Telecoms Supplier Security Standard

Purpose

This document forms part of the Agreement entered into between a TRI Supplier and Sky and as such sets out the security obligations that Sky places on TRI Suppliers in relation to the protection of Sky PECNs and Sky PECSs. This document should be read in conjunction with the Telecoms Security Obligations set out in the Agreement.

The Telecoms Supplier Security Standard ("TSSS") is a supplementary document to the Sky Security Standard ("SSS") that identifies additional security requirements for suppliers whose goods, services, or facilities are provided or made available to Sky for use in connection with any Sky PECN or Sky PECS.

Sky will, from time to time, conduct audits of its telecoms suppliers to ensure compliance with Sky's security requirements (as described in the Agreement). The nature of the audit that will be performed will be communicated to Supplier by the Sky business relationship owner.

In the event of a conflict between these requirements, the SSS or any other security requirements that Sky may have specified then the most stringent requirement should be applied.

These requirements are intended to reflect the latest guidance from the UK's National Cyber Security Centre (NCSC) and OFCOM.

Sky may update these security requirements to reflect any updated official guidance from NCSC or OFCOM (or any other competent authority in the United Kingdom).

The latest version of these requirements will be available at: https://www.skygroup.sky/corporate/about-sky/suppliers

Certain terms used in this TSSS are defined in Appendix 1. Except where expressly stated otherwise, terms defined in other sections of the Agreement shall have the same meaning when used in this document.

Sky Telecoms Supplier Security Standard

If Supplier is a TRI Supplier, then it must demonstrate compliance with each of the applicable security standards set out in this document. The requirements are broken down by category of Supplier. Supplier is only required to comply with those requirements relating to the category of Supplier it falls within for the goods, services or facilities it is supplying to Sky. To the extent that the Supplier falls into more than one category it must comply with the requirements applicable to each relevant category. All TRI Suppliers must comply with the requirements of paragraph 7.

1. Measures applicable to suppliers of Network Equipment

1.1. If Supplier supplies Network Equipment, it must comply with the requirements of this paragraph 1. Supplier will also need to adhere to certain of these requirements if it provides professional services to deploy or configure Network Equipment or support for Network Equipment.

1.2. Supplier must provide a recommended up-to-date secure configuration of any Network Equipment it is providing to Sky.

1.3. Where a suggested secure configuration is supplied, it shall include the ability to disable management functionality not required for its specific purpose, and those management functionalities permitted shall be by secure, encrypted and authenticated protocols only.

1.4. Supplier must supply up-to-date guidance on how equipment should be securely deployed.

1.5. Supplier must ensure all equipment it deploys meets the recommended secure configuration (as a minimum), and that any deviation from this is recorded and the risk assessed in agreement with Sky. Supplier shall promptly notify Sky prior to a change being made to the way in which Network

Equipment operates that requires a significant change to the secure configuration of the Network Equipment.

1.6. Default passwords shall be changed upon initialisation of any device or service and before its use for the provision of the relevant network of service. Supplier may not include default credentials or hardcoded accounts in the initial configuration of products or services or use default credentials for any operational products or services deployed in respect of any Sky PECN or Sky PECS.

1.7. Supplier must provide to Sky a 'security declaration', signed off by Supplier at an appropriate governance level, that: i) explains how they produce secure equipment (and maintain the security of such equipment throughout its lifetime); and ii) records any differences in process across product lines. Supplier must ensure it maintains its equipment's security throughout its lifetime. The 'security declaration' must cover all aspects described in the Vendor Security Assessment submitted to Supplier by Sky and Supplier is encouraged to publish its response to the Vendor Security Assessment.

1.8. Supplier must maintain and adhere to, as a minimum, the standards set out in its 'security declaration'.

1.9. If Supplier claims to have obtained any internationally recognised security assessments or certifications of its equipment (such as Common Criteria or NESAS), Supplier must share with Sky the full findings that evidence this assessment or certificate.

1.10. Supplier must ensure that proprietary encryption algorithms are not used for any purpose, unless reviewed by independent qualified experts unaffiliated to the vendor in question and approved by Sky.

1.11. Where Supplier procures equipment for use in connection with any Sky PECS or Sky PECN, Supplier must ensure the security functionality of all such equipment has been tested during procurement, prior to contract award, including by ensuring Negative Testing and Fuzzing of Equipment interfaces.

1.12. Where Supplier uses third-party testing in relation to the security of the Network Equipment, this shall only be accepted by Sky if it is repeatable, performed independently of the Network Equipment supplier and is clearly applicable to Sky's deployment (e.g. relates to the hardware, software and configuration that is being supplied).

1.13. If Supplier chooses to outsource security testing to an independent third party, Sky shall be notified prior to finalizing the scope of the assessment and offered the opportunity to request additional information regarding the selected independent third party and the method of assessment proposed.

1.14. Supplier must have policies and procedures in place to take such measures as are appropriate and proportionate in the procurement, configuration, management and testing of equipment provided to Sky for use in connection with any Sky PECN or Sky PECS, to ensure the security of the equipment and functions carried out on the equipment.

1.15. Supplier must support all equipment and all software and hardware subcomponents supplied for the length of the Agreement. The period of support of both hardware and software shall be written into the Agreement.

1.16. Supplier shall publish an end-of-life bulletin significantly in advance of when their security support will end and, in any event, with at least 12 months' prior written notice (or such longer period as is agreed in writing between Supplier and Sky).

1.17. Supplier shall prioritise critical security patches over functionality upgrades wherever possible and deliver critical security patches separately to feature releases to maximise the speed at which the patch can be deployed.

1.18. Supplier must maintain records of and provide details (product and version) of major components used in the provision of Relevant Deliverables (including major third party components) and third party dependencies, including open source components and the period and level of support.

1.19. Supplier must establish (if not already present) and provide Sky with a copy of a vulnerability disclosure policy which should inform Sky of the single point of contact for Supplier and details around timescales of communication to Sky in the event of identification of a vulnerability. Supplier

shall include in its vulnerability disclosure policy a public point of contact for communication of vulnerabilities.

2. Additional measures applicable to CPE suppliers

2.1. If Supplier provides CPE, in addition to complying with the requirements of paragraph 1, it must also comply with the requirements of this paragraph 2.

2.2. Supplier shall ensure that WAN CPE management interfaces are only accessible from specified management locations (e.g. URL or IP address).

2.3. Supplier shall ensure that management of the CPE shall use a secure protocol (e.g. TLS 1.2 or newer).

2.4. Supplier shall ensure that the CPE's customer-facing management interfaces shall only be accessible from within the customer's network by default. By default, all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.

3. Additional measures applicable to suppliers of SIMs

3.1. If Supplier supplies SIMs, it must comply with the requirements of this paragraph 3.

3.2. Supplier shall ensure that a range of transport keys are used when transferring SIM key material.

3.3. Supplier shall ensure that the confidentiality, integrity and availability of sensitive SIM Card data is appropriately protected throughout its lifecycle.

3.4. Supplier shall ensure their security has been independently audited and shall share detail of such independent audits e.g. those performed under the GSMA's SAS scheme, to enable Sky to properly assess risks to sensitive SIM Card data.

4. Measures applicable to Third Party Administrators

4.1. If Supplier is a 3PA, it must comply with the requirements of this paragraph 4, and paragraph 5.8.

4.2. If Supplier has access to management systems, it must maintain (and promptly provide to Sky following any updates) an up-to-date record (including details of their roles, responsibilities and expected frequency of access) of all 3PA Supplier Personnel who:

4.2.1. have access to any Sky PECN otherwise than merely as end-users of a public electronic communications service provided by means of such Sky PECN;

4.2.2. have access to any Sky PECS otherwise than merely as end-users of the service.

4.3. Supplier must immediately notify Sky when an individual who is involved in the provision of Third Party Administrator services ceases to be an employee or subcontractor of Supplier or changes role so that their access can be timely updated.

4.4. Access by 3PAs to any Sky PECN shall be the minimum necessary to perform such 3PA's contractual function. In particular, access to security critical functions given to a person who uses any Sky PECS or Sky PECN shall be limited to that which is strictly necessary to enable the person to undertake the activities which Sky authorises the person to carry on.

4.5. Sky retains the right to determine permissions of the accounts used by 3PAs to access any Sky PECN and Supplier acknowledges that Sky may log and record all 3PA access into and all Privileged Access activity undertaken during any management session for any Sky PECN.

4.6. Supplier shall comply with Sky's directions in relation to their Supplier Personnel who are involved in the provision of Third Party Administrator services, including any direction from Sky that any member of Supplier Personnel should no longer have access to any Sky PECN.

4.7. 3PAs are not permitted to have routine, direct access to Network Equipment. Supplier shall only access Network Equipment via Sky designated mediation points owned and operated by a Sky Group member.

4.8. Supplier shall ensure that all Privileged Access is temporary, time-bounded and based on a ticket associated with a specific purpose. This access must be granted by someone other than the user performing the administrative activity.

4.9. Supplier must take such measures as are appropriate and proportionate to ensure that each user or system authorised to access security critical functions uses a credential which identifies them individually when accessing those functions and these must not be shared.

4.10. Supplier must implement technical controls to prevent one public electronic communications network provider, or their networks or environments from adversely affecting any other provider or their network (including Sky Group members or any Sky PECN) and implement both logical separation within their Third Party Administrator network to segregate customer data and networks and separation between 3PA management environments used for different provider networks. Supplier shall implement and enforce security enforcing functions at the boundary between its network and Sky's network.

4.11. Supplier must also implement technical controls to limit the potential for users or systems to negatively impact more than one provider. 3PAs must implement logically-independent PAWs per provider and independent administrative domains and accounts per provider.

4.12. Where there is a business need for doing so, Supplier may permit administrators to have multiple roles, each with its own account, provided the risk of doing so has been considered, accepted and communicated in agreement with Sky as part of Sky's risk management processes.

4.13. Supplier must monitor and audit the activities of their Supplier Personnel when accessing any Sky PECN.

4.14. Supplier shall:

4.14.1. maintain a record of all access by Supplier Personnel to security critical functions of any Sky PECN or Sky PECS, including the persons obtaining access;

4.14.2. identify and record all cases where Supplier Personnel's access to security critical functions of any Sky PECN or Sky PECS exceeds the person's security permission;

4.14.3. have in place means and procedures for producing immediate alerts of all manual amendments by Supplier Personnel to security critical functions;

4.14.4. provide to Sky promptly details of all activity undertaken by Supplier Personnel relating to security critical functions of any Sky PECS or Sky PECN to enable Sky to analyse promptly the details for the purpose of identifying any anomalous activity;

4.14.5. ensure all data required for the purpose of the monitoring and analysis obligations under Annex 2 and 4.14.1 to 4.14.3 (including for Network Equipment in security critical functions) is held securely for at least 13 months and promptly made available to Sky on request;

4.14.6. take steps to prevent activities that would restrict, in respect of any Sky PECN or Sky PECS, the monitoring and analysis required under the ECSMR.

4.15. Supplier shall share with Sky any logs related to the security of Supplier's network to the extent such logs relate to access into any Sky PECN in the form reasonably required by Sky from time to time to enable Sky's compliance with Telecoms Security Law.

4.16. Supplier must carry out its own regular testing for the purpose of identifying the risks of security compromises occurring in relation to the Sky PECN or Sky PECS. Supplier must promptly provide Sky with the outputs of such tests. The tests may include network or application penetration tests or tests of any part of the network or service which supports or serves or is involved in the provision of a Sky PECN and/or Sky PECS, including where underpinned by remote access methods. The test must involve simulating, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise. Supplier must ensure, so far as is reasonably practicable that:

4.16.1. the manner in which the tests are to be carried out is not made known to the persons involved in identifying and responding to the risks of security compromises occurring in relation to the network or service or the persons supplying any equipment to be tested, and

4.16.2. measures are taken to prevent any of those persons being able to anticipate the tests to be carried out.

The tests shall include tests in relation to the competence and skills of persons involved in the provision of the network or service and the possibility of unauthorised access to places where any Sky Group member keeps equipment used for the purposes of the network or service.

4.17. Any 3PA networks that could impact a member of Sky Group (as a provider of a PECN and/or PECS) must undergo the same level of testing as such Sky Group members apply to themselves (e.g. TBEST testing as set for Sky Group by Ofcom).

5. Measures applicable to Managed Service Providers

5.1. If Supplier is a Managed Service Provider, it must comply with the requirements of this paragraph 5. Suppliers who are Managed Service Providers must also comply with the requirements of paragraphs 4.8 to 4.11 and 4.13 to 4.17 and may need to comply with paragraph 1.19, if applicable to the Relevant Deliverables.

5.2. Supplier must operate on a least privilege basis, with accounts generated from a least privilege role template, modified as required. Supplier may only permit Supplier Personnel to access Sky's systems for the purpose of performing authorised responsibilities essential to their business role or function. Permissions associated with accounts shall not be copied from existing users. Non-persistent credentials (e.g. username and password authentication) shall be stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.

5.3. Supplier must require Multi Factor Authentication for access to an account capable of making changes to security critical functions. For accounts capable of making changes to security critical functions, the following measures shall be adopted relating to multi-factor authentication: (a) the second factor shall be locally generated, and not be transmitted; and (b) the multi-factor authentication mechanism shall be independent of the Sky PECN or the Supplier's network and PAW. Soft tokens (e.g. authenticator apps) may be used.

5.4. If Supplier is hosting a product or service for Sky, Supplier must conduct its own real-time monitoring in order to identify security events, alerts and incidents and promptly notify Sky of their occurrence, log all Privileged Access and provide Sky with those logs where reasonably requested.

5.5. Supplier must ensure:

5.5.1. all break-glass privileged user accounts must have unique, strong credentials per network equipment;

5.5.2. break-glass privileged user accounts are present for emergency access outside of change windows;

5.5.3. any persistent credentials and secrets (e.g. for break-glass access) are protected and not available to anyone except for the responsible person(s) in an emergency;

5.5.4. alerts are raised on use of any break-glass privileged user accounts/emergency accounts, the circumstances investigated to ensure suspension of these requirements has not compromised the network, and all activity logs audited post emergency. Where an 'emergency' event occurs, this shall be recorded and audited, along with the reason and time period for which controls were suspended;

5.5.5. where any break-glass privileged user account credentials are used, these are changed after use;

5.5.6. central storage for persistent credentials is protected by hardware means to ensure that data cannot be removed from the operational environment and accessed.

5.6. If Supplier exposes signalling functionality (i.e., has direct connectivity to external signalling networks on Sky's behalf), Supplier shall perform periodic assessment to understand what network equipment, network and Sky user data could be compromised through malicious signalling traffic and advise Sky of the same.

5.7. Supplier must ensure that if it is sending data over signalling networks on behalf of Sky, the external exposure of customer data, customer identifiers and network topology information is minimised.

5.8. Supplier will inform Sky if the operation of any part of a Sky PECN or Sky PECS takes place outside the United Kingdom and must ensure that any tools or functionalities which it is providing are not capable of being accessed from, and are not stored on, equipment located in a Listed Country.

5.9. If any tools are stored on equipment located outside the United Kingdom and enable monitoring or analysis: (a) in real time of the use or operation of the Sky PECN or Sky PECS; or (b) of the content of signals, Supplier shall provide information and assistance reasonably requested by Sky to enable Sky to take measures to identify and reduce the risks of security compromises occurring as a result of such tools being stored on equipment located outside the United Kingdom. Such information and assistance is only required where Sky is dependent on Supplier to identify and reduce the relevant risks.

5.10. Supplier will deploy effective security related patches to Network Equipment within either 14 days or a period notified to Sky that is proportionate to the risk of security compromise which the patch or mitigation addresses (and taking into account any reasonable requests made by Sky). Supplier will put in place effective alternative mitigations until the relevant patch has been deployed. Where a patch addresses an exposed, actively-exploited vulnerability, these patches must be deployed as soon as can reasonably be achieved, and at most within 14 days of release.

6. Measures applicable to NOF suppliers

6.1. If Supplier provides Network Oversight Functions, it must comply with the requirements of this paragraph 6.

6.2. Supplier must appropriately design and segregate Network Oversight Functions securely from other parts of Sky's or Supplier's network, with NOFs being housed and operated on Trusted Platforms.

6.3. NOFs shall not share trust domains or host pools with workloads that are not NOFs.

6.4. The management plane used to manage NOFs shall be isolated from other internal and external networks, including the management plane used by other equipment.

6.5. Supplier may only use dedicated management functions (e.g., Jump Boxes) to manage NOFs and Supplier may only access these functions through designated PAWs. Supplier must exercise control over these network management functions at all times. NOFs shall only access services (e.g. AAA, network time, software updates) over interfaces which are internally-facing to Sky.

6.6. Supplier must ensure that all significant or manual changes to NOFs/security critical functions are, before the change is made, proposed by one person authorised by Sky and approved by another person from among the responsible persons, assigned with an appropriate role.

6.7. Supplier must ensure that all changes to NOFs/security critical functions are automated wherever possible and are monitored in real time to alert for any unauthorised activity. Where automation is not possible, Supplier must ensure that suitable approvals have taken place for manual activity.

6.8. Supplier must ensure that all user access on NOFs is limited to a minimal set of trusted Privileged Users based on least privilege, pre-authorised by Sky and that such user access identifies a user individually.

6.9. Supplier must ensure that services supporting or containing NOFs (including operating system and application software) are rebuilt from an up-to-date known-good software state every 24 months. Supplier must ensure workstations or functions (e.g. jump boxes) (operating systems and above) used to manage NOFs, are rebuilt from an up-to-date known-good software state every 12 months.

6.10. Supplier confirms that any equipment performing NOFs is operated within the United Kingdom by UK-based employees using equipment located in the United Kingdom unless Supplier has agreed with Sky that is not reasonably practicable and an alternative location acceptable to Sky.

6.11. If a Supplier is providing MFA supporting or authorisation functions, they need to be in a separate security domain to the corporate security domain.

7. Measures applicable to all suppliers

7.1. All Suppliers must comply with the requirements of this paragraph 7.

7.2. Where Supplier requires access to information it shall request and hold the minimum information necessary to provide the Deliverables required.

7.3. If providing a support service to Sky, Supplier will keep its own records of the products and/or services used or intended to be used on the Sky PECN or Sky PECS including, but not limited to type, location, software, and hardware information and identifying information of equipment supplied by Supplier which is used or intended to be used as part of the network or service.

7.4. Where data is stored outside the United Kingdom, Supplier shall maintain a list of locations where the data is held and provide this to Sky upon request and Sky reserves the right to reject such locations for security risk reasons. No security permission may be granted to, or exercised by, a person while the person is in a Listed Country.

7.5. Supplier shall ensure that any network or user data it accesses is properly protected and only visible or accessible to appropriate employees from appropriate locations and shall provide Sky with such information and assistance as Sky may reasonably require to assess and verify the same.

7.6. Supplier shall avoid transferring control of Sky's network and user data to third parties, except where necessary. Any such transfer of control shall be limited to the necessary and defined purpose and shall be through a defined process in each case as agreed in advance with Sky. When sharing user or network data Supplier shall use an encrypted and authenticated channel.

7.7. Supplier shall share, via automated means as far as possible, indications of potential anomalous activity and Supplier shall support Sky to promptly assess, investigate and address potential malicious activity which may affect any Sky PECN, or Sky PECS.

7.8. Supplier shall supply necessary information (including details of normal system and traffic behaviour (e.g. source and destination, frequency of communication, protocols and ports used, and expected bandwidth consumed)) to enable Sky to update asset management and network monitoring systems in relation to all equipment and services supplied so that security staff can identify and track down anomalies within networks. If any of the information provided by Supplier under this requirement changes, Supplier must provide updated information to Sky without undue delay. For the avoidance of doubt, network changes that could impact network security shall be notified to those monitoring the network. Monitoring processes shall be maintained and modified if necessary.

7.9. Supplier must remediate all security issues that pose a security risk to a Sky PECN or Sky PECS discovered within products supplied by Supplier within a reasonable time of being notified, providing regular updates on progress in the interim. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.

7.10. Supplier shall ensure that information which could be used to obtain unauthorised access to any Sky PECS or Sky PECN (whether or not stored by electronic means) is stored securely.

7.11. Passwords and credentials must be managed, stored and assigned securely and revoked when no longer needed.

7.12. Supplier must avoid common credential creation processes and take other appropriate and proportionate measures to ensure that credentials are unique and not capable of being anticipated by others.

7.13. Supplier shall not use equipment that is no longer supported by their vendor in the provision of Relevant Deliverables to Sky, unless expressly agreed otherwise in writing with Sky.

7.14. Risks identified by persons involved at any level in the provision of the Sky PECN or Sky PECS are to be reported to: telecoms-supplier-risks@sky.uk.

7.15. If Supplier engages a third-party contractor for any goods, services, or facilities pertaining to any Sky PECN or Sky PECS, Supplier must ensure that it flows down all applicable security requirements under this TSSS to relevant third-party contractors by means of contractual arrangements, ensuring the third-party contractor is working to the same security standards in terms of the specific goods, services or facilities it is supplying, providing or making available to Supplier. Where Supplier is using third parties to provide goods, services, or facilities pertaining to any Sky PECN, Sky PECS, Supplier must, prior to contract, and at least annually thereafter, identify, document and address the risks (including as part of risk management and procurement processes) of a security compromise occurring in relation to a Sky PECS or Sky PECN as a result of things done or omitted by the third party

supplier (including risks arising during the contract lifecycle and as a result of other persons being used in the third party's relevant supply chain) and ensure it can continue to provide its Relevant Deliverables securely if the third-party contract is terminated.

7.16. Supplier acknowledges that Sky retains control and oversight of its network and user data.

7.17. Supplier shall collaborate with Sky to ensure there is a clear and documented shared-responsibility model as between Sky and Supplier.

Appendix 1 – Defined Terms

The following terms used herein shall have the following definitions:

“Agreement” means the agreement(s) between Sky and Supplier which incorporates this security standard by inclusion or reference

"Customer Premises Equipment" or “CPE” refers to equipment provided and managed by or on behalf of the Sky Group to customers of the Sky Group that is used or intended to be used as part of a Sky PECN or Sky PECS. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit.

"Fuzzing" means an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to assess a system’s vulnerability to them.

"Jump Box" means a system on a network used to access and manage devices in a separate security zone.

"Listed Country" means a country listed in the Schedule to the ECSMR (as amended, supplemented, or replaced).

"Managed Service Provider" means any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on Sky Group premises, in its managed service provider’s data centre (hosting), or in a third-party data centre and any other person specified as a Managed Service Provider under Telecoms Security Law.

"Management Network" is a collective term for systems that are responsible for the management of a Sky PECN.

"Management Plane" means the interfaces and connectivity and supporting equipment that allows Network Equipment to be managed.

"Multi Factor Authentication" (or "MFA") means an authentication method that requires the user to provide two or more verification factors to gain access to a resource.

"Negative Testing" means the process of validating the application against invalid inputs. Invalid data is used in testing to compare the output against the given input and results monitored for potential vulnerabilities.

"Network Equipment" means either software or hardware component of a Sky PECN that transmits or receives data or provides supporting services to components of the Sky PECN that transmit or receive data, including both virtual machines and physical hardware.

"NESAS" means the GSM Association’s Network Equipment Security Assurance Scheme: an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry.

"Network Oversight Function" (or "NOF") means the components of any Sky PECN that oversee and control the security critical functions, which make them vitally important in overall network security. They are essential for Sky to understand the network, secure the network, or to recover the network. These include systems that collect and process logging and monitoring data and MFA supporting and authorisation functions.

"Privileged Access" means an access to network equipment where greater capabilities are granted than a standard user or customer. Any access over the Management Plane, or to management ports of Network Equipment is Privileged Access.

"Privileged Access Workstation" (or "PAW") means an appropriately secured device which is able to make changes to security critical functions via a Management Plane.

"Privileged User" means a person who is granted Privileged Access, through their role, access and credentials, or through any other means.

"SIM Card" means a unique hardware component or token, and associated software, used to authenticate the subscriber's access to the network, encompassing the hardware UICC/eUICC, the SIM/USIM/ISIM applications, eSIM and RSP functionality and any SIM applets.

"Third Party Administrator" or "3PA" means any Managed Service Provider which provides group functions or external support for third party supplier equipment (e.g. third-line support function).

"Trusted Platform" means a secure platform which has the characteristics defined in Secure by default platforms - 22 September 2016.

"UICC" means any physical card SIM-like credential allowing network access, including permanently soldered-in UICCs in some handsets and IoT devices. (An eSIM does not require a UICC).

"Vendor Security Assessment" means the vendor security assessment aligned to the format prescribed in Annex B of the Code.