security strategy may be composed of multiple layers as shown below. The combination of security controls taken from each layer build to deliver a bespoke security solution for each operator. Efficient and cost-effective security approaches can be delivered by matching security controls to the threat model, understanding the security benefits built-in by lower level and existing security controls and by customising the security decisions in the higher-level security levels. Areas showing co-incident requirements demonstrate a potential duplication meaning it might be possible to remove duplicate controls. This can be applied across multiple frameworks[2]. The resulting set of security approaches builds the overall security strategy.

The underlying security approaches can act together to provide a baseline security level on which to build a security strategy.



[2] E.g. CIS Critical Security Controls Navigator (cisecurity.org)

Security Standards

Within the mobile eco-system, 5G functional security enabling standards are developed by the 3rd Generation Partnership Project (3GPP). Other standards bodies such European Telecommunications Standards Institute (ETSI) provide the underlying virtualisation standards and bodies such as the Internet Engineering Task Force (IETF) develop IP or other underlying low level internet secure communications protocol standards. GSMA through GSMA working groups and specific task forces then develop the deployment and interoperability security standards.

In large part, industry developed international standards have had huge success in developing mobile network specifications that deliver multivendor, interconnected networks from the early 2G GSM networks on through 5G today. However, in some cases, it can take some time to reach practical standards adoption. For example, 3GPP's IP Multi-media Subsystem (IMS) (which was specified in 3GPP Release 5[3]), actual uptake and implementation took a considerable time. This, sometimes protracted, timescale gap emphasises the importance of industry engagement early in the standards development process in order to reap the benefit later. There have also been challenges in areas such as Voice over LTE (VoLTE) S8 Home Routing and 5G Roaming PRINS specifications where earlier alignment of security design and operational requirements may have reduced the need for subsequent challenging pre-deployment modifications.

Industry Best Practice

There are a range of industry security best practices that can be adopted, notably GSMA's set of Fraud and Security recommendations. These fraud and security best practices are developed and ratified by industry experts using their real-world experience and cover the end-to end scope of mobile networks from the device, the mobile network, interconnect and signalling.

These recommendations offer a set of security principles that can be exploited, moulded and applied to enhance network security in a bespoke manner to reflect each operator's approach.

Industry Assurance and Certification

Global industry assurance and certification schemes offer a route to assure a common level(s) of security, enabling re-use of equipment, designs and documentation with global recognition. Whilst there are a range of assurance and certification schemes in existence, this report focuses on the NESAS Scheme developed by GSMA and 3GPP[4], to demonstrate the benefit of such international rather than, often differing, national approaches. NESAS is a network equipment security assurance scheme operated and maintained by GSMA, with contributions from 3GPP, covering the methodology and security targets for equipment under test. It defines a globally applicable security baseline that network equipment vendors can meet.

The NESAS approach consists of the following steps:

1. Equipment vendors design and develop their network products according to internally defined development processes
2. Equipment vendors internally assess that their product development and lifecycle management processes meet the security requirements defined by GSMA
3. Equipment vendors subject their product development processes to independent auditors to assess compliance levels to the security requirements;

[3] 3GPP are now working on Release 18

[4] It should be noted GSMA also operates other certification scheme such as the UICC Security Assurance Scheme (SAS) and eUICC Security Assurance (eSA). Consideration is also being given to launching a Mobile Device Certification Scheme

4. Equipment vendors submit their network products to independent test laboratories for NESAS evaluation against the defined security requirements;
5. Auditors and labs provide the report of their audits and tests to the manufacturer and indicate their findings and the level of compliance against the security requirements the vendor has achieved.

The objective of NESAS is to provide an industry-wide security assurance framework to facilitate a strong baseline security level across the whole industry.

NESAS is of value to both operators and vendors. It is intended to be used alongside other mechanisms to ensure a network is secure. In particular it should be complemented by an appropriate set of security policies covering the whole lifecycle of a network. These policies can also include the application of GSMA published security recommendations[5] and participation in the GSMA's operational security services such as CVD [8] and T-ISAC [9].

One of the motivations for developing NESAS was that the scheme would help vendors and operators agree a set of common security requirements and avert fragmented regulatory security and certification requirements. NESAS should be used globally as a common baseline. Individual operators or national IT security agencies may impose additional security requirements on top of NESAS. However, additional security requirements are unlikely to be internationally recognised and could introduce one off testing / certification costs which cannot be easily reused. It is therefore important that industry works together to further develop NESAS to address any common reoccurring additional requirements from stakeholders in multiple jurisdictions. GSMA is receptive to suggestions to improve NESAS and to extend its scope.

With the increasing complexity of mobile networks and heightened security awareness, NESAS was designed to meet the needs of disparate stakeholders including:

- Mobile network operators,
- Equipment Vendors,
- Official/Governmental information security agencies and regulators.

In many countries, MNOs are tasked by regulation to deploy and run, reliable and robust networks. As one element of achieving this, MNOs rely on secure network equipment being provided by their vendors. Thus, for MNOs, it is important to be able to understand the level of security within any specific product provided by their chosen vendors. The following two approaches are considered suitable to achieve this:

- Firstly, assessment of the security related to the product development and lifecycle management processes
- Secondly, security evaluation of network equipment products by a competent test laboratory with standardised security tests against an agreed security target.

Both approaches – process assessment and product evaluation by testing – help MNOs determine the achieved level of security of a network product. This point is reinforced according to ENISA when discussing device and service certification schemes, "*Certification is a tool that allows product vendors and service providers to demonstrate and advertise the cybersecurity of their solutions…. the goal is to harmonise the recognition of the level of cybersecurity of ICT solutions …, allowing vendors and service providers to reach more customers*."[6]

[5] Eg, GSMA | FS.31 GSMA Baseline Security Controls - Security

[6] Cybersecurity Certification (europa.eu)

For governments and national regulators, NESAS can be leveraged to assist telecommunication networks in reaching resilience levels resistant to cyber threats and their consequences.

Key benefits to governments, national security authorities and regulators, include:

- One global security scheme which reflects the security needs of the entire ecosystem, commensurate with national security needs.
- Can instil trust in the security and resilience of national telecommunications networks.
- Through the ability to compose additional layers that can accumulatively be tested and certified, help avoid fragmentation of security requirements across the global market.
- Independently established, it is defined by the industry through the GSMA and 3GPP in a neutral geopolitical environment.
- Visibility of security capabilities of equipment vendors and their success at reaching the standards required by the industry.
- Maintained and evolved by the industry in line with emerging technical developments and the cyber threat landscape.
- Promotes supply chain competition and choice by encouraging equipment vendors to achieve desired security standards.

National Regulations

There are an increasing range of national and regional regulations covering cloud, IoT, data protection and network security. For example, the UK's Supply Chain Review[7] has resulted in new legislation to be enforced through the national regulator, OFCOM, with significant fines for non-compliance. Strict national controls will necessitate a design, configuration and operational response from operators and product vendors that should be aligned to reflect the baseline of security already in place due to the use of international standards, availability of industry best practices and global assurance and certification schemes. Alignment allows the maximum benefit to be extracted from existing controls and then additional security measures can be established on a risk basis on top.

Company Security Practices

Every operator will have established security controls and approaches, procurement requirements, penetration test schemes, known improvement activities and security operations experience that have been shaped and refined over time. These will reflect the installed network and can be improved as network enhancements are planned and delivered.

Risk-driven Controls

Given that a strong security base will have been established from the previously described security approaches, a bespoke risk management activity can be used to identify and assess any residual areas of weakness or tactical mitigations that may enhance the overall security posture.

[7] https://www.gov.uk/government/news/new-telecoms-security-law-to-protect-uk-from-cyber-threats

The Lifecycle Perspective

The mobile industry has long aimed to deliver robust security arrangements to protect its networks, customers and services. This security approach is delivered through a lifecycle approach starting well before a service goes live. The foundations of security are built through choosing to adopt solutions utilising internationally recognised standards, architectural design choices, and shortlisting vendor solutions that already have a strong baseline security assurance built in.

The security of product and service lifecycles are based upon cradle to grave threat identification and risk management. Scientific and product innovation act to develop, patent, licence, undertake market tests and to mature solutions through the early Technology Readiness Levels (TRL). The following sections discuss the development of robust security supply arrangements through a series of lifecycle lenses.

The 'Define' Lifecycle Phase

Following earlier research and innovation, the 'Define' stage seeks to incorporate innovations, intellectual property and designs into standardised form through internationally recognised standards bodies. Technical standards are usually produced by standard development organisations (SDOs) such as 3GPP, ETSI, ITU, IETF, etc.

A mobile technical standard can typically take between 12 – 24 months to develop. The development of products and services based on 3GPP and GSMA standards has enabled mobile telecoms services to be delivered to consumers in an efficient manner, enabling both global roaming of subscribers and international connectivity.

3GPP is notable for its extensive work in defining the nature of modern mobile networks through the various standards releases. These include Security Assurance Specifications that are used extensively in the GSMA's NESAS certification scheme.

The membership of standards bodies varies from vendor and industry representatives through to extensive representation by governments. Given the technical nature of many standards, considerable technical skill, peer review and experience are brought to bear. The process involves a long-term commitment and individuals with a strong track record often progress to senior guiding roles in SDOs.

The strategic importance of providing leadership in the development of international standards is highlighted in the latest UK National Security Strategy[8] "*Power will increasingly be held by countries that have a strategic advantage in science and technology and access to the data that drives innovation, enabling them to exert influence over others and to shape global standards in ways that best fit their own economic and political interests.*

Similarly, even though it is still relatively early in the roll-out of 5G, the development of 6G standards is close by. The UK Government note in their wireless infrastructure strategy[9]

The decisions that will shape 6G will be made over the next few years, with the global development of 6G likely to follow a similar timeline to 5G. Critical pre-standardisation research is already underway and we expect that 6G standards-setting will have begun by 2025.“

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085304/National_Cyber_Strategy_2022_-_GOV.UK.pdf

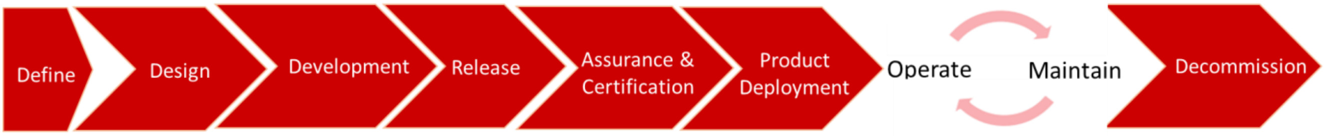
[9] https://www.gov.uk/government/publications/uk-wireless-infrastructure-strategy/uk-wireless-infrastructure-strategy#chapter-7--shaping-the-development-of-6g

A Mobile Network *Product* Lifecycle

This section examines both a product centric lifecycle (typically used by product vendors) and, later, an aligned mobile network operator-centric lifecycle. These lifecycles coincide when a network operator selects a given vendor product as part of their service offerings.

Product–Centric Lifecycle

Mobile network products are developed by vendors through their own lifecycle approach. A possible lifecycle is illustrated below. This section discusses the stages up to and including the Product Assurance and Certification stage. A later section describes the following product lifecycle stages where a product is actually deployed into an operational network.



The Define stage was discussed previously.

Product Design

Product design is an area of obvious competitive advantage and approaches may be honed over long periods to incorporate best practices. A number of security techniques may be utilised during this phase including:

- Adopting a Zero Trust[10] approach
- Adopting a secure by design philosophy
- Utilising internally recognised standards
- Implementing support for a secure root of trust
- Threat modelling
- Including support for application-based segmentation.

Product Development

Product development takes the design through to a viable product. Product development activity can sometimes take 12-18 months to complete but the total time between standards development and MNO service market launch may be 5+ years.

A number of security techniques may be utilised during this phase including:

- Utilising internally recognised standards
- Developing software through secure coding techniques
- Adopting a robust Software Development Lifecycle
- Protecting the code repository
- Undertaking source code analysis and peer review
- Checking backward compatibility through regression testing
- Management of the use of open-source software

[10] *National Institute of Standards and Technology (NIST) NIST Special Publication 800-207 Zero Trust Architecture*

Product Release

Product release enables the product to be formally released to market. A number of security techniques may be utilised during this phase including:

- Comprehensive Release notes and Build Specifications
- Availability of a Software Bill of Materials (SBOM)
- Provision of comprehensive security documentation and secure configuration guidance
- Support arrangements and associated Service Level Agreements

Industry Product Assurance and Certification

Product assurance and certification to an industry developed scheme was discussed in an earlier section of this report. To briefly recap, the objective of a security assurance scheme such as NESAS is to provide an industry-wide security assurance framework to facilitate strong baseline security levels across the whole industry.

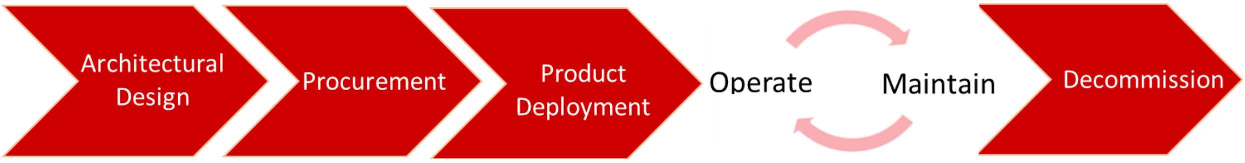
NESAS is of value to both operators and vendors and is intended to be used alongside other mechanisms to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network. These policies can also include the application of other published GSMA security recommendations and participation in the GSMA's operational security services such as CVD [8] and T-ISAC [9].

A significant strength of global certification scheme is that it provides an efficient, certify 'once', deploy globally outcome. It is recognised that security assurance and certification schemes have their limitations. As described earlier, they comprise just a part of an overall layered security strategy that supports legacy equipment and wider service arrangements with differing security strategies. Product security testing does not provide 100% protection certainty of immunity from attack. Deployment, configuration, patching and wider operational security are all vital in ensuring that a given product operates in a secure manner. Also, assurance and certification schemes must evolve over time as the threat landscape changes.

Security assurance is a cost component of mobile eco-system products and services. For global assurance and certification schemes this cost is effectively spread across all markets for a given product regardless of whether a global evaluation or certification is recognised in that jurisdiction. Since NESAS style evaluations are likely to become a mandatory regulatory requirement in many regional markets, it is important industry and governments work together to gain the benefits of global industry schemes regardless of whether a specific country solely adopts the global scheme or adds something in addition, or as an alternative.

A Mobile Network *Service* Lifecycle

This section examines a network service-centric lifecycle (typically used by network operators). This lifecycle coincides with the product lifecycle (discussed above) when a network operator selects a given vendor product as part of their service offerings. A possible lifecycle is illustrated below.



Architectural Design

For mobile network solutions the lifecycle begins with architectural design that will usually be undertaken at the systems level (i.e., deploying a *system* of products). A number of system-level security techniques may be utilised during this phase including:

- Adopting a Zero Trust approach
- Adopting a secure by design and privacy by design philosophy
- Adopting a secure by assurance or certification philosophy including evaluated products in the short or long list of possible vendor products
- Maximising vendor choice by utilising internally recognised standards
- Consideration of regulatory requirements
- Threat modelling and associated risk assessment

Procurement

The procurement lifecycle phase includes a range of activities that ultimately lead to vendor selection and deployment. Activities at this stage include development of vendor assessment criteria, budget allocation, agreement of commercial terms, invitation to Tenders (ITTs), shortlisting, Best and Final Offers (BAFO) and contract award purchasing decisions. This phase is characterised as commercially competitive, considers the whole life costs and will aim to adopt a multi-vendor procurement to enhance competitive cost advantages and to spread supplier risk.

The availability of equipment developed to internationally recognised technical standards enables access to the best value global supply market. By selecting products that are both standards compliant and security evaluated means the equipment is effectively cost neutral across all operators as these are already ‘sunk’ costs included within the product. It also enables the successful inter-working of multi-vendor choices.

National interventions in supply chain selections can act to limit the range (and competition) of vendor selection. There are emerging national and regional efforts to effect a longer-term increase in vendor choice. It is currently unclear as to the longer-term success of these initiatives given the intellectual property and open-source components that are common to most vendors. Additional national or deployment-specific requirements can increase costs, risk and deployment timescales.

Operate / Maintain

The Operate / Maintain lifecycle phase enables the deployment, test, roll-out and full-scale use of products and services (developed through the preceding network product lifecycle) to consumers. The duration of this phase varies but supply contracts and capital investments may typically assume 5 -10 year lifetime with review milestones (that can result in the asset lifetime being extended well beyond the original planned obsolescence). Managed service provision of support, remote software / control arrangements and service level agreements (SLAs) are important differentiators. Supply chain interventions due to new governmental legislation or policy stances can drive significant costs if a 'rip and replace' vendor change is enforced[11].

5G was designed to utilise virtualised / cloud infrastructure, the security of which is vital to the security of the 5G virtualised network functions. In this arrangement, security of software and its associated updates are vital to consider. Operators are moving more towards Development, Security, Operations (DevSecOps) processes that more closely integrate security considerations in the software builds. The advantage of this approach is to increase the speed of code deployment into live networks. As development and operations become more closely linked it allows a faster cycle time of code development and deployment and the potential to deploy smaller incremental code changes. Adopting the right assurance and certification scheme, can support in life patching and avoid full re-certification of software products.

Operate / Maintain can incorporate a range of security practices to augment baseline security including:

- Implementing least privilege controls
- Supporting role-based access control
- Implementing vulnerability management programmes and engaging in the GSMA CVD scheme
- Security Incident and Event Management
- Tracking and responding to threat intelligence and by sharing to protect the wider ecosystem through GSMA's T-ISAC service.
- Undertaking red team exercises to better understand the tactics of advanced persistent threat actors and attack vectors.

In addition to security assurance of 5G network functions, NESAS with appropriate SCASs, is able to evaluate many of the security challenges associated with virtualisation and cloud. NESAS, or similar approaches, provide limited assurance of DevSecOps aspects as evaluation of 5G Network Products alone cannot prevent poor deployment security or operational security hygiene choices (e.g., adequate separation of sensitive network functions from other functions). However, the benefit of assurance that individual products are initially secure on their own (which NESAS can attest), gives a much stronger security start point for DevSecOps aspects than without that initial assurance.

Decommission

Decommission / system closure terminates equipment and service usage and involves decommissioning, data deletion, system wiping and environmentally secure equipment disposal. Closure can be driven by a number of factors including equipment obsolescence, vendor ban, service closure (e.g., 3G) and lack of support.

[11] Eg https://www.lightreading.com/5g-and-beyond/replacing-huaweis-80000-5g-antennas-would-cost-germany-billions/d/d-id/783837

Engaging in GSMA's industry best practices

The GSMA is committed to building security resilience by providing a range of advice, guidelines, recommendations, working group activities, discussion fora and threat mitigations; some of which are outlined below. It is through these activities that the GSMA makes an ongoing contribution and provides leadership in mobile network security. GSMA member engagement in GSMA's security activities is straightforward, delivers real-time intelligence value and also acts to deliver long-term value through using existing and developing new valuable guidelines, services and recommendations.

Fraud and Security Working Group[12]

The GSMA's Fraud and Security Group (FASG) drives the GSMA's management of fraud and security matters related to mobile technology, networks and services. FASG provides an open, receptive and trusted environment within which fraud and security intelligence and incident details can be shared in a timely and responsible way. FASG has a number of sub-groups including the Fraud and Security Architecture Group, the Device Security Group, the Roaming and Interconnect Fraud and Security Group and the Security Assurance Group.

Network Equipment Security Assurance Scheme[13]

The Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and the GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and lifecycle management processes, as well as using 3GPP-defined security test cases for the security evaluation of network equipment products. The scheme has been designed to be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to define additional security requirements.

Telecommunication Information Sharing and Analysis Center (T-ISAC)[14]

The GSMA T-ISAC is the central hub of security information sharing for the telecommunications industry. Driven by the ethos "one organisation's detection is another's prevention", the T-ISAC operates on the principle that information sharing is essential for the protection of the mobile ecosystem, and the advancement of cyber security for the telecommunications sector.

Coordinated Vulnerability Disclosure Programme (CVD)[15]

The GSMA CVD programme gives security researchers a discreet route to disclose a vulnerability, affording the industry an opportunity to assess the impact and mitigation options, before details of the discovered vulnerabilities enter the public domain. The programme works with mobile operators, suppliers and standards bodies to develop fixes and mitigating actions to protect customers' security and trust in the mobile communications industry.

[12] https://www.gsma.com/aboutus/workinggroups/fraud-security-group
[13] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[14] https://www.gsma.com/security/t-isac/
[15] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

Security Accreditation Scheme[16]

The Universal Integrated Circuit Card (UICC) in mobile devices, and its associated applications and data play a fundamental role in ensuring the security of the subscriber's account and related services and transactions. The GSMA's Security Accreditation Scheme enables mobile operators to assess the security of their UICC and embedded UICC (eUICC) suppliers, and of their eUICC subscription management service providers.

eUICC Security Assurance[17]

The GSMA eUICC Security Assurance (eSA) scheme is an independent security evaluation scheme for evaluating embedded UICCs (eUICCs) against the provisions of protection profiles for eUICCs. The scheme aims to establish trust for service providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secure against state-of-the-art attacks. The scheme is based on the 'common criteria' methodology, optimised for GSMA-compliant eUICCs.

eUICC Compliance

In addition to the security assurance of eSIM solutions used with the mobile terminal, GSMA also defines and operates a global PKI scheme that is used to allow trust between the different entities in the eSIM ecosystem. This includes mechanisms to ensure relevant security assurance (eSA and SAS), as well as functional mechanisms to ensure interoperability. Satisfactory completion of the relevant compliance measures permits the issuance of a suitable PKI certificate so that products can be trusted in the overall ecosystem.

GSMA Security Publications[18]

The GSMA security website includes a number of informative and instructive publications, whilst GSMA members can exclusively access additional content specifically addressing a wide range of fraud and security topics. These include the GSMA Mobile Telecommunications Security Landscape reports.

Reach out to get involved!

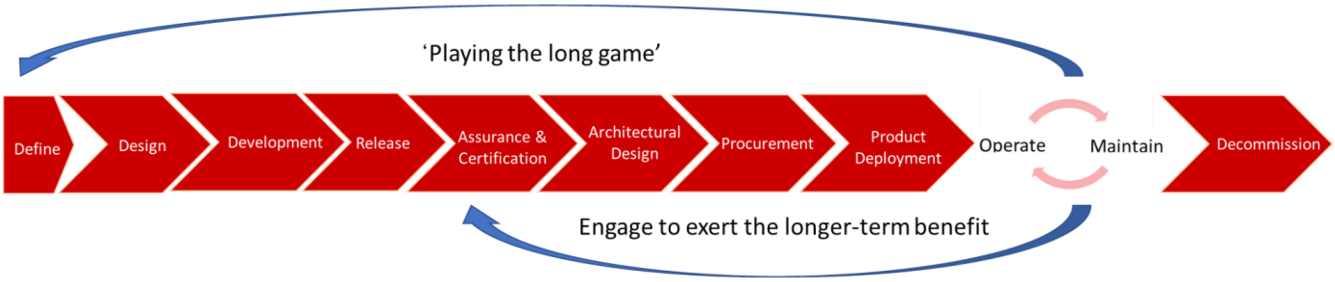
[16] https://www.gsma.com/security/security-accreditation-scheme/
[17] GSMA | GSMA eUICC Security Assurance: Test. Trust. Assure. - Services
[18] https://www.gsma.com/security/

The Art of the Long Game

An understanding of security risk coverage by mapping the sets of security controls (such as international standards, industry best practices, assurance scheme and certifications) allows an efficient security investment strategy to be developed. Existing systems, specific new technology and security assured product choices can lead to well developed baseline of in-built security controls. Any remaining security areas of risk can attract specific risk mitigation activities such as implementation of additional controls, contractual risk transference, risk acceptance and / or insurance.

The mobile industry has long aimed to deliver robust security enablers to protect its networks, customers and services. This security objective is delivered through a lifecycle approach starting long before a service goes live. The foundations of security are built through architectural design choices, choosing to adopt solutions utilising internationally recognised standards and shortlisting vendor solutions that already have a strong baseline security assurance built in.

The previous sections have illustrated how operational security is developed through an added-value lifecycle, where each stage contributes to the next. These lifecycle views come together as illustrated below.



Given the long in-life stage, there is considerable benefit for industry involvement in:

- Reaping a longer-term security benefit by actively supporting the development of international standards
- Applying and developing industry-developed security best practices through active engagement in GSMA's working groups
- Developing coherent vendor arrangements that avoid fragmentation through actively supporting and specifying the use of industry assurance and certification schemes such as GSMA's NESAS
- Strengthening the collective operational security response through threat intelligence sharing through joining and contributing to GSMA's T-ISAC scheme and security vulnerability sharing through GSMA's CVD scheme.

However, more fundamentally, with the EU and other regions already pursuing certification agendas (which are likely to become mandatory in the near future), it is important that industry comes together to develop, augment and promote fit for purpose industry schemes such as NESAS or SAS that address those regulatory needs. Having a scheme already in place which can demonstrate that real world security threats are being adequately mitigated provides the opportunity for "safe harbour", when regulators look to assess how to apply regulations.

Similarly, in most cases, developing such schemes or SCASs, as part of the technology development as 3GPP has done with its SCAS documents, is less industry impactful (e.g., cost and launch delays) than being forced to retro-fit/develop as an afterthought.

Finally, it is especially important that more mobile operators are actively involved in ensuring that NESAS, SAS or other schemes meet operator needs, as ultimately the operators are both the customers of the result of assurance and certification and they absorb the costs of those scheme (regional or global) regardless of whether they were initially involved in their creation.

The relative ease of engagement in these areas means that playing the 'long game' for security can deliver high impact engagements with long-term residual value.

Over the coming year, the GSMA will continue to support its members on a range of diverse critical security matters.

To get in touch, or to get more closely involved, please email security@gsma.com.