
# Guidelines for Independent Remote Interconnect Security Testing

## Version 1.0

## 03 November 2017

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

### Security Classification: Non-confidential



### Copyright Notice



### Disclaimer



### Antitrust Notice

# Table of Contents

# 1 Introduction

## 1.1. Overview

Systems and infrastructures, with their inherent and surrounding security properties and mechanisms, may be designed and intended to function securely and resist attacks on their confidentiality, integrity and availability. It is, however, prudent to subject systems and infrastructures to security testing to verify the effectiveness and adequacy of these properties and mechanisms. While such testing and verification should be performed by the owner or provider of infrastructures and systems, the entity using or receiving the resulting services, as well as third parties with said entities' interests in mind, may find it valuable to perform their own testing. Within IT and Internet, independent remote third party security testing and research of products and services exposed to the general public (as distributed products or Internet-exposed services and interfaces) has become commonplace; and even a valued source of knowledge, where researchers are encouraged by industry actors welcoming responsible disclosure and some also offering reward ("bug bounty") programs. The telecommunications industry has also come of age in this respect, for its publicly exposed interfaces.

Regardless of any premise of sender and carrier responsibilities for responsible and controlled use of their assigned global title (GT) ranges, the signalling and interconnect networks are in reality semi-open. While advanced attackers may gain a presence by their ability to influence a national operator or by actually running an operation of their own, it is apparent that for a multitude of reasons even lesser resourced actors are able to gain and use a presence on telecommunications signalling and interconnect networks, and use said access relatively arbitrarily for potentially nefarious purposes.

Realising the above paradigm change from "closed network" to "exposed interfaces", the growing need for security testing is apparent. Operators' maturity, both in securing their signalling and interconnect interfaces as well as in realising the need to test them for verification of the resulting security, differs substantially. This has prompted third parties with varying motivations to perform unsolicited (as seen by the receiving party) security testing over interconnect.

While the well-intentioned independent security testing over interconnect potentially brings great value and should be embraced by the industry, it may also entail non-negligible operational risk and raises a number of questions such as when to regard observed activities as malicious, whether notification is required, how to handle and disclose findings, requirements for minimum competence and qualifications of the testing party, the distribution of responsibilities between sending GT owner, testing outfit and carrier, and more.

These guidelines are not built on a false assumption of a closed network. Instead, they recognise that security testing, and malicious misuse of access to the signalling and interconnect networks, will be a reality regardless of any guidelines. However, these guidelines serve to outline how the industry expects responsible unsolicited security testing over interconnect to be performed, and what the industry actors will regard as benign (non-malicious). They are a framework within which entities performing or aiding in such testing may choose to operate, thus having the benefit of industry actors treating their testing as benign.

## 1.2. Scope

This document provides guidelines on the security roles and responsibilities of testers and signalling interconnect partners in relation to the performance of independent remote interconnect signalling security testing as described in this document. Independent remote testing is considered to be third-party initiated testing in the absence of any testing request, agreement or guidance from the destination network.

Testing requested by operators from contracted testers will be subject to terms and conditions developed and agreed by the parties in advance, so is not within the scope of this document.

This document is primarily intended for use by testers, and for reference by mobile network operators, and any organization that uses a signalling interconnect with mobile operators.

This document is intended to be technology-neutral. It applies to existing interconnect technologies such as Signalling System Number 7 (SS7), GPRS Roaming Exchange (GRX), Diameter and IP Exchange (IPX) but also to future technologies.

## 1.3. Abbreviations

| Term | Description |
|---|---|
| AVP | Attribute Value Pair |
| CVD | Co-ordinated Vulnerability Disclosure |
| DNO | Destination Network Operator |
| DoS | Denial of Service |
| DRA | Diameter Routing Agent |
| EAP-AKA | Extensible Authentication Protocol Method for Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement |
| GRX | GPRS Roaming Exchange |
| GT | Global Title |
| IMSI | International Mobile Subscriber Identity |
| MAP | Mobile Application Part |
| MSISDN | Mobile Station International Subscriber Directory Number |
| MVNO | Mobile Virtual Network Operator |
| ONO | Originating Network Operator |
| IPX | IP Exchange |
| PCAP | Packet Capture |
| PRD | Permanent Reference Document |
| SCCP | Signaling Connection Control Part |
| SIM | Subscriber Identity Module |
| SNO | Spoofed Network Operator |
| SS7 | Signalling System Number 7 |
| STP | Signalling Transfer Point |
| UICC | Universal Integrated Circuit Card |

### 1.4. References

| Ref | Doc Number | Title |
|---|---|---|
| [1] | GSMA PRD BA.20 | Fraud Prevention Procedures |
| [2] | GSMA PRD FS.22 | Co-ordinated Vulnerability Disclosure |
| [3] | ISO/IEC 27001:2013 | Information Technology – Security Techniques – Information Security Management Systems; http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534 |
| [4] | ISO/IEC 29147:2014 | Information Technology – Security Techniques – Vulnerability Disclosure; http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170 |
| [5] | ISO/IEC 30111:2013 | Information Technology – Security Techniques – Vulnerability Handling Processes; http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231 |
| [6] | N/A | GCCS – Introducing Responsible Disclosure: Experiences in The Netherlands: A Best Practice Guide; https://www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf |

# 2 Interconnect Security Testing Roles

This section explains the different interconnect security testing roles

## 2.1 Tester

The tester initiates the sending of interconnect signalling messages via originating host equipment and a signalling network to the destination network. The originating host equipment and network address used to send the messages may belong to the tester or may be provided to the tester by a third party. For example, a telecommunications network operator may lease an SS7 GT address or range to a security researcher.

### 2.1.1 Assumptions regarding the tester:

- Has legitimate or authorised access to the interconnect signalling network (e.g. SS7), and is performing testing in accordance with the conditions of that access. Testing conducted via a compromised originating mobile network and without that operator's knowledge is not acceptable.
- Should seek to possess SIMs of the destination network or have confirmed consent (with evidence of consent) of the subscribers for that SIM. If SIM possession or consent is not practically achievable, the tester should use test International Mobile Subscriber Identities (IMSIs)/ Mobile Station International Subscriber Directory Numbers (MSISDNs) from the destination network operator (DNO), if such test IMSI/MSISDN range and information is available. If neither of the options above are possible, testing against random IMSIs is only permitted with the explicit permission of the DNO and in compliance with applicable data privacy regulations.

- Has sufficient knowledge and experience of interconnect signalling to know if significant risk, damage or operational impact at the destination network is likely to be caused by the testing.
- The tester might have knowledge and insight of the network topology.

## 2.2 Originating Network Operator (ONO)

The originating network grants use of its signalling equipment and/or part of its allocated network address range to the tester.

## 2.3 Destination Network Operator (DNO)

The destination network receives the interconnect signalling messages sent by the tester.

Types of destination networks:

- Destination network operators that allow independent remote testing, provided that:
    - It is not malicious;
    - It does not affect the service of subscriptions other than those held by the tester or subscriptions for which the tester has obtained consent to test against; and
    - Advance notification is given to the DNO by the tester (as described in section 4.2)
- Destination network operators that do not wish to receive unsolicited interconnect signalling messages for testing or other purposes, and treat all such messages to be malicious.

If a subscription used for interconnect security testing is being used in a roaming environment, both the home network and the visited network should be considered as DNOs.

Independent remote testing by a tester without providing advance notification to the destination network is considered irresponsible as any signalling traffic, even innocuous looking and legitimate, may cause unexpected and service-affecting behaviour within the destination network and requires the operator to be ready for this. It may also increase the time and effort necessary by the destination network to restore normal service and operations. Such testing may be considered as malicious by the destination network.

Assumptions regarding the DNO

- As the testing is independent, it is assumed that the DNO has not (at least intentionally) provided network information to the tester.
- The DNO may provide test IMSI/MSISDN ranges to the tester, either by advertising them publicly, or in response to tester requests.
- Messages are received by a live production network, and not a test environment. For some attack scenarios, test environments do not provide reliable results (e.g. different screening and filtering and security policy, normal load from other users missing, some nodes not present e.g. charging).
- Maintains a publicly advertised and easily discoverable contact channel for testers to provide advance notification to, which is monitored by MNO staff able to recognise

and act on such notifications. The use of a dedicated mailbox is recommended (e.g. security@<MNO_name>.com), although it should be acknowledged that MNOs and corporate operator groups may maintain different contact addresses to facilitate appropriate routing of communications, e.g.

- security.<country>@<globaldomain>.com
- security@<country>.<globaldomain>.com
- security@<localoperatordomain>.com).

### 2.4 Spoofed Network Operator (SNO)

For some legitimate test cases involving impersonation, the tester may wish to spoof the originating network address of signalling messages. Use of spoofing should be limited to test cases where such behaviour is essential to uncover vulnerabilities (e.g. test if originating-address based security controls can be bypassed). Other than that spoofing should not be used.

The tester should seek to use alternative addresses within the originating network range if possible, and only use the address space of a third party where absolutely necessary. A third party spoofed network operator (SNO) whose address is spoofed will receive answer messages from the DNO. The tester should obtain consent from the SNO to use its network address, in order to avoid negative operational and reputational impact on the SNO.

## 3 Interconnect Security Testing Types

### 3.1 Prior Knowledge Level

Interconnect security testing may be classified into the following categories based on the prior knowledge held by the tester:

- White-box testing: Testing performed with knowledge of the internal structure/design/implementation of the object being tested.
- Grey-box testing: Testing performed with partial knowledge of the internal structure/design/implementation of the object being tested.
- Black-box testing: Testing performed without prior knowledge of the internal structure/design/implementation of the object being tested.

To ensure that test results reflect real-life use cases, this document assumes that independent remote interconnect security testing will include grey-box and black-box testing. MNOs should assume that genuine attackers may have some information about the destination network (e.g. IMSIs of targeted subscriptions) prior to an attack.

Non-targeted attacks don’t require an attacker to have prior access to specific IMSI information. Any valid IMSI is sufficient for such attacks, and this could be guessed or deduced by a genuine attacker by trial and error or by prior information gathering.

### 3.2 Network Infrastructure Denial of Service (DoS) Attack Testing

Testing of potential DoS attacks against network infrastructure should be done in close co-operation with the DNO due to the associated risk of operational impact. Network infrastructure DoS testing is considered to be any testing that may result in the exhaustion of a network infrastructure resource or service. For example, nesting of attribute value pairs

(AVPs) in Diameter to the extent that stack resources could be exhausted would be considered a DoS attack or fuzzing. DoS testing against network infrastructure is therefore not acceptable as part of independent remote testing and is out of scope for this document.

As seen in practice, even innocuous and legitimate signalling traffic may trigger bugs in signalling software, and may crash or cause denial of service against infrastructure of the DNO or even infrastructure on the signalling path (Signaling Connection Control Part (SCCP) carrier, GRX/IPX carrier, intermediate Diameter Routing Agents (DRAs), intermediate Signalling Transfer Point (STPs), etc.) These involuntary DoS events cannot be foreseen and should not be considered after the fact (a posteriori) as DoS attack testing.

# 4 Responsibilities of the Tester

## 4.1 Test Equipment Security

The tester's equipment deployed in the ONO should be compliant with basic security requirements.

Testers should also consider the need to adequately protect their signalling-attached/-capable equipment against unintended harm (e.g. if the tester is sending messages that may trigger unexpected response messages from the DNO) and from malicious attacks from both public networks and the ONO local network (e.g. attempts by a malicious party to use the equipment to send malicious traffic in parallel with independent security testing traffic).

## 4.2 Before Testing Begins

The considerations and actions for the tester are illustrated in Figure 1 and described below.

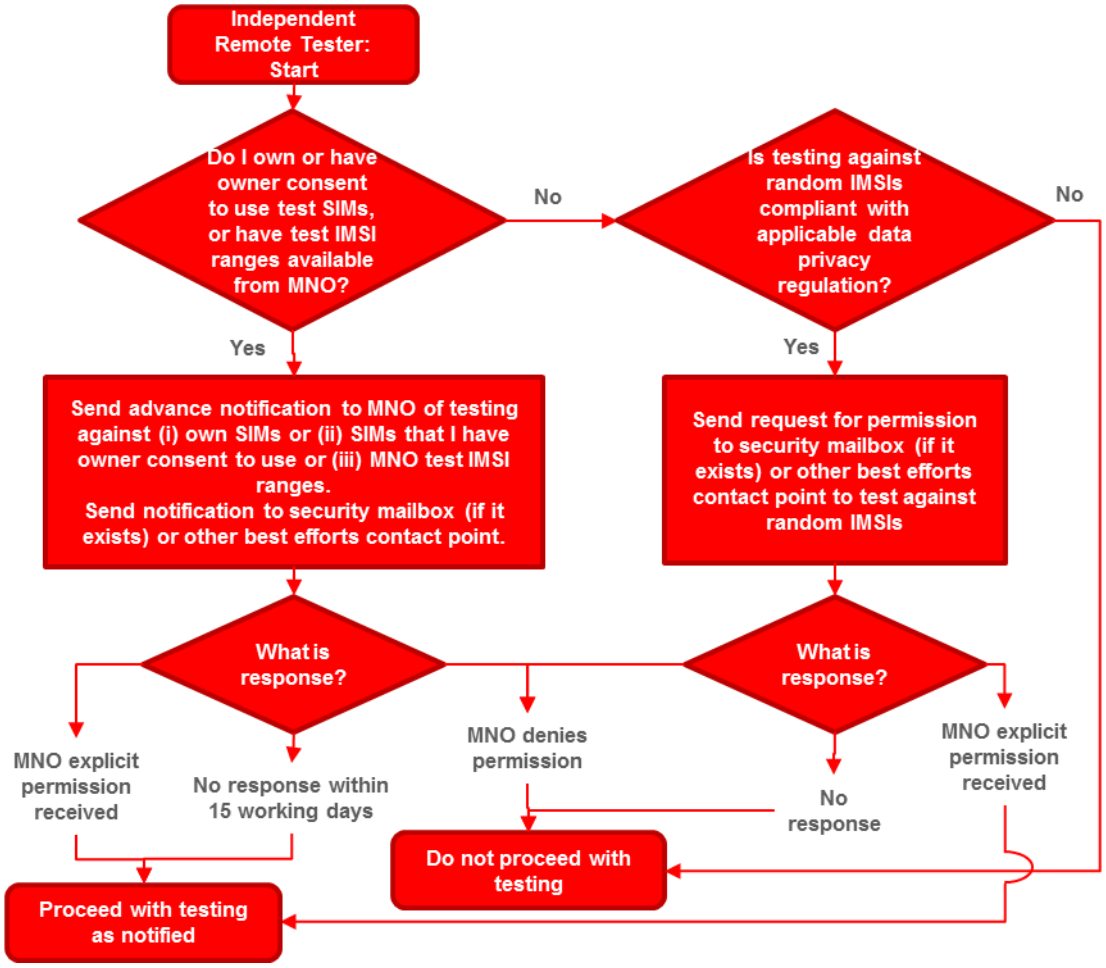


**Figure 1 - Obtaining permission to perform testing**

### 4.2.1 Legality and Operator-Specific Policies

A tester should confirm that performing independent remote testing is legal in the relevant jurisdictions before performing any such testing. The most relevant jurisdiction would be the country of the DNO. Other jurisdictions that might be relevant could be the country where the tester is located and the country where the originating signalling equipment is located. If a DNO has a publicly advertised policy on independent remote testing (e.g. testing is not permitted; testing is permitted without explicit DNO consent), the contents of that policy will take precedence over these guidelines, and that policy should be adhered to by the tester.

### 4.2.2 Test Notification to DNO

Testers should identify themselves and provide advance notification of independent remote testing to the DNO in advance of such testing, in accordance with the timeframes specified below. If test SIMs are in a roaming network during the test, testers should notify both home and visited DNOs.

If possible, advance notification should be sent to the DNO that hosts the signalling or core network equipment, rather than to a mobile virtual network operator (MVNO) that may be hosted on a network.

The tester shall provide advance notification via the publicly advertised contact channel to the DNO (e.g. security@<MNO_name>.com). If no publicly advertised contact channel is apparent to the tester, he may contact the GSMA (security@gsma.com) to request a security contact point at the DNO. The GSMA will share security contact point details at the DNO (if available) with the tester.

Notification should include, as specifically as possible without compromising the purpose and outcome of the testing, the following information:

- The contact details of the tester (email address and phone number at a minimum)
- The approximate date and time of the start and end of the tests, so that precise timing and sources cannot be used to interfere with the outcome of the test as noted below,
- Test objectives (e.g. eavesdropping, charging avoidance, location tracking)
- The nature of the tests, i.e. one time tests or repeated testing (whether successful or not)
- The list of messages that the tester intends to send
- The destination network addresses or prefixes that will be used during the testing. Optionally, the origin address or prefix may be indicated by the tester but that may be used to interfere with the outcome of the test, so in this case it is kept optional as noted below.
- The maximum rate and approximate number of messages that will be sent during this period.
- As the signalling will usually deviate from what has is normally sent by the ONO, the notification should explicitly state this.

NOTE: Some types of tests, typically large scale benchmark style tests, should not require advance disclosure (in notification) of the precise time and the sending information (e.g. GTs, IP, Origin Realm and Origin host), as this would permit operators to put in place temporary controls to artificially influence the outcome of the tests. DNOs that want to be part of independent remote testing may have to accept not having advance knowledge of the precise time and originating GTs used in testing.

If a tester will be testing using SIMs that they own or have owner consent to use, they may notify the DNO of this. The tester may optionally share the associated IMSIs with the DNO. If the tester does not have ownership or owner consent to use specific SIMs for testing, they may request test IMSIs/MSISDNs from the DNO or use test IMSI/MSISDN ranges published by the DNO if available. If a tester wishes to test against other specifically targeted or random IMSIs, they should clearly specify this as part of the advance notification, so that the DNO can consider this when deciding whether to grant testing permission or not.

The tester should request the DNO to provide details of a point of contact within the DNO who will be available during the tests.

The tester should provide the DNO with a reasonable opportunity (at least fifteen business days in the DNO country of operation) to indicate if it wishes to be excluded from the test activity (opt-out), and to provide point of contact details. The tester should comply with any DNO request to be excluded from the test activity.

In case of opt-out, the tester may indicate that the operator has opted-out in the publicly disclosed results of the testing.

If the DNO agrees to testing only under certain conditions (e.g. at specific times), then such testing is no longer considered independent, as it is subject to the influence of the DNO as part of a separate contract. The tester must decide whether to engage with the DNO and proceed in accordance with the DNO's conditions (outside the scope of this document), or not to include that DNO in the test campaign.

If a tester is using the equipment or network address of an ONO, they may have obligations to notify the ONO of their testing plans. Such obligations are for agreement between the tester and the ONO and are out of scope of these guidelines.

#### 4.2.2.1 Testing in the Absence of Explicit DNO Permission

Both testers and DNOs should ideally seek to have explicit agreement in place between them in relation to whether permission to perform independent testing has been granted. However, the absence of explicit DNO permission should not prevent independent remote testing in some cases (see below), since such testing, if done in a responsible manner, increases security and ultimately benefit the DNO's customers.

The guidance provided below is intended to facilitate independent remote testing and reduce the burden placed on the tester. However, the tester should be aware of the risk that a lack of response from the DNO does not preclude legal action from DNO and/or local authorities toward the tester at a later stage.

- If the tester does not get a reply from a DNO within fifteen business days of sending notification of his intention to test **using the tester's own SIMs, SIMs that the tester has owner permission to use, or DNO-allocated test MSISDN/IMSI ranges**, the tester may proceed with testing in accordance with the notification provided.

  If the tester becomes aware that their attempt to notify the DNO via the primary advertised or assumed contact point (e.g. security@<MNO_name>.com mailbox) fails, the tester may request details of a security contact at the DNO from GSMA (security@gsma.com). The tester may try to contact the DNO using different approaches (e.g. multiple emails to multiple contacts, telephone, social networking) to give the DNO the maximum opportunity to opt-out of independent remote testing. If the tester can reasonably assume that their notification has been delivered to a suitable contact point at the DNO, but no response has been received, they may proceed with testing.

- If the tester does not receive explicit permission from a DNO to test **using random MSISDN/IMSI ranges**, the tester may not proceed with testing.

### 4.3 Signalling Standard Compliance

The signalling used should be syntactically and sequentially correct in accordance with valid technical standards. Any approved versions of technical standards are permitted, specifically old versions.

Proprietary extensions of the signalling may be used in order to elicit knowledge of specific vulnerabilities in specific proprietary equipment, provided they do not intend DoS testing or other discouraged testing.

MNOs are unlikely to want to receive syntactically incorrect signalling, as it may cause unexpected disruption. It may also disrupt the signalling carrier equipment. Sending syntactically incorrect messages is usually part of DoS testing or used to get remote code execution into a network node. Both are very dangerous scenarios for a network and should not be part of independent remote testing, as described in section 3.2.

In general, any kind of fuzz testing should not be part of independent remote testing, as described in section 3.2.

## 4.4 During Testing

### 4.4.1 Messages Used

The signalling used must not be intentionally harmful to, significantly degrade or otherwise be of a nature that can reasonably be expected to cause harm or significant degradation of receiving operator's network or services, also including the receiving operator's customers.

The signalling used shall not cause monetary loss to the ONO or DNO to any significant degree or for deliberately fraudulent purposes. Testing shall be only sufficient to prove a security or fraud vulnerability and not to exploit it for monetary gain. No costs shall apply and no billing items be visible to any subscriber not acting as a test SIM.

The signalling used shall be at a modest volume and should not be likely to constitute a denial of service attack.

This document does not try to exhaustively list messages that should or should not be permitted. Even messages believed by the tester to be harmless may cause problems (e.g. denial of service) if sent in large volumes. The tester should instead accept responsibility to not intentionally do any harm to network operations, and to be sufficiently qualified to make an informed judgement on the level of risk associated with their actions.

The subsequent sections give general guidance on the types of signalling that are permissible in different circumstances and specific examples for clarity. Notwithstanding the fact that this document is primarily technology-neutral, the examples given are SS7 Mobile Application Part (MAP) messages that should be permitted from an independent remote testing point of view (implicitly authorised) and which should not (require explicit authorisation from DNO in advance). This list is not intended to be exhaustive.

#### 4.4.1.1 Messages That Extract Information

Some messages are designed to extract information such as IMSI or location and not affect the state of the subscriber. These messages are very unlikely to cause harm if sent in modest volume from a valid or a spoofed origination. The tester may send these messages during testing, subject to the conditions described in section 4.2.

Examples from SS7 MAP include:

- MAP_PROVIDE-ROAMING-NUMBER (OpCode: 4)

- MAP_SEND-PARAMETERS (OpCode: 9)
- MAP_INTERROGATE-SS (OpCode: 14)
- MAP_SEND-IDENTIFICATION (OpCode:15)
- MAP_SEND-ROUTING-INFORMATION (OpCode: 22)
- MAP_SEND-ROUTING-INFO-FOR-GPRS (OpCode: 24)
- MAP_CHECK-IMEI (OpCode: 43)
- MAP_SEND-ROUTING-INFO-FOR-SM (OpCode: 45)
- MAP_SEND-AUTHENTICATION-INFO (OpCode: 56)
- MAP_RESTORE-DATA (OpCode: 57)
- MAP_SEND-IMSI (OpCode: 58)
- MAP_ANY-TIME-SUBSCRIPTION-INTERROGATION (OpCode: 62)
- MAP_PROVIDE-SUBSCRIBER-INFO (OpCode: 70)
- MAP_ANY-TIME-INTERROGATION (OpCode: 71)
- MAP_PROVIDE-SUBSCRIBER-LOCATION (OpCode: 83)
- MAP_SEND-ROUTING-INFO-FOR-LCS (OpCode: 85)
- MAP_SUBSCRIBER-LOCATION-REPORT (OpCode: 86)

Retrieved private information should be managed as described in section 4.4.3.

#### 4.4.1.2 State-Changing or Charge-Triggering Messages

The tester may have their own SIM belonging to the DNO (or may have permission from the SIM owner to use it for testing purposes) and may want to temporarily change the state of the associated IMSI for testing purposes. Alternatively, the tester may have received test IMSIs/MSISDNs or ranges from the DNO. They are only affecting their own service, or the service of a consenting or test subscriber, and this is permitted subject to the conditions described in section 4.2. For example the following MAP signalling would change the state of the IMSI, and may require subsequent messages to recover the IMSI to a “normal” state:

- MAP_UPDATE-LOCATION (OpCode: 2)
- MAP_CANCEL-LOCATION (OpCode: 3)
- MAP-INSERT-SUBSCRIBER-DATA (OpCode: 7)
- MAP_DELETE-SUBSCRIBER-DATA (OpCode: 8)
- MAP_REGISTER-SS (OpCode: 10)
- MAP_ERASE-SS (OpCode: 11)
- MAP_ACTIVATE-SS (OpCode: 12)
- MAP_DEACTIVATE-SS (OpCode: 13)
- MAP_UPDATE-GPRS-LOCATION (OpCode: 23)
- MAP_PURGE-MS (OpCode: 67)

Messages that cause charging events are permissible only if the tester owns or has owner or DNO consent to charge the associated subscriptions. For instance, the following would be permitted, but should be used with caution to avoid triggering an excessive number of charging events:

- MAP_MT-FORWARD-SHORT-MESSAGE (OpCode: 44)
- MAP_MO-FORWARD-SHORT-MESSAGE (OpCode: 46)
- MAP_PROCESS-UNSTRUCTURED-SS-Request (OpCode:59)

If it is not practically possible for the tester to own or have consent for the SIMs used for testing purposes without unreasonably increasing the cost and effort of testing, (e.g. for large-scale multi-national testing), then the tester should test using DNO-allocated test IMSIs. Random or other specific IMSIs should not be targeted unless explicit permission for this has been given by the DNO and such testing is permitted under applicable data privacy regulation.

#### 4.4.1.3 High-Risk Messages

Messages as described above that are badly formed or represent a DoS attack should not be sent by a legitimate tester. No fuzzing of messages should be permitted – i.e. all messages should conform to specifications.

Messages that potentially impact a large number of subscribers or subscribers where the sender does not hold or have permission to impact an IMSI should not be sent. For example:

- MAP_RESET (OpCode: 37) – if sent with a large number of IMSIs

Messages that cause a billing impact to either the originating or the terminating IMSI are only permitted if all impacted IMSIs are test IMSIs or with permission of the bill payer.

### 4.4.2 Test Frequency / Duration

As far as is reasonably possible, testers should seek to perform testing within the normal business hours of the DNO to ensure availability of appropriate DNO resources to deal with any unexpected disruption. If testing is planned out of core DNO business hours to avoid high-usage hours impact, this should be highlighted in the advance notification message sent by the tester to the DNO.

The start and end time of the tests as well as the maximum rate and number of messages and the duration of testing should not intentionally cause unexpected or service-affecting behaviour within the destination network. These parameters should also adhere to what the tester has notified the DNO in advance.

Continuous testing should not be conducted, even if not doing any apparent harm to the network, unless explicit permission to do this has been granted by the DNO to the tester.

### 4.4.3 Data Protection

The research/testing activities shall not include system intrusion in excess of testing the exposed signalling functions and interfaces, and shall specifically avoid extensive information exfiltration/-leakage in excess of what is required to confirm the vulnerability in question and/or secondary testing towards functions and interfaces which were not directly exposed at the time when the testing was initiated (so-called *post-exploitation activities*)

Testers should not abuse any vulnerabilities discovered by, for example, downloading more data than is necessary to demonstrate the vulnerability, or by changing or deleting data. Testing that yields personal data should only be related to SIM cards that the tester owns or has owner or DNO consent to use for testing. Any testing against random IMSIs (where permitted – see section 4.2) that yields personal data should only be done in compliance with applicable data privacy legislation. The scale of probing of network data should be limited to the minimum needed to confirm a vulnerability.

### 4.4.4 Logging

The tester should keep a log (e.g. via packet capture (PCAP) traces) of the following during testing in order to support test results confirmation and/or sharing with the DNO and investigation of any issues:

- Time and date of message exchange
- Originating GT(s), IP address, Origin Realm, Origin Host used or any other information used to identify the sender
- Detailed messages sent (i.e. including all used parameters)
- Detailed responses received

Detailed log or PCAP traces may disclose proprietary testing methods developed by the tester that constitute intellectual property rights, so there may be instances where the tester is not willing to share these in full, and may choose to provide alternative evidence of test results to the DNO (where this is necessary - see section 4.5.1).

### 4.4.5 Detection of Potential Disruption

Where possible, the tester is encouraged to monitor for potential disruption caused at the DNO by his testing. The tester should monitor the contact channels that they provided to the DNO in case the DNO needs to alert the tester to some disruption. The tester should also monitor for normal service on any test SIMs being used.

If the tester suspects that their activity is causing disruption at the DNO, they should stop testing, contact the DNO to validate this, and offer assistance, including sharing of logs and of any other type of information useful for troubleshooting.

## 4.5 After Testing

### 4.5.1 Test results sharing and coordinated vulnerability disclosure

If new vulnerabilities are found during testing that are specific to a DNO and that were not previously reported to the DNO, the tester is expected to disclose these according to that operator's responsible disclosure policy, if such a policy exists and is available to testers in a reasonably accessible manner. If the DNO does not operate a co-ordinated vulnerability disclosure (CVD) process, the tester should report test results in a secure way to the DNO contact point from where they received a response to the advance notification. (e.g. security@<MNO-name>.com mailbox). The DNO and the tester should agree an appropriately secure method for communicating sensitive information. In the unlikely event that the DNO and tester cannot agree a secure way of reporting the vulnerability, and if the DNO will not accept liability for receiving the information via an insecure method, the tester does not have to disclose sensitive information to the DNO that would allow exploitation of the vulnerability.

If a general vulnerability is found affecting many operators, the tester isn't required to report individually to each operator. Depending on the vulnerability, the tester could report to a specific affected equipment vendor, or via the GSMA CVD process. In addition, if the security research / testing

- has the characteristics of being a condition measurement / benchmarking, and

- notice of the tester's intention to fully and publicly disclose results has been provided to all participating DNOs in the advance notification,

then responsible disclosure via each DNO's CVD process is not required.

Test results must not be used for any purpose other than legitimate security research e.g. not used for abuse.

If no vulnerabilities were found, then the tester should briefly notify the DNO of this outcome. However, the tester is not expected to share test results.

When sharing the test results with the DNO, the tester is encouraged, but not required, to consider the following items/structure:

- Executive summary
- Statement of scope
- General statement of methodology
- Statement of limitations
- Testing narrative
- Test results (including PCAP traces if tester evaluates this doesn't leak his IPR)
- Findings
- Tools used
- Clean-up of the environment after testing

The responsible party should be provided with a reasonable period to respond to a security vulnerability found during testing before public disclosure by the tester. This period should be in accordance with what is specified in the vulnerability disclosure policy of the responsible party. The tester should not share information about discovered vulnerabilities with others during this period.

If the responsible party does not have a CVD process, the tester should allow 60 business days for the responsible party to respond to a security vulnerability found during testing before public disclosure.

If the tester publishes information about found vulnerabilities, he shall remove or anonymize any operator and/or vendor data, such as name, identity prefixes, or other operator and/or vendor specific information.

## 4.6 Corrective Action

The tester is encouraged to reasonably share enough information with the DNO so that the DNO or affected vendor can understand the identified issues and how they could be remediated, especially if publishing results publically that include vulnerabilities.

The tester shall not knowingly withhold from the DNO or affected vendor, information in their possession about the disclosed vulnerability that could reasonably be assumed to be relevant for the DNO's or affected vendor's ability to effect remedial action(s).

# 5 Responsibilities of the Originating Network Operator

The ONO is ultimately responsible to the DNO for ensuring that outgoing signalling from its network and/or assigned network addresses is legitimate, regardless of whether the signalling was initiated by third parties whose security research/testing is facilitated by the DNO. GSMA members should access and refer to GSMA confidential PRD BA.20 [1] for details of ONO liability in scenarios where the DNO or its customers are subject to malicious attack as a result of signalling originating from the equipment or network address of the ONO. The liability terms in BA.20 apply regardless of whether malicious signalling was initiated by the ONO or a separate tester. In order to facilitate and encourage legitimate testing, which is of benefit to the industry, interconnect security testing conducted in accordance with the recommendations in this document is not considered to be malicious and is not subject to the liability terms specified in BA.20. The ONO is responsible for providing evidence that the messages originating from its network were part of testing activity in accordance with the recommendations in this document.

To manage this responsibility, an ONO should ensure that it is aware of the nature of testing being performed by any testers using its network e.g. by requiring testers to send advance notification of test plans to the ONO. The ONO may also wish to manage outbound messages from its network (e.g. use an outbound firewall to detect unwanted messaging issued from their GTs that have been leased to a third party).

An ONO should also provide support to a DNO in response to any DNO requests about signalling that has come from the ONO's network.

# 6 Responsibilities of the Destination Network Operator

All mobile network operators should have a publicly advertised contact point for testers to notify them of proposed interconnect security testing.

The DNO should have a process for dealing with interconnect security testing requests and a clear internal decision making authority and process. The DNO should also have a policy that determines what other stakeholders the DNO should share the testing notification with (e.g. signalling providers, MVNOs, signalling firewall solution providers)

The DNO should maintain a record of testing notifications received, and the contact details for the tester and the ONO. The DNO should maintain a record of any test IMSI/MSISDN ranges provided to testers, including the period within which they may be used.

The DNO is recommended to closely monitor its logs during periods of independent remote testing and promptly advise the tester of any service-affecting network issues observed during testing.

The DNO's network should respond to test signalling the same as it would as for real attacks. However, detailed investigation of traffic shouldn't be necessary for test signalling. The DNO should be able to distinguish between test signalling and real attacks by checking the origin and destination network addresses used in test messages (as shared by the tester as part of advance notification). If known, the DNO may also distinguish between test signalling and real attacks via the test IMSIs/MSISDNs used.

The DNO is recommended to implement a vulnerability disclosure process to facilitate reporting of results by testers. Information on deploying a coordinated vulnerability disclosure process can be found in [2], [3], [4], [5] and [6].

The DNO should respond to testers in accordance with the terms of their CVD process (or within 60 business days if no CVD process is in place) if a vulnerability is reported to it.

If the DNO wishes to impose conditions on independent remote testing, it should acknowledge that by definition, such testing can no longer be considered as independent. In such a scenario the DNO should engage with the tester and discuss whether and how testing should continue under bilateral agreement.

# Annex A Document Management

## A.1. Document History

| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
|---|---|---|---|---|
| 1.0 | 3 Nov 2017 | First published version | TG | David Maxwell, GSMA |

## A.2. Other Information

| Type | Description |
|---|---|
| Document Owner | Fraud and Security Group |
| Editor / Company | David Maxwell, GSMA |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.