# 5G CYBERSECURITY CERTIFICATION SCHEME

## CALL FOR APPLICATIONS FOR THE AD HOC WORKING GROUP ON THE PREPARATION OF A CANDIDATE EU 5G CYBERSECURITY CERTIFICATION SCHEME

## 1. INTRODUCTION

The European Union Agency for Cybersecurity, ENISA, is the Union's Agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act[1], the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. To support and enhance the cybersecurity in the field of 5G, the Commission requested the Agency - in line with ENISA's mandate under Article 8 (1) (b) of the Cybersecurity Act - to prepare this candidate European cybersecurity certification scheme for 5G networks (EU 5G scheme).[2]

Within this framework, ENISA is now launching this call for the expression of interest in the 5G Ad Hoc Working Group (hereinafter referred to as the AHWG) in accordance with Article 49 (4) of the Cybersecurity Act and the ENISA Management Board Decision on Ad Hoc Working Groups for European cybersecurity certification schemes[3]. For further details regarding the key tasks of the AHWG, we refer to section 3.

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[2] Under the ENISA Single Programming Document 2020-2022, this activity is outlined under point O.6.1. The request is an element of a comprehensive EU approach on 5G cybersecurity translated into the EU 5G Toolbox of risk mitigating measures to support EU Member States enhancing their 5G cybersecurity.

[3] DECISION NO MB/2019/11 OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY ON THE ESTABLISHMENT AND OPERATION OF AD HOC WORKING GROUPS FOR EUROPEAN CYBERSECURITY CERTIFICATION SCHEME

# 2. BACKGROUND OF THE AD HOC WORKING GROUP

Upon completion of this call for expression of interest, the Agency will establish an AHWG. The establishment of AHWGs is provided in Article 20(4) of the Cybersecurity Act Regulation (EU) 2019/881, stating that *"the Executive Director may set up Ad Hoc Working Groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation*".. In addition, article 49(4) of the CSA provides the specific requirement that *"[f]or each candidate scheme, ENISA shall establish an Ad Hoc Working Group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise".*

The members of the AHWG are selected according to the highest standards of expertise, aiming to ensure appropriate gender, nationality and expertise balance with regard to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry (including SMEs), users, and academic experts in network and information security[4], with knowledge on the functioning of the Cybersecurity Market. Depending on the nature of the AHWG and its goals, selection criteria are defined. Along these lines, the Agency seeks to interact with a broad range of stakeholders.

# 3. SCOPE OF THE AD HOC WORKING GROUP

The work of this specific AHWG is related to the preparation of an EU 5G scheme. By considering general market trends and drivers, both at the demand and the supply side, the AHWG will support ENISA in the preparation of an EU 5G scheme.

The EU 5G scheme in general needs to:

- Comply to the CSA, provide consistency with other schemes of the EU cybersecurity certification framework and re-use the EU CC and EU CS or elements of those as far as possible.
- Fit seamlessly with the suite of solutions for 5G security created by the NIS cooperation group (EU coordinated risk assessment, 5G threat landscape, 5G toolbox)

The preparation of the EU 5G scheme includes to define the means for cybersecurity certification of 5G network components and processes (the how to certify, hereinafter referred to as the "certification means") related to the eUICC and the accreditation of stakeholders of the eUICC supply, and the remote SIM provisioning processes. Elements from current industry schemes GSMA's NESAS, SAS-SM, SAS-UP and eSA schemes, the relevant eUICC protection profile and ETSI/3GPP's 5G standards are planned to be re-used.

This process is planned to take place in cooperation with GSMA, a broad range of 5G stakeholders, such as industry, organisations, public entities, EU and/or national bodies, offices or agencies, standardisation organisations and international organisations.

In terms of the context where certification should be applied, the EU 5G scheme should concentrate on certified security for subscriber-related use cases of the 5G ecosystem. In particular:

1. The supply and deployment of identified 5G network equipment
2. Management of subscriber identities
3. Remote SIM provisioning
4. 5G authentication (incl. roaming)

[4] Recital 59 CSA.

5. Subscriber connectivity services

The programme for the preparation of the EU 5G scheme consists of 2 phases:

**Phase 1:**
1. "As-is" translation of elements of existing schemes into their EU-equivalents
2. Identification of security and certification requirements to the relevant use cases, components and processes based on the risk of their intended use
3. Identification of gaps and first outline of the necessary enhancements and/or improvements of the "as-is" versions of the certification means

**Phase 2:**
1. Implementation of enhancements / improvements.
2. Preparation and drafting of the EU 5G scheme

In Phase 1, the work of the AHWG will be subdivided into 3 Work Streams (WS) focusing on:
1. "As-is" translation of existing scheme elements into an EU-equivalent of NESAS
2. "As-is" translation of existing scheme elements into an EU-equivalent of SAS-SM and SAS-UP and GSMA's eUICC certification scheme
3. Risk-based definition of security and certification requirements for components that support the before mentioned use cases and gap analysis

The contents of Phase 2 will largely be defined by the results of the gap analysis, which will be conducted at the end of Phase 1.

This call for interest will therefore focus on Phase 1 with the option to either extend the existing AHWG with a reorganisation of Work Streams and members or members of the reserve list, or result in a new call for expression of interest for an AHWG for Phase 2.

# 4. APPLICATION PROCEDURE

ENISA is looking for support and expertise from the participants of the AHWG:
- as representatives of 5G stakeholders who are authorized to speak on behalf of their organisations and help us to understand the 5G stakeholder's objectives and provide views on the various aspects of the defined context (see chapter below on "scope"), and
- the representatives mentioned above should be experts who know in detail about the examined use cases and about the technical, security, operational and deployment aspects of certain areas of the defined context, aspects which are related to or covered by the type of 5G stakeholder they represent.

Experts in the required field are invited to submit their application to the Agency via the dedicated section on the ENISA web site. Applications must be completed in one of the official languages of the European Union. However, applications in English would facilitate the evaluation procedure. If a language other than English is used, it would be helpful to include a summary of the CV and/or the application in English. An application will be deemed admissible only if it is submitted before or on the deadline.

All applicants must specify whether they apply for full membership as an expert, or they apply for additional 'participant' status (see also sections 5 and 6) as representative of a 5G stakeholder organisation or a potential observer organisation.

In the application form, applicants will be required to declare the organisation they work for as well as other relevant affiliations and contractual relationships with third parties.

This call for interest will focus on Phase 1 with the option to either extend the existing AHWG with a reorganisation of Work Streams and members or members of the reserve list, or result in a new call for expression of interest for an AHWG for Phase 2.

**Required expert profiles**

ENISA, taking into due account the advice of the Commission, will assess the applications upon general criteria and upon the evidence for specific expertise as required per work stream of the AHWG.

As described before, the AHWG will be subdivided in 3 Work Streams. Each Work Stream requires a different skill set, competences and expertise of individual 5G stakeholder representations. National Authorities involved in the national 5G deployments, are invited to participate via the NIS Cooperation Group or other relevant Member States groups.

The following table provides an overview of the different fields of 5G expertise that should be represented in the particular work streams (WSs) and lists the required areas of expertise that applicants should demonstrate.

| 5G stakeholder types | AHWG – WS1 | AHWG – WS2 | AHWG – WS3 |
|---|---|---|---|
| **Consumer interest groups** | Representation as observer upon request | Representation as observer upon request | Objectives with services and use cases given in the 5G context<br>Potential risks for own objectives in the areas of security and privacy |
| **Standard development organisations** | 5G standards and industry specifications<br>ICT security and certification standards (incl. plans for future developments)<br>Terminology | eUICC specifications<br>ICT security and certification standards in particular ISO/IEC 15408 and PP, ISMS (incl. plans for future developments)<br>Terminology | 5G architecture and security architecture, ISO/IEC 27XXX, ISO/IEC 15408, risk and cybersecurity assessment, application of controls<br>Terminology |
| **Mobile network operators (MNO) / Mobile service providers** | Objectives and requirements with regards to the EU 5G scheme for network functions | Objectives and requirements with regards to the EU 5G scheme for the eUICC and the EU-equivalent of SAS-SM and SAS-UP | Sectorial trends, geopolitical context, business processes & objectives, targeted services<br>Potential risks for own objectives, information on threats, attack scenarios, cyber threat intelligence<br>Architecture and implementation aspects for all use cases within the selected 5G context (incl. customer identification and registration, payment), GSMA SAM<br>Aspects of security and assurance implementation (technical and business impact)<br>Objectives and requirements with regards to the EU 5G scheme |
| **Network equipment suppliers** | Security aspects of network equipment and the supply chain (incl. subcontractors or platform suppliers) | Not applicable | Mobile network equipment trends, geopolitical context, business processes & objectives<br>Potential risks for own objectives, information on threats, attack scenarios, cyber threat intelligence with focus on |

| 5G stakeholder types | AHWG – WS1 | AHWG – WS2 | AHWG – WS3 |
|---|---|---|---|
| | Auditing / evaluation of network equipment & related processes<br><br>Practical expertise in the application of GSMA's NESAS<br><br>Objectives and requirements with regards to with regards to the EU 5G scheme | | network equipment and the use cases 'network equipment supply and deployment', '5G authentication incl. roaming' and 'Subscriber connectivity services'<br><br>Objectives and requirements with regards to the EU 5G scheme |
| **eUICC suppliers** | Not applicable | Security aspects of eUICC and the eUICC supply chain (incl. subcontractors or platform suppliers)<br><br>Practical expertise in the application of SOG-IS or GSMA's GSMA eSA for the eUICC and GSMA'S SAS-UP<br><br>SOG-IS/EU-CC, PP-100, PP-084<br><br>Practical experience in the application of SAS-SM for stakeholders of the Remote SIM provisioning.<br><br>Objectives and requirements with regards to the EU 5G scheme | eUICC / ieUICC trends, geopolitical context, business processes & objectives<br><br>Potential risks for own objectives, information on threats, attack scenarios, cyber threat intelligence with focus on eUICC and eSIM provisioning and the use cases 'Subscriber ID management', 'Remote SIM provisioning'<br><br>Technical implementation and security aspects of the eUICC supply chain and the RSP process<br><br>GSMA SAM<br><br>Objectives and requirements with regards to the EU 5G scheme |
| **Subscription management platform service providers (SM-DP+, SM-DS)** | Not applicable | Implementation and security aspects of the RSP process (incl. subcontractors or platform suppliers)<br><br>Practical expertise in the application of GSMA'S SAS-UP<br><br>Practical experience in the application of SAS-SM for stakeholders of the Remote SIM provisioning.<br><br>EU/CSA schemes<br><br>Objectives and requirements with regards to the EU 5G scheme | RSP trends, geopolitical context, business processes & objectives<br><br>Potential risks for own objectives, information on threats, attack scenarios, cyber threat intelligence with focus on eUICC and eSIM provisioning and the use cases 'Remote SIM provisioning' and '5G authentication'<br><br>Technical implementation and security aspects of the eUICC supply chain and the RSP process<br><br>GSMA SAM<br><br>Objectives and requirements with regards to the EU 5G scheme |
| **Mobile device suppliers** | Not applicable | eSE and its use as secure platform for mobile applications, eUICC, GSMA SAM | Potential risks for own objectives, information on threats, attack scenarios, cyber threat intelligence with focus on |

| 5G stakeholder types | AHWG – WS1 | AHWG – WS2 | AHWG – WS3 |
|---|---|---|---|
| | | EU/CSA schemes<br>Objectives and requirements with regards to the EU 5G scheme | eUICC and support of mobile applications by eSE or eUICC<br>Objectives and requirements with regards to the EU 5G scheme |
| **CABs, testing laboratories** | Auditing / evaluation of network equipment & related processes<br>GSMA's NESAS<br>Objectives and requirements with regards to the EU 5G scheme | Evaluation for SOGIS / EU-CC, PP-100, PP-084<br>GSMA's SAS-UP, SAS-SM<br>Objectives and requirements with regards to the EU 5G scheme | Not applicable |

Representatives of 5G stakeholders who apply for the participation in an AHWG work stream should demonstrate all the expertise requested for this stakeholder type in the work stream. Under this condition, applicants may apply for the participation in more than one work stream.

Also, experts who are not representing a 5G stakeholder organisation may be selected if they demonstrate top level expertise in several areas of expertise required by an AHWG work stream.

In addition, all AHWG members must comply with the following general selection criteria:

- Representatives must be mandated and empowered by their 5G stakeholder to support the AHWG's decisions.
- The members are expected to participate actively to AHWG meetings, to prepare and contribute to the work of the AHWG. There must be a commitment to an availability of 1 or 2 working days a week and the flexibility to work for the AHWG partially outside working hours because of possible time zone differences.
- Experts must demonstrate at least 3 years practical experience in the requested areas of expertise as displayed in the table above.
- Good knowledge of English allowing active participation in the discussions and in the drafting of related deliverables.

### 4.1 DEADLINE FOR APPLICATION

This call is launched on the 7th of June 2021 and it will remain open until 30 June 2021 at 12:00 EET (Athens time zone). After the deadline, no incoming applications will be taken into consideration.

# 5. APPOINTMENT OF MEMBERS

The members of the AHWG shall be appointed by the Executive Director of ENISA from a list of suitable applicants duly selected in line with this call, followed by the establishment of a list of the most suitable applicants. If there are more suitable candidates than the number of members needed in the AHWG, a reserve list of candidate members will be established. Whenever an AHWG member leaves the AHWG, the Executive Director will appoint a new member selected from the reserve list. The appointment will be for a period equal to the duration of the AHWG, prolonged if deemed necessary and appropriate. The selection of members is based on the selection criteria given in chapter 3 of this ToR.

Members that are no longer capable to contribute effectively to the group's deliberations, or members that in the opinion of the Agency do not comply with the confidentiality conditions set out in Article 339 of the Treaty on the functioning of the European Union or who resign, will no longer be allowed to participate in meetings of the AHWG and may be replaced for the remaining duration of the AHWG by members on the reserve list.

The members of the ad hoc working group, as well as invited experts and observers, are subject to the obligation of professional secrecy, which by virtue of the Treaties and the rules implementing them applies to all members of the institutions and their staff, as well as, by analogy, to the Commission's rules on security regarding the protection of Union classified information, laid down in European Commission Decisions (EU, Euratom) 2015/44310 and 2015/444.[5]

# 6. ORGANISATION OF THE AD HOC WORKING GROUP

### GENERAL RULES

The AHWG will be managed under the responsibility of experts of the Agency. Project management and administration will be covered by ENISA staff.

The activities of the AHWG will follow a structure and work plan that will be proposed by ENISA in the kick-off phase of the AHWG. For the time being, due to COVID-19 conditions, the AHWG, its work streams and task forces shall convene only virtually. In the future meetings in premises of the Agency may be possible depending on the circumstances.

The results and state of the work of the AHWG will be shared with the participants and will be presented frequently to ENISA's stakeholders.

Apart from formal members of the AHWG appointed by the Executive Director of the Agency, there are other roles contributing to the work of the development of the scheme: there are parties participating in the role of observer and in the role of additional participant.

### OBSERVERS

In the development of this scheme there are many stakeholders that have an interest in following the developments of scheme building. Those parties that are not directly involved in the development of the scheme but nevertheless have a clear and justified interest due to the type and role of their organisation, can be given a role as observer. Observers can attend meetings, may contribute to discussions and ask questions to allow them to follow the developments in the scheme. They cover their own expenses.

### ADDITIONAL PARTICIPANTS

5G stakeholders may be invited to nominate their representatives as additional participants, if there is a duly justified need for specific expertise (e.g. in proof-of-concept experiments or other experimental activities). These participants are not appointed as AHWG members, but contribute to the work because of their expertise in the specific field. They cover their own expenses.

# 7. TRANSPARENCY

The members, additional participants and observers of the AHWG are subject to the obligation of confidentiality according to article 27 of Regulation (EU) 2019/881 and by virtue of the Treaties and the rules implementing them applies to all members of the institutions and their staff, as well as, by analogy, to the Commission's rules on security regarding the protection of Union classified information, laid down in European Commission Decisions (EU, Euratom) 2015/44310 and 2015/444.[6] In addition, they are also subject to the conditions of Regulation (EC) No 1049/2001 on access to documents[7]. Therefore, everybody is subject to the obligation to sign a statement of

5 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).
[6] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).
[7] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Exceptions are intended to protect public security, military affairs, international relations, financial, monetary or economic policy, privacy and integrity of the individual, commercial interests, court proceedings and legal advice, inspections/investigations/audits and the institution's decision-making process.

confidentiality. This statement of Confidentiality is as annex 3 attached to the Executive Director Decision upon the appointment of the AHWG.

The members, additional participants and observers of the AHWG should share information within their organisation only on a need-to-know-basis and when duly justified, unless the information is indicated by writing, or by announcement of the Chair of the AHWG or of particular Work Streams as confidential by classification. Information of the AHWG can only be made public upon prior approval of the AHWG Chair.

After official publication by ENISA of the list of appointed AHWG members, they are allowed to disclose their membership to the public and describe the general scope of the work of the AHWG.

## 7.1 DECLARATION OF INTEREST

The members, additional participants and observers of the AHWG are subject to the obligations of article 25 (2) of the Regulation (EU) 2019/881. Members of the Management Board, the Executive Director, and external experts participating in ad hoc working groups, shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.

If there is a conflict of interest, the relevant member shall bring this forward without undue delay and declare in writing, any conflicting interests that might be considered to be prejudicial to their independence in relation to the items on the agenda. Each member of the AHWG will be provided a form where they can indicate to which items of the agenda there are alleged conflicts of interest. He or she shall abstain from participating in the discussion of and if applicable voting on such items. This applies only to the topic of the agenda that raises the conflict of interest, meaning that the AHWG member can fully participate in the meeting related to all the remaining topics. As a rule, a draft agenda of the AHWG meetings will be available prior to the meetings.

The signed declaration forms of AHWG members are subject to article 26 (2) of Regulation (EU) 2019/881 meaning that the Agency is obligated to make the declarations on interest public in a register. Upon the dissolution of the AHWG the declarations of interest of all members will be removed from the public register. If members leave the AHWG before the dissolution of the AHWG, the data will likewise be removed from the public register.

If there are any unclear issues relating to the Governance, the confidentiality requirements and/or interests of the AHWG that interfere with the personal, professional and/or organisation interests that the AHWG member represents, the member will bring this to the attention of the Chair of the AHWG or of particular Work Streams in order to look for a mutual, workable solution, in accordance with these Internal Rules of Operation.

If there are any unclear issues relating to the Governance of the AHWG, the confidentiality requirements and/or interests of the AHWG that interfere with the personal, professional and/or organisation interests that the AHWG member represents, the member will bring this to the attention of the Chair of the AHWG or of particular Work Streams in order to look for a mutual, workable solution, in accordance with these Internal Rules of Operation.

## 7.2 DECLARATION OF IPR

Participants of the AHWG will be requested to report upon kick-off of the AHWG or as soon possible during the operation of the AHWG if they have knowledge of IPR related to the subjects discussed.
Inputs by AHWG participants which involve IPR will only be considered in duly justified cases. In such cases, the participants shall explicitly declare the relevant IPR to ENISA.

If AHWG members do not bring forward any IP right, or timely changes related to these rights, they cannot hold the Agency responsible for the consequences of the (re)-use of the material and possible subsequent IP right infringements of these parties.

# 8. PERSONAL DATA PROCESSING

ENISA ensures that personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[8]. Personal data is processed according to a personal data protection notice that has been made publicly available. ENISA is supervised by the EDPS, http://www.edps.europa.eu. For any further enquiries, you may contact the ENISA Data Protection Officer at: dataprotection@enisa.europa.eu.

# 9. REMUNERATION OF EXPERTS

In exceptional cases, individual experts may be eligible for remuneration due to a certain role assigned by the Agency. They may be remunerated for their expertise related to the specific deliveries in the AHWG, in line with the ENISA Financial Regulation.[9]

# 10. REIMBURSEMENT

Members of an AHWG may be reimbursed for their travel and subsistence expenses. If a member is from a location other than the location required for the provision of services or place of meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost effective) from the European country/city in which the contractor is officially registered to another European city.
2. A "per diem" applicable to the country in which the meeting will take place is based upon the allowance set by the European Commission[10].
3. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible as member.

Representatives of Member States, observers and additional participants are neither remunerated nor reimbursed.

# 11. TERMINATION OF THE MANDATE OF THE AD HOC WORKING GROUP AND DISSOLUTION

When the tasks of the AHWG will be completed and in case no prolongation will be planned, the end-of-life phase of the AHWG will follow. In this phase ENISA in consultation with the AHWG will propose which outputs available will be archived or will be maintained further, taking into account IP rights (copyright, use of logo's, labels, etc.).

In principle most AHWG material, in particular the AHWG deliverables, will be made publicly available, but all copy rights are reserved under ENISA, as changes to the EU 5G scheme material are subject to the implementing act of the Commission. This is why any use of the material generated by the AHWG group should be subject to discussion and brought under the right type of copyright. This may also lead to return or deletion of

[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
[9] "ENISA Financial Regulation"
[10] https://ec.europa.eu/international-partnerships/system/files/per-diem-rates-20200201_en.pdf

some of the material that is in the hands of AHWG members and not deemed suitable for re-use or any type of reproduction or distribution.

Once all tasks are fulfilled of the AHWG and no prolongation is planned, the AHWG will be honourably discharged from its duty and dissolved.

# 12. LIST OF ABBREVIATIONS

| | |
|---|---|
| 3G | 3rd Generation Mobile Network |
| 3GPP | 3rd Generation Partnership Project |
| 5G | 5th Generation Mobile Network |
| AHWG | Ad Hoc Working Group |
| CSA | EU Cybersecurity Act |
| CV | Curriculum Vitae |
| ECCG | European Cybersecurity Certification Group |
| EDPS | European Data Protection Supervisor |
| ENISA | European Union Agency for Cybersecurity |
| eSA | eUICC Security Assurance |
| eSIM | Embedded SIM |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| EU 5G scheme | Candidate EU 5G cybersecurity certification scheme, in preparation under the CSA |
| EU CC scheme | Candidate EU Common Criteria cybersecurity certification scheme, in preparation under the CSA |
| EU CS scheme | Candidate EU cybersecurity certification scheme for Cloud Services, in preparation under the CSA |
| eUICC | Embedded Universal Integrated Circuit Card |
| GSMA | Global System for Mobile Communications (GSM) Association |
| GSMA SAM | GSMA Secure Applications for Mobile |
| IEC | International Electrotechnical Commission |
| ieUICC | Integrated eUICC |
| IPR | Intellectual Property Rights |
| ISMS | Information security management system |
| ISO | International Organisation for Standardization |
| MNO | Mobile network operator |
| NCCA | National cybersecurity certification authorities |
| NESAS | Network Equipment Security Assurance Scheme |
| SAS | GSMA Security Accreditation Scheme |
| SAS-SM | Security Accreditation Scheme for Subscription Management Roles |
| SAS-UP | Security Accreditation Scheme for UICC Production |

| | |
|---|---|
| NIS 5G SG | Subgroup on standardisation and certification of the 5G Work Stream of the NIS Cooperation Group |
| NIS 5G WS | 5G Work Stream of the NIS Cooperation Group |
| PP | Protection Profile |
| RSP | Remote SIM provisioning |
| SIM | Subscriber Identification Module |
| SM-DP+ | Subscription Manager Data Preparation (enhanced) |
| SM-DS | Subscription Manager – Discovery Server |
| SME | Small and Medium-sized Enterprise |
| SOG-IS | Senior Officials Group-Information Security Systems |
| WS | Work stream |