T-ISAC Service Offering
Version 2.0
16 March 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

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.

Table of Contents

1 Introduction

1.1 Overview

Information sharing is essential for the protection of the mobile ecosystem, and the advancement of cybersecurity for the telecommunications industry.

Sector-specific Information Sharing and Analysis Centres (ISACs) are non-profit, member-driven organisations formed to share information within the industry.

Historically the GSMA have managed threat sharing on an ad-hoc basis. Rather than managing these threats reactively and engaging informally, the GSMA developed the Telecommunication Information Sharing and Analysis Centre (T-ISAC) to act as the sector specific ISAC for the mobile telecommunications industry.. The service provides a place where security issues from the Mobile Industry can be raised, managed and discussed in a trusted environment.

The GSMA T-ISAC proposal was initially conceived by the GSMA's Fraud and Security Advisory Panel (FSAP) [1] to provide an industry tailored capability to respond to the increased volume and complexity of security threats. This proposal was developed further by the GSMA's Technology Group's (TG) [2] Fraud and Security Group (Group FASG) [3] and was sponsored and approved by the GSMA Board [4] in February 2018.

It is essential for industry organisations, such as the GSMA, to lead and have in place processes that are capable of sharing any security threats that could impact the industry and its customers. The GSMA T-ISAC provides proactive and reactive threat alerting, intelligence sharing and a dissemination service which is interoperable with any existing functions or contacts within an organisation.

The GSMA T-ISAC is keen to cooperate in order to better protect the mobile industry, mobile users and the wider industry ecosystem. The GSMA does so in accordance with the GSMA T-ISAC process defined in this document.

1.2 Objectives

The main objective of the GSMA T-ISAC is to provide a forum in which information and intelligence regarding cyber threats against its members can be shared and published in a secure and trusted manner, to better protect the industry from cyber security threats as a whole.

GSMA Security Operations encourages GSMA members from across the mobile ecosystem to join the GSMA T-ISAC (Annex C). The GSMA T-ISAC operates under a single ethos of "One person's detection is another person's prevention" and relies on the sharing and dissemination of proactive and reactive intelligence.

The objectives and steer of the GSMA T-ISAC are agreed by the GSMA T-ISAC Governance Team (see 4.3) and must provide value to all GSMA members; recognizing that these members will have varying security maturity. The GSMA T-ISAC Governance team comprises of Subject Matter Experts (SME) within GSMA member organisations who operate or support various Intelligence, Security Operations Centre (SOC) teams and Cyber Security Incident Response Teams (CSIRT).

1.3 Scope

This document outlines the policy, process and functionality of the GSMA T-ISAC, ensuring the rights and responsibilities are clearly understood and delivered correctly.

This document, and its associated components, has been built around best practice recommendations contained in FIRST [5], RFC [6] , and NIST [7] detailing expectations regarding CSIRT functions.

The GSMA T-ISAC model is for GSMA members only, and is interoperable with its constituencies existing functions (e.g. CSIRT, Security team, Fraud Team).

Additionally, the GSMA T-ISAC will provide input into the industry threat landscape and associated resources to support GSMA member activities.

1.4 Abbreviations and Definitions

Term	Description
CSIRT	Cyber Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
Goverance team	This team consists of GSMA staff, GSMA T-ISAC members and representatives from the GSMA's Fraud and Security Group (FASG). They manage the strategic requirments for the T-ISAC
NIST	National Institute of Standards and Technology
Press team	The team manage all press related activities for the T-ISAC
RFC	Request for Comments
Service Manager	The service manager is responbile for the day to day management of the T-ISAC
SOC	Security Operations Centre
Security Operations Director	The role is accountable for the T-ISAC service
T-ISAC	Telecommunications Information Sharing and Analysis Centre
TLP	Traffic Light Protocol

1.5 References

Ref	Doc Number	Title
[1]	FASP	https://infocentre2.gsma.com/gp/bsg/TG/FSP/Pages/Default.aspx
[2]	TG	https://infocentre2.gsma.com/gp/bsg/TG/Pages/Default.aspx
[3]	FASG	https://infocentre2.gsma.com/gp/WG/FSG/Pages/Default.aspx
[4]	GSMA Board	https://www.gsma.com/aboutus/leadership/gsma-board
[5]	FIRST	https://www.first.org/
[6]	RFC	https://www.ietf.org/standards/rfcs/
[7]	NIST	https://www.nist.gov/
[8]	Membership Types	https://www.gsma.com/aboutus/wp-content/uploads/2019/08/AA.16-v3.19.pdf

Ref	Doc Number	Title
[9]	Member NDA	https://www.gsma.com/aboutus/wp-content/uploads/2019/08/AA.16-v3.19.pdf
[10]	MISP	https://www.misp-project.org/
[11]	TLP	https://www.first.org/tlp/. Further information regarding the TLP and how to utilise appropriately can be found in the Participant Pack referenced in section 2.3.4 of this document.
[12]	NIST (CSF)	https://www.nist.gov/cyberframework
[13]	GSMA CVD	http://gsma.com/cvd
[14]	T-ISAC	https://infocentre2.gsma.com/gp/wg/FSG/WAR/Pages/Default.aspx

2 T-ISAC Services

The GSMA T-ISAC services aim to serve both and support proactive and reactive intelligence use cases. The GSMA T-ISAC aligns the services against the NIST Cyber Security Framework (CSF) [12]:

1. Intelligence Sharing
2. Security Advisory
3. Intelligence Alerting
4. Reporting

2.1 Intelligence Sharing

Summary	The GSMA T-ISAC will host a solution to support intelligence sharing between constituents. This service is to encourage all to share anomalies and industry-wide impacting issues.
Platform	Malware Sharing Indicator Platform (MISP)[10]
Definition	The GSMA T-ISAC will research and develop strategic, operational and tactical cyber threat intelligence (CTI) to be provided to members. Based on industry trends, specific topics or general CTI, this may be developed by the GSMA, GSMA T-ISAC Members or Strategic Intelligence Partners. GSMA T-ISAC will also develop and own a platform to facilitate intelligence sharing, taking in feeds from GSMA T-ISAC members and Open Source Intelligence (OSINT), assess the intelligence and publish via the sharing platform.
Interface with Other Services	Security Advisory, Security Advisory, Reporting

Table 1: Intelligence Sharing

2.2 Security Advisory

Summary	**Security Advisory will provide threat assessment and recommended actions based on known issues targeting the telecommunications industry.**
Definition	Provide GSMA T-ISAC members with assessments and advice on particular cyber threats targeting the industry. Security Advisories may be provided by members, in reference to mobile devices, applications or infrastructure. Inputs may also include submissions to the GSMA's CVD [13] programme.
Interface with Other Services	Intelligence Sharing, Intelligence Alerting

Table 2: Security Advisory

2.3 Intelligence Alerting

Summary	**GSMA T-ISAC constituents receive up to date security alerts regarding the latest threats. A member receives only those alerts that are relevant to them to which they have signed for via the relevant platform.**
Platform	**T-ISAC Mailing List [14]**
Definition	Alerting GSMA T-ISAC members to the submission of new intelligence or events through the GSMA T-ISAC provided sharing platform. In the event of a major issue or threat, high-priority alerts may be pushed to all GSMA T-ISAC members to inform them of the issue.
Interface with Other Services	Intelligence Sharing

Table 3: Intelligence Alerting

2.1 Reporting

Summary	This service is a quality management service for the industry, to provide reports that support sharing with the GSMA T-ISAC as well as understand the current state of the industry. All of the above services are subject to the reporting service.
Definition	Developing and sharing reports based on the GSMA T-ISAC performance as well as industry trends and global reported activity. There will be monthly, quarterly and yearly reporting to highlight the number of submissions received into the GSMA T-ISAC to the Governance Team and GSMA leadership. Reports can be requested by contacting the GSMA T-ISAC Director(s) at the GSMA.
Interface with Other Services	Intelligence Alerting, Security Advisory, Intelligence Sharing,

Table 4: Reporting

3 Governance

As the GSMA T-ISAC is provided by members, for members, the GSMA ensure that the voice and opinion of the industry is heard via the GSMA T-ISAC Governance Team (see Table 5).

This team consists of GSMA staff, GSMA T-ISAC members and representatives from the GSMA's Fraud and Security Group (FASG). Please contact the GSMA T-ISAC Service Manger (see Annex C) for more information on how to join this team.

Every 2 months, the Governance Team will meet to discuss the development and requirements for the T-ISAC. Actions will be taken and tracked by the GSMA T-ISAC Service Manager (see Table 5)

4 GSMA T-ISAC Membership

4.1 Membership Types

In order to build and maintain trust in the services provided by the T-ISAC, the constituency consists of GSMA members [8] which fall into the following categories:

- Operator Members -as defined in the GSMA Articles of Association (AA.16).
- Associate Members & Rapporteurs as defined in the GSMA Articles of Association (AA.16).

Industry affiliated partners of Operator Members may be regarded as part of the constituency. Invitation requests can be made from current GSMA T-ISAC members. Final sign off of these additionals sits with the Security Operations Director.

4.2 GSMA Responsibilities

The GSMA is fully committed to the GSMA T-ISAC programme and recognises the value in engaging with industry and providing this service to strengthen the industry security posture. For its part, the GSMA endeavours to:

- Focus on industry-wide impacting threats.
- Assess factors such as the efficacy of the submission, the accuracy of the threat, the quality of the report submitted, the severity and global applicability of the vulnerability, etc.
- Treat cases with confidentiality, unless required not to in order to comply with legal obligations.

4.3 GSMA T-ISAC Roles and Responsibilities

Roles	Responsibility
Security Operations Director	• Service Owner (Accountable for service delivery) • Communicate escalations to the GSMA CTO, Board, FSAP, and FSMT as required. • Shape the GSMA T-ISAC strategic roadmap, aligning to industry needs
GSMA T-ISAC Members	• Be a GSMA member • Regularly engage with the GSMA T-ISAC to consume and share information. • Exercise caution and restraint with regard to personal or company data. • Classify shared information appropriately based on the Traffic Light Protocol. • Ensure compliance with data protection regulations and local law.

Roles	Responsibility
	• Refrain from using the GSMA T-ISAC to replace any regulatory reporting responsibilities.
GSMA T-ISAC Service Manager	• Coordinate GSMA T-ISAC • Provide a professional single point of contact for GSMA's members. • **Respond with acknowledgement to all TLP [Amber] and TLP [Red] submissions** • Act on reports of incidents from outside the constituency. • **Keep the submitter informed of the progress particularly pertaining to the remediation action (where applicable).** • **Treat submissions with confidentiality. Do not share any identifiable details, unless required to in order to comply with legal obligations.** • Feedback to the constituency, reporting threats or vulnerabilities. • Conduct post-incident reviews (if deemed necessary) • Manage the Intelligence Sharing platform(s) • Develop reports based on industry trends. • Pass information about vulnerabilities to the T-ISAC. • Coordinate GSMA T-ISAC Governance Team and invite the relevant SMEs to the meetings • Drive the GSMA T-ISAC strategic roadmap
Governance Team	• To provide support to the Service Manager in order to resolve incidents as quickly as possible. • Provide expert insights and co-ordination of relevant information sources etc. • To review and assess the development of the GSMA T-ISAC to ensure it aligns to members requests and views
GSMA Press Team	• Responsible for all statements made to the press regarding GSMA T-ISAC and industry wide threats on behalf of the GSMA members. • Contact point press@gsma.com

Table 5: GSMA T-ISAC Roles and Responsibilities

4.4 Membership Documentation

The GSMA T-ISAC has developed a membership pack containing best practices regarding cyber threat intelligence and information sharing. The pack includes; FS.32 GSMA T-ISAC Service Offering (this document), Executive Briefing, Confidentiality Statement, Participant Pack and access to media content for training and education.

Executive Briefing: The GSMA recognises that membership to an external body or program incurs resource, time and potential financial investment. Therefore, the Executive Briefing is a short, high level document summarising the T-ISAC, with the aim to help organisations get buy-in from executive and/or board level leadership (0).

Participant Pack: Members are encouraged to partake in intelligence sharing; the GSMA provides platform(s) to make this easier and caters to varied security maturities. The Participant Pack provides a detailed guide on how to onboard, interact and make the most of all the services provided by the T-ISAC. The Participant Pack is aimed at the day to day user

sharing intelligence (e.g. Security Analyst/Engineer, Cyber Threat Intelligence and Security Management).

GSMA Member Confidentiality Statement: GSMA members sign Article 18.1 of the GSMA Articles of Association (AA.16) when they join the GSMA [8]. This article outlines the expected Non-Disclosure Agreement (NDA) regarding confidential activities between GSMA members.

Media Content: The GSMA T-ISAC platform is composed of a number of technical components. The GSMA recognises that not all members will have the ability to integrate with the primary platform. GSMA T-ISAC has developed video content to instruct and train new and current members on how to use the platform. This media content is aimed at anyone wanting to interact with the GSMA T-ISAC and its members and can be provided to on boarded members of the GSMA T-ISAC.

5 Secure Communication

Due to the nature of the intelligence shared within the T-ISAC, data classifications are followed to ensure confidentiality for GSMA T-ISAC members. Participants of the GSMA T-ISAC should classify any incident or information shared with an appropriate classification according to TLP [11]. Advisories and reports issued from GSMA T-ISAC may incorporate information from initial submission(s), provided this does not breach the TLP marking.

The GSMA provides a Confidentiality marking for documents, table 2 providing a map of these markings against TLP. Submissions using other classification markings (e.g. Confidential, Classified and Secret) will not be accepted.

Secure communication channels are required to achieve confidentiality, integrity and authenticity. This is enforced by the GSMA T-ISAC as follows:

- The ability to protect the shared information using a pre-shared key encryption service. This ensures that there is a method of communication that is secure and verifiable.
- Article 16 of the GSMA Membership, this article outlines the expected Non-Disclosure Agreement (NDA) regarding confidential activities between GSMA members.

Traffic Light Protocol (TLP) / GSMA Confidentiality Marking	Description (NIST Guidelines)
RED GSMA Confidential – Member Only	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.
AMBER GSMA Confidential – Member Group Only	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.

GREEN GSMA Confidential – All GSMA T-ISAC Members	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.
WHITE Non-Confidential – Openly Shared	TLP: WHITE information may be distributed without restriction.

Table 6: GSMA and TLP confidentiality markings

6 Disclaimers

The service information contained in this document may be subject to change without prior notice. Access to and distribution by the GSMA of this, and any associated, documents is made pursuant to the regulations of the GSMA.

The GSMA Telecommunication Information Sharing and Analysis Centre (“GSMA T-ISAC”) is intended to protect the safety of mobile networks and mobile end-users alike. Any information provided or activities associated with the GSMA T-ISAC are for “information only” and provided “as is”. Any representations, warranties and guarantees of any kind (whether expressed, implied, or statutory, including without limitation any warranties of merchantability, fitness for a particular purpose, non-infringement, quality, accuracy, completeness, title or quite enjoyment) are expressly disclaimed and excluded.

A beneficiary of any activity or recipient of any information associated with the T-ISAC, will only be able to engage in such activities or receive any information without reliance on, representations, warranties or guarantees of another parties. The GSMA T-ISAC Governance Team, the GSMA, its officers, employees, contractors, consultants, member and affiliated parties:

i. hereby disclaims any liability with respect to a the accuracy, completeness or timeliness of any actions or information; and
ii. shall not be liable for any consequences, claims (including third party claims), obligations, promises, agreements, disputes, demands, damages or causes of action, known or unknown, now or in the future, in relation to any documentation, materials, information or activities;

Associated with the GSMA T-ISAC (irrespective if such information or actions were provided by themselves or a third party);

The information associated with the GSMA T-ISAC does not necessarily reflect the views and opinions held or constitute an endorsement of any views and opinions by the GSMA T-ISAC Governance Team, the GSMA, its officers, employees, contractors, consultants, member and affiliated parties.

Annex A Execuritve Briefing

T-ISAC_1_PAGE.pdf

Annex B Triage and Analysis

As part of the triage process, threats will be categorised and mapped to a severity matrix.

Severity	Description
None	No impact to the GSMA membership or wider industry. Usually for information only.
Low	Minimal effect on the GSMA membership or wider industry. Low impact incident or intelligence submission. Minor impact to member organisation and no potential to impact the wider industry.
Medium	Moderate effect on the member or wider industry. Some impact to member organisation or possibility to impact a small section of the wider industry.
High	Critical impact to member or wider industry. Significant potential to impact other members. Substantial impact to member organisation or high potential to impact the wider industry.

Table 7: Severity Matrix

Where required the GSMA T-ISAC Service Manager will conduct initial triage of submitted intelligence and respond appropriately aligned with the severity matrix. The GSMA T-ISAC Service Manger will operate under Service Level Obligations (SLOs) for any required response.

Severity	Initial Response (working days)	Subsequent Response (working days)	Target Formal Notification (working days)
None	N/A	Ad-hoc	N/A
Low	10	20	Month
Medium	5	10	Business Week
High	2	<5	72 hours

Table 8: Service SLO

Annex C GSMA T-ISAC Contact Information

These are the full details for how to contact the T-ISAC:

Name: GSMA Telecommunication Information Sharing and Analysis Centre

Mailing Address: The Walbrook Building, 25 Walbrook, London, United Kingdom EC4N 8AF

Website: gsma.com/t-isac

Email Address: t-isac@gsma.com

Public Key:

GPG Key ID – 5F6D72F2

GPG Fingerprint – 3E72 6A23 4B45 4042 34FC 2969 6704 1D0B 5F6D 72F2