Global Title Leasing Code of Conduct
Version 1.0
29 March 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document has been produced in response to concern in the public and private domain regarding the leasing of SCCP Global Titles, or “GTs”, to both members and non-members of the GSMA. This document addresses the various uses of leased GTs, with a particular focus on unauthorised use cases. Unauthorised use typically exploits known vulnerabilities that are documented in GSMA PRD FS.11 [5] and elsewhere and could potentially form an attack in extreme cases.

Whilst this document focuses on GT leasing, which by its very nature relates to SS7 traffic, the same risks could apply to other network addressing resources used in other protocols. However, although this document addresses the general principle of leasing network addressing resources, it is currently only applicable to SS7. The principles of this document can apply equally to other protocols (e.g. Diameter, GTP-C and HTTP2/5G). Specifically, leasing of network addressing resources used by these protocols, especially in the absence of transparency, should be avoided and other options to meeting legitimate business needs should be explored first. This document may be further developed in the future to add specific requirements for such protocols.

Section 5, "Global Title Leasing Code of Conduct”, has been produced as a code of conduct (CoC) to which GT Lessors and Transit Carriers may self-declare compliance. The roles of these participants are described in section 2.2. It is envisaged that all GT Lessors and Transit Carriers that support the proper policing of GT Leasing will self-declare their adherence to the CoC. Whilst this document is non-binding, any party that voluntarily commits itself to the CoC is understood to treat those requirements as binding upon itself.

1.2 Scope

This document is a reference document addressing the leasing of Global Titles used within SS7 networks, motivations for this practice, how they are used and a code of conduct to prevent abuse and the introduction of undesirable risks for mobile network operators (MNOs) and their customers. The focus of this document is on addressing the security and privacy risks associated with this practice with the goal of delivering transparency, traceability and accountability.

The following activities are considered as out of scope:

1. Hosted services, such as those offered by third parties or centrally within a MNO group. In this case it is reasonable for the host to use the GT of its customer, this **is not** considered GT leasing. If the client’s GT is used for any other purpose than hosted services, then that other activity is GT leasing and must comply with the requirements of this CoC.

2. Use of GTs by roaming enabling services as defined in PRDs BA.21 [8] and BA.23 [9].

3. Details regarding the vulnerabilities of mobile networks and how these vulnerabilities can be exploited are outside the scope of this document.

Additionally, consequences for those parties that lease GTs that have enabled unauthorised usage are outside of the scope of this document. Such activity is subject to the terms of the commercial relationship between the relevant parties.

1.3 Definitions

Term	Description
Global Title	A global title (GT) is an address used in the SCCP protocol for routing signalling messages on telecommunications networks

1.4 Abbreviations

Term	Description
API	Application Programming Interface
CdPA	Called Party Address
CgPA	Calling Party Address
CoC	Code of Conduct
DoS	Denial of Service
GT	Global Title
GTT	Global Title Translation
LoA	Letter of Authority
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
(S)PC	(Signalling) Point Code
RAEX	Roaming Agreement Exchange
SCCP	Signalling Connection Control Part
SS7	Signalling System No. 7
NRA	National Regulatory Authority
PRD	Permanent Reference Document

1.5 References

Ref	Doc Number	Title
[1]	ITU-T E.164	Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan.*
[2]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[3]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[4]	GSMA PRD BA.20	Fraud Prevention Procedures
[5]	GSMA PRD FS.11	SS7 Interconnect Security Monitoring and Firewall Guidelines
[6]	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures

Ref	Doc Number	Title
[7]	GSMA PRD IR.77	InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers
[8]	GSMA PRD BA.21	Network Extension Principles
[9]	GSMA PRD BA.23	Outbound Roaming Solutions Handbook

1.6 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [2] and clarified by RFC8174 [3], when, and only when, they appear in all capitals, as shown here.

2 Global Title Leasing

2.1 Introduction to Global Titles

In accordance with the recommendations of the International Telecommunications Union [1], national numbering plan administrators are responsible for administering their national telecommunications numbering plans. As such, number ranges are assigned around the world in accordance with local regulation (note that there are nuances for global services and shared country codes that are beyond the scope of this document). In some markets a strict approach to compliance with the ITU recommendations applies whilst in others there is a lighter touch regulatory regime that may exist with less oversight. In all cases, number resources are assigned to number range holders and never “given” to them. This is an important distinction.

The difference in approach to number range assignment means that in some cases only a licensed MNO may receive mobile numbering resources, whereas in other cases companies that do not offer any type of mobile network service may receive numbering resources. An example of this could be SMS aggregators that transit SMS traffic but do not operate mobile networks.

It is important to re-iterate that numbering resources are owned by a nation state and are merely assigned to the number range holder. Assignments can be withdrawn at any time, in accordance with local regulations.

2.2 GT Leasing Parties

There are different stakeholders relevant to GT leasing, which are defined below:

- **GT Assignee** – this is the party that asserts “ownership” of a GT – this is a self-declaration that the party has been assigned the number range by the appropriate national regulatory authority and has elected to use all or part of that range for Global Title addresses. Note, typically, there is no verification of the veracity of this information.
- **GT Lessor** – this is a GT Assignee that has decided to lease one or more of its GTs to a third party, the GT Lessee, through a bilateral agreement..

- **GT Lessee** – third party who will use a leased global title from a GT Lessor
- **GT Sub-Lessee** – this is an additional third party who has entered into an agreement with the GT Lessee to sub-lease a GT from it.
- **Transit Carrier** – this is an international carrier or IPX that carries signalling traffic. In the case of Diameter and GTP traffic, there should be a maximum of two consecutive Transit Carriers. In the case of SS7 traffic, there can by multiple consecutive Transit Carriers. The Transit Carriers are responsible for delivering traffic to the Target Operator. It is possible for a Transit Carrier to additionally be a GT Lessor, separate from its role as a Transit Carrier.
- **Target Operator** – this is the MNO to which the signalling traffic is destined. This may be the home network of the subscriber or a visited network in the case of roaming. The Target Operator may or may not have a roaming agreement with the GT Lessor, but with the exception of a specific commercial agreement, doesn't have a roaming agreement with the GT Lessee (or Sub-Lessee).

2.3 Benefits of GT Leasing

The leasing of GTs to third parties can be beneficial for a range of purposes and stakeholders. Whilst the use of GT leasing might be helpful, there is no requirement for it to support any particular service. The following claimed benefits, from the perspective of the GT Assignee, Lessor or Lessee, are provided as examples for educational purposes and the list is not exhaustive.

Benefits for the GT Assignee:

- Opportunity to access a new revenue stream by becoming a GT Lessor.

Benefits for the GT Lessor:

- Potential additional revenue

Benefits for the GT Lessee:

- Can gain access to the SS7 signalling network for e.g.:
    - "Thick" MVNOs that have their own core network that require such resources but may not be able to obtain them due to local regulations or they may be required to use such GTs due to local regulation; or
    - Third parties providing innovative value added services; or
    - Security companies conducting penetration testing

2.4 Issues and Concerns with GT Leasing

GT leasing has evolved through the emergence of commercial relationships that were built up over time without any industry standardisation, specifications, or recommendations. As a result, there is no agreed framework governing the relationships between GT Lessors and the networks to which they are interconnected. Not all the parties engaged in GT leasing have given consideration to the impact of GT leasing upon either the networks to which

traffic generated by GT leasing is destined nor to the subscribers of those networks. There are various issues and concerns that have either never been addressed or have been addressed in a piecemeal manner. A summary of some of the key issues follows, most of which are related to the lack of transparency of the true originator and recipient of traffic from/to leased GTs. This section has been provided for educational purposes.

- GT leasing hides the true source and identity of the party sending the signalling traffic.
- There is no ability for the Target Operator to independently perform due diligence on the true originator of traffic i.e. the GT Lessee. Cooperation of either the Transit Carrier or GT Lessor is required.
- There is no requirement or accountability for the GT Lessor to specify in their IR.21 document which GTs or GT ranges are being leased. The concern relates to the anonymity of the lessee of the GTs or GT ranges and the challenges this can present in fault finding and intelligence sharing.
- There is no known or explicit limitation to the GT Lessee or Sub-Lessee on their ability to continue to further sub-lease the GT to other third parties.
- The Target Operator has not given consent to be interconnected to the GT Lessee or GT Sub-Lessee.
- The Target Operator may not be aware that the signalling connection established for an intended use case may also be used for other purposes without consent.
- Commercial value may be assigned to information obtained via leased GTs for which the Target Operator is not compensated – despite them providing network resources to support these services.
- Distribution of malicious traffic across multiple coordinated leased GTs (from multiple GT Lessors) adds complexity in identifying the true originator/source of the malicious traffic.
- Fault investigation is complex. There is no verification as to the type and validity of the SS7 node using the leased GT, increasing operational complexity and increased security vulnerability for the Target Operator.
- Additional costs to the Target Operator (e.g. SS7 transit charges).
- Disruption to legitimate services. The operation of third party services by a GT Lessee or GT Sub-Lessee can impact on legitimate services offered by the Target Operator. In extreme cases, this can lead to denial of service (DoS) of the target user’s device.
- Third party services enabled via GT leasing and offered by a GT Lessee or GT Sub-Lessee cannot be guaranteed and may be disrupted if a Target Operator implements measures to block what it considers to be unauthorised use. In such cases, the third-party service provider may be open to accusations of mis-selling.

- The Target Operator (and potentially others in the signal path) may be in breach of data protection or privacy legislation through the leakage of personal identifiable information.

- Correct identification of the GT Lessor may be challenging where the Target Operator has incorrectly configured IR.21 data. Specifically, even though the GT Lessor may have provided transparent GT Lessee data in the GT Lessor's IR.21, the Target Operator may have failed to properly invoke that data. Incorrect, incomplete or imprecise IR.21 data provided by the GT Lessor may also give an impression that no GT leasing is taking place even though this may be untrue.

- The use of leased GTs for malicious or unauthorised purposes can lead to reputational damage for the GT Lessor and its country's national numbering resources.

2.5 Potential impacts of GT Leasing and GT Sub-Leasing to the GT Lessor

The very foundation of GT leasing is a bilateral agreement where the GT Lessee benefits from the GT Lessor's resources . However, it is important to appreciate that those resources (e.g. roaming partner relationships, signalling connectivity etc.) may have been accumulated over several decades of effort and investment by the GT Lessor. One reason the GT Lessor accumulated those resources was to enhance its domestic coverage, subscriber base and roaming business value. None of these are easy to accumulate and are the result of significant expenditure and investment.

When a GT Lessor leases a GT to a third party, it is placing its reputation and brand into the hands of that third party and indeed into the hands of any additional parties to which the third party may sub-lease the GT. In this case the GT Lessor would probably have limited or no commercial or technical visibility of this arrangement. If that trust is breached then the consequences may be severe. It is important that any GT Assignee considering GT Leasing is aware of the pitfalls of this business model. The additional revenues that this business may yield could be very small compared to the impact of any potential reputational damage.

3 Global Title Leasing Use Cases

GSMA strongly advises that GT leasing should not be used. The following is a list of use cases, historically deployed using GT leasing. In each case solutions could have been deployed without the use of GT leasing.

- SMS aggregators aggregate traffic from multiple sources, typically enterprises but potentially also mobile operators, and route that traffic for delivery to the recipients of those messages.

- Penetration Testing: Security companies that engage in external penetration testing require access to Global Titles to execute their tests.

- Location tracking for fraud prevention e.g., banks may require the location of customers that have consented to share this information.

- Information about customer account status to prevent fraud e.g., “Know your customer”. This may be through confirmation of call divert status or whether a recent SIM swap has taken place.
- “Thick” MVNOs and sponsored roaming providers that have their own core networks may require GTs from their host networks for their own core network nodes.
- Mergers and acquisitions e.g. where a GT Assignee or GT Lessor has sold part of its business but continues to offer network access services to the new entity.
- Non-standardised interworking from non-3GPP networks (CDMA, WiMAX, Wi-Fi) to 3GPP networks.

Note that this list of Global Title leasing uses cases is provided for example purposes only and does not constitute an exhaustive list of approved Global Title leasing use cases.

Due to potential misuse of SS7, and the obligations and liabilities imposed on GT Assignees under BA.20, the GSMA strongly advises that other options / architectures should be considered as an alternative to using GT leasing. For example, where an application programming interface (API) is used to fulfil the aforementioned use cases, it should be restricted to the specific use case only, comply with data protection requirements and must be delivered with the specific consent of the Target Operator and their subscribers, where applicable.

4 GT Leasing Traffic Routing Options

There are two potential scenarios with respect to how signalling traffic is routed to the GT Lessee.

- **Routing via Lessor** - in this case signalling traffic is routed to the GT Lessee via the GT Lessor’s network; and
- **Routing via Lessee Only** – in this case signalling traffic is routed without passing through the GT Lessor’s network. This means that traffic to or from the GT Lessee is routed directly to/from them via the Transit Carrier.

4.1 Routing via Lessor

In this scenario, the Transit Carrier has visibility of the traffic received from the GT Lessor’s network. This offers significant legal, commercial and technical advantages to the GT Lessor. By ensuring that all signalling traffic passes through the GT Lessor’s network it has full visibility of the traffic and can implement appropriate technical controls. Additionally, the GT Lessor can monitor the traffic to ensure compliance with the relevant contractual, regulatory and legal obligations. However, for the GT Lessee, these advantages are the inverse - traffic routing and management becomes more complex, especially where The GT Lessee is aggregating traffic from multiple different GT Lessors.

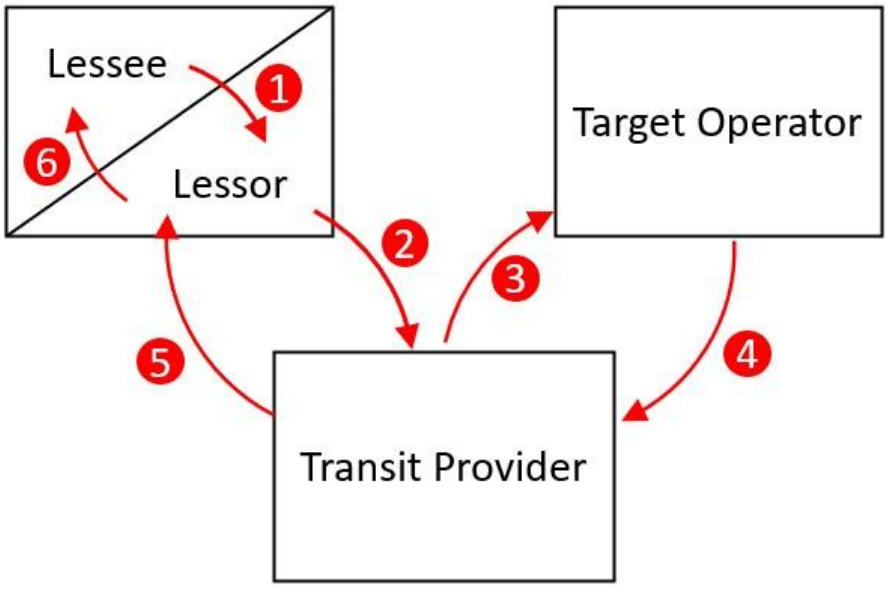

Figure 1 – Routing via Lessor

Figure 1 above illustrates the high-level signalling flow as follows:

- Point 1 - traffic originates from the GT Sub-Lessee/GT Lessee. For simplicity, the Sub-Lessee has not been included in the diagram.
- Point 2 - traffic is sent using the GT Lessor network.
- Point 3 - the Target Operator receives the traffic. Here the Target Operator may be the subscriber's home network or roaming partner in case the subscriber is roaming.
- Point 4 - the Target Operator responds to the message
- Point 5 - the Transit Carrier delivers the response back to the GT Sub-lessee/Lessee via the GT Lessor Network.

A more complete diagram is included in Annex A illustrating the signalling flow together with illustrative calling and called addresses and point codes.

4.2 Routing via Lessee Only

In this scenario, the Transit Carrier will have visibility of the traffic originating from the GT Lessee's network, albeit the calling GT indicates to all subsequent recipients of the traffic that the traffic originated from the GT Lessor network even though this is not the case.

This approach offers the GT Lessee significant advantages, as it can avoid any kind of scrutiny by the GT Lessor of the traffic it is sending and receiving, and it has the benefit of more direct access to the signalling traffic. This allows the GT Lessee the flexibility to select its own Transit Carriers and set its own commercial rates, which could disadvantage the GT Lessor. Typically, the Transit Carrier (and other Transit Carriers in the signalling path) will require the GT Lessee to provide a "Letter of Authority" from the GT Lessor confirming that the GT Lessee has authorisation to use the GT and therefore to receive the traffic directly.

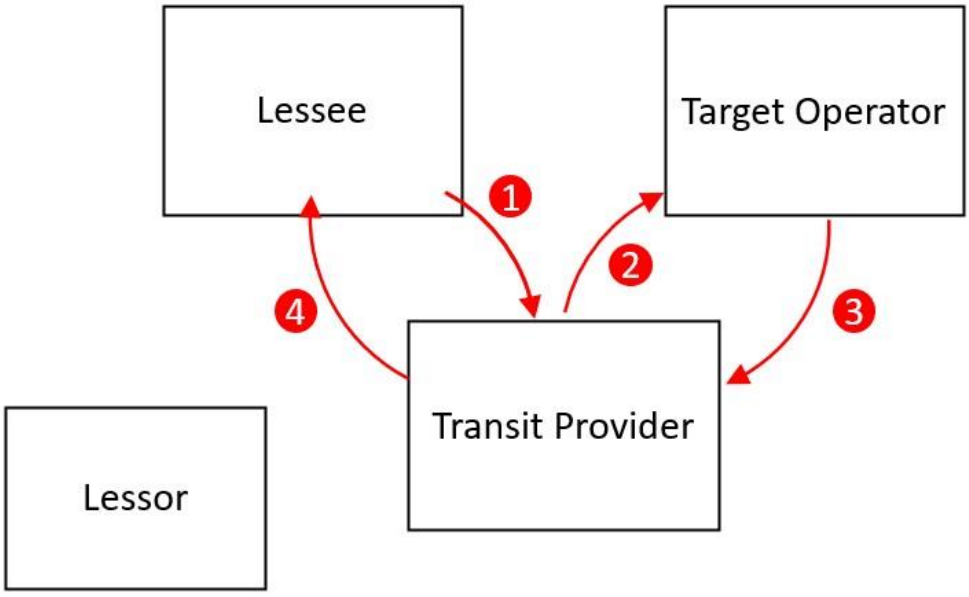

Figure 2 – Routing via Lessee Only

Figure 2 above illustrates the high-level signalling flow as follows:

- Point 1 - traffic originates from the GT Sub-Lessee/ Lessee
- Point 2 - Target Operator receives the traffic
- Point 3 - Target Operator responds to the message
- Point 4 - Transit Carrier routes the response back to the GT Lessee.

A more complete diagram is included in Annex A illustrating the signalling flow together with illustrative calling and called addresses and point codes.

Note that in this scenario the GT Lessor plays a significantly diminished role and has no visibility of traffic originating from or terminating to the GT Lessee's network. As the GT Lessor is responsible and liable for all Global Titles assigned to them, and is responsible for ensuring the security of Global Title use to protect both the GT Lessor and the Target Operators, Routing via Lessee Only should be discontinued because of the security and privacy risks the practice poses for mobile users.

5 Global Title Leasing Code of Conduct

This optional CoC is aimed at all GT Lessors and/or Transit Carriers. While it may appear desirable also for GT Lessees to directly addressed by this CoC, they are typically not GSMA members. As only GT Lessors and Transit Carriers may formally declare compliance with this CoC to the GSMA, GT Lessees are covered only indirectly, through requirements directed towards the above stakeholder types.

All mandatory requirements are included in this section 5 only. GT Lessors, by their very nature, provide the critical numbering resources to access the SS7 networks whilst Transit Carriers typically enable the connectivity. As such, it is critical that these ecosystem

participants adhere to this CoC and all such players are strongly encouraged to fully adopt the recommendations set out below.

Any party wishing to comply with this CoC should be aware that partial compliance with the requirements (i.e. statements using “SHALL”, “MUST” and/or “MUST NOT”, but not statements using “SHOULD” and/or “MAY”) is non-compliance and none of the requirements can be varied for any individual party.

Whilst GT Assignees and Target Operators are not directly involved in the act of GT Leasing and are not eligible to formally declare compliance with the CoC to the GSMA, they are nonetheless encouraged to otherwise declare their support for this CoC to further encourage the adoption of best practice across the ecosystem.

5.1 GT Lessors

GT Lessors are required to adhere to the following requirements to comply with this CoC. A GT Lessor is, by definition, a GT Assignee that has decided to monetise its GT resources. The decision to monetise resources has consequences and this CoC imposes appropriate requirements on all GT Lessors.

Once a decision has been taken to become a GT Lessor, the GT Lessor should be aware that it is legally liable for any harm caused to the Target Operator, irrespective of whether it or the GT Lessee generated malicious traffic that may result in harm. PRD BA.20 [4] is unambiguous on this matter. GT leasing is not a preferred method of gaining access to a roaming operator’s network. Although previously tolerated to support some use cases, it can obfuscate the true source of signalling making fault finding and network and user protection more difficult and is discouraged.

1. GT Lessors MUST take responsibility for their Global Titles and the consequences (predictable or otherwise) of their decisions in relation to GT Leasing. They SHALL acknowledge that they are always responsible for the signalling generated by their GT Lessees and SHALL have appropriate measures in place to ensure compliance.

2. GT Lessors MUST ensure that they are familiar with the details of BA.20 [4] related to the liability resulting from GT Leasing.

3. GT Lessors SHALL commit to conduct due diligence on any potential GT Lessees before providing them with access to any GTs. This SHOULD include both a review of the company and the declared use cases that they plan to support using the leased GTs. Additionally, upon adopting this CoC, GT Lessors SHALL conduct a retrospective and periodic due diligence of all existing GT Lessees.

4. GT Lessor SHALL require the GT Lessee to use a Transit Carrier that has signed up to this Code of Conduct.

5. GT Lessors, who are Full Members of the GSMA, MUST provide clear and current information within their IR.21 using the appropriate RAEX format, or free text fields prior to RAEX being updated, to clearly declare which of their GTs are subject to GT Leasing. This information MUST be provided with complete transparency and be available to all GSMA members.

6. The GT Lessor's IR.21 MUST detail the business name of the GT Lessee and the type of signalling node that is using the leased GT.

7. GT Lessors MUST implement real-time technical controls on the use of leased GTs to ensure they are compliant with the recommendations of FS.11 and to ensure their use is limited to the specific declared use cases defined in the agreement(s) between GT Lessor, GT Lessee and roaming partner. For the avoidance of doubt, contractual controls only are not considered adequate and outsourcing real time technical controls, such as an outbound firewall, is not recommended due to the sensitive nature of traffic and the risks involved.

8. GT Lessors SHALL cease allowing the Routing via Lessee Only method with effect from 31st December 2023.

9. GT Lessors MUST NOT implement any new Routing via Lessee Only arrangements from the date on which compliance with this Code of Conduct is declared.

10. Where traffic is routed using the Routing via Lessee only method, only to support legacy arrangements during the transition period to 31st December 2023, the GT Lessors MUST arrange to receive either a passive feed of all traffic routed to or from the GT Lessees, or access to a near real-time service enabling the GT Lessors to query all traffic routed to or from the GT Lessees. This MUST be implemented for all relevant traffic only at the time of adopting this CoC.

11. GT Lessors MUST disclose full details of their GT Lessees upon request of Target Operators where evidence is supplied to confirm that traffic received by the Target Operators using GT Lessor's leased GTs was in breach of the relevant PRDs. This will assist the investigations of the Target Operators (where multiple GTs may have been used), and will facilitate threat intelligence sharing.

12. GT Lessors MUST NOT object to being named in threat intelligence sharing reports as a party that originated traffic that was in breach of the relevant PRDs. This does not negate the right to reply to such reports.

13. GT Lessors MUST consent to the Transit Carrier providing signalling traces related to traffic originating from their GTs to the Target Operators upon request.

14. GT Lessors MUST retain summary signalling data (i.e. aggregated data which includes Originating Point Codes, Calling and Called GTs, MTP3 information, SCCP information and MAP information) for GTs leased to GT Lessees for 4 months minimum.

15. GT Lessors MUST store full signalling trace data for at least 10 calendar days.

16. Threat intelligence sharing is considered "best practice" and as such GT Lessors SHOULD support and participate in threat intelligence sharing.

17. As a principle, sub-leasing of GTs is not recommended and SHOULD be avoided. However, there are circumstances e.g. business restructuring where such a relationship is created. Where GT sub-leasing takes place, the following clauses MUST be adhered to:

a) GT Lessors MUST contractually oblige any GT Lessees to declare any instances where the GT Lessees have allocated addresses to GT Sub-Lessees. In such scenarios, the GT Lessors MUST engage the GT Sub-Lessees in the same manner as GT Lessees per 5.1, (notably clauses 3,4,5 and 6).
b) GT Lessors MUST NOT allow GT Sub-Lessees to further sublet addresses to other parties.

18. Where GT Lessees or GT Sub-Lessees are identified by the GT Lessors as falsifying information in a declaration of use case, or in declarations of Sub-leasing, the GT Lessors MUST terminate the GT Lessees or Sub-Lessees traffic with immediate effect, and SHOULD inform other carriers through threat intelligence sharing.

19. GT Lessors that declare compliance with this CoC MUST comply in good faith with the CoC Complaints process.

5.2 Transit Carriers

Transit Carriers are required to adhere to the following requirements to comply with this CoC. Any Transit Carrier that signs up to this CoC SHALL adhere to the relevant PRDs. Traffic is typically cascaded through a chain of Transit Carriers and the rules in this CoC apply equally to all of those Transit Carriers that also declare compliance with the CoC.

It is acknowledged that satisfying these requirements will require effort and investment by Transit Carriers. This could lead to additional commercial charges from Transit Carriers to their customers.

1. Transit Carriers SHALL cease enabling the Routing via Lessee Only method with effect from 31st December 2023. The Routing via Lessee Only method is prohibited after that date.

2. Transit Carriers MUST NOT implement any new Routing via Lessee Only arrangements from the date on which compliance with this Code of Conduct is declared.

3. Transit Carriers MUST ensure that they comply with the binding requirements of PRD IR.77.

4. Upon request from a Target Operator, Transit Carriers MUST provide details of whether traffic received by the Target Operator using leased GTs was subject to Routing via Lessor or Routing via Lessee Only.

5. Where Transit Carriers are routing traffic directly to GT Lessees to enable the Routing via Lessee Only method, prior to its prohibition on 31st December 2023, they MUST send either a passive feed (i.e. a real-time copy of the live traffic) of all traffic routed on behalf of the GT Lessees to the GT Lessors or provide access to a near real time service enabling the GT Lessors to query all traffic routed to or from the GT Lessees. This ensures that the GT Lessors have full visibility of all traffic destined to the GT Lessees. This MUST be implemented for all relevant traffic at the time of adopting this CoC.

6. Transit Carriers MUST support Target Operators by providing details of traffic that transited their network that is the subject of Target Operator investigation. This applies whether the Transit Carrier has a commercial relationship with the Target Operator or not, within the constraints permitted by data privacy regulations.

7. Upon request from a Target Operator, including a copy of a relevant signalling trace for traffic that transited towards or terminated in the Target Operator's network, a Transit Carrier MUST provide an unmodified signalling trace for ingress traffic using leased GTs transiting its network towards the Target Operator.

8. Transit Carriers MUST retain summary signalling data (i.e. aggregated data which includes Originating Point Codes, Calling and Called GTs, MTP3 information, SCCP information and MAP information) for leased GTs for 1 month minimum.

9. Transit Carriers MUST store full signalling trace data for at least 7 calendar days.

10. Transit Carriers MUST identify the source of the traffic that was delivered to the Target Operators. In the case that multiple Transit Carriers are involved in the delivery of this traffic, Transit Carriers that have declared compliance with this CoC SHALL identify the party from whom they received the traffic.

11. Where Target Operators are unable to block traffic from GT Lessees, the Transit Carriers SHOULD block that traffic to those Target Operators upon request from the Target Operators.

12. Transit Carriers that lease GTs MUST comply with all the requirements of section 5.1.

13. Threat intelligence sharing is considered "best practice" and as such Transit Carriers SHOULD support and participate in threat intelligence sharing.

14. Transit Carriers MUST NOT object to being named in threat intelligence sharing reports as a party that transited traffic that was in breach of the relevant PRDs. This does not negate the right to reply to such reports.

15. Transit Carriers MAY block any traffic deemed fraudulent as a proactive measure without prior request from Target Operators. Transit Carriers SHOULD inform Target Operators and GT Lessors that such blocks have been implemented.

16. Transit Carriers that declare compliance with this CoC MUST comply in good faith with the CoC Complaints process.

6 Best Practice Recommendations

The following recommendations are included as best practice for GT Assignees and Target Operators and do not form part of the CoC.

6.1 GT Assignees

GT Assignees are advised to proceed with caution when considering the matter of GT leasing. All other options/architectures (e.g. use of APIs) should be explored first before using GT leasing. Where there are legitimate uses of GT leasing, any arrangement enabling

such services should ensure both contractual and technological means to enforce such legitimate usage and to block any unauthorised usage (as outlined in 5.1).

GT Assignees should commit to reviewing the requirements placed upon GT Lessors in this code of conduct and should agree to comply with all of them should they become GT Lessors.

6.2 Target Operators

1. Target Operators should consider implementing the recommendations outlined in FS.11 where applicable.

2. Target Operators that are recipients of signalling that is in breach of the relevant GSMA PRDs should share threat intelligence since threat intelligence sharing is considered “best practice”. This is detailed in section 7 below.

3. Target Operators should identify the networks from where attacks originated, and should attempt to attribute attacks to their true source. This is critical for any investigation into any breach and is also important for correlation of distributed attacks (as well as for threat intelligence sharing).

4. Target Operators should review and, where appropriate, update their commercial contracts with GT Lessors and Transit Carriers to ensure all parties are compliant with this CoC.

5. Target Operators should not accept signalling traffic originating from any party with whom they do not have an agreement to terminate such traffic. They SHOULD consider blocking calling party GTs that are not assigned to a GSMA operator member with which they have a roaming or interworking contract or otherwise a bilateral agreement. This is considered best practice.

6. Target Operators should not accept signalling messages from GTs assigned to non-members of the GSMA. Where they do so, they do so at their own risk.

7 Threat Intelligence sharing

To increase awareness of the problems associated with GT Leasing, MNOs should consider using services that share threat intelligence. Various commercial solutions are available as well as the GSMA’s T-ISAC MISP instance (misp.gsma.com). This applies equally to Target Operators, as well as GT Lessors, and also applies to other parties such as signalling firewall or other signalling security providers, where they have the appropriate authorisation from their customers (typically a Target Operator).

Annex A Detailed Signalling Flow Diagrams

A.1 Routing via Lessor

Figure 3 illustrates the complete signalling flow for Routing via Lessor, complete with illustrative calling and called party addresses as well as point codes and Global Title Translation (GTT).

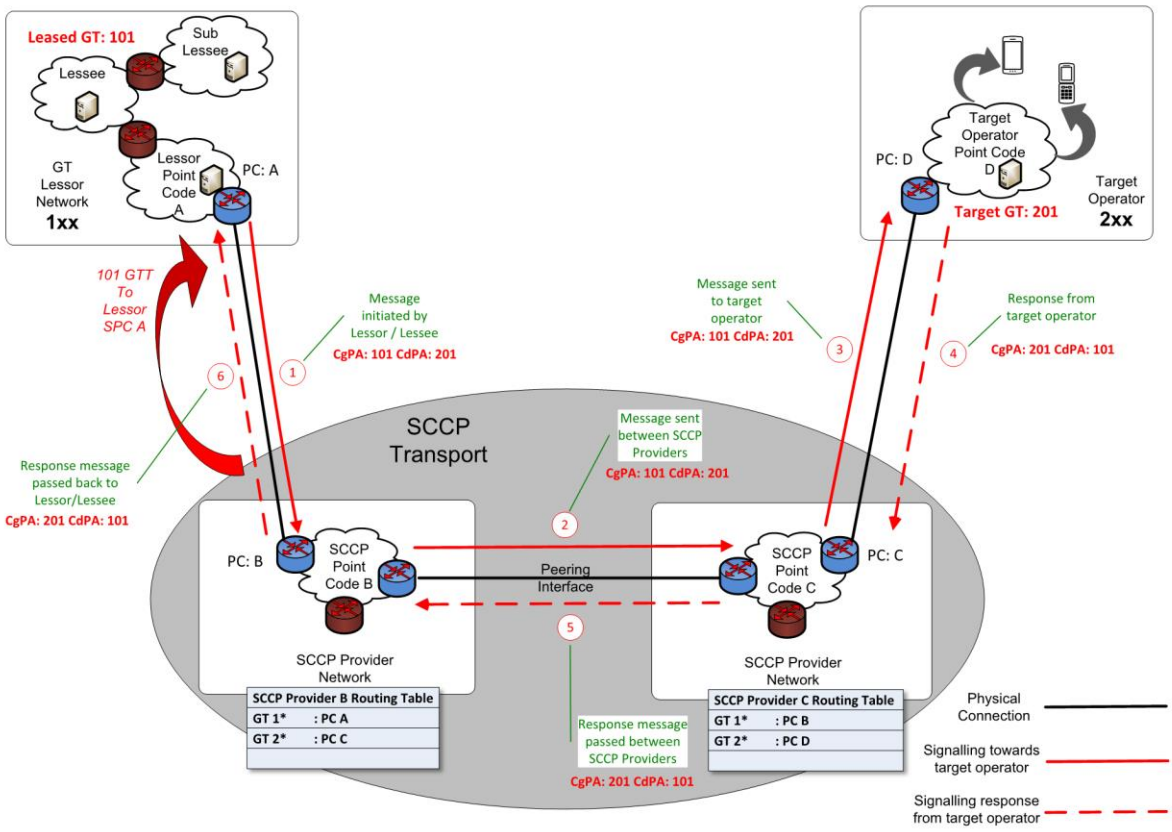

Figure 3 – Routing via Lessor Signalling Flow

A.2 Routing to Lessee Only

Figure 4 illustrates the complete signalling flow for Routing via Lessee Only, complete with illustrative calling and called party addresses as well as point codes and Global Title Translation (GTT).

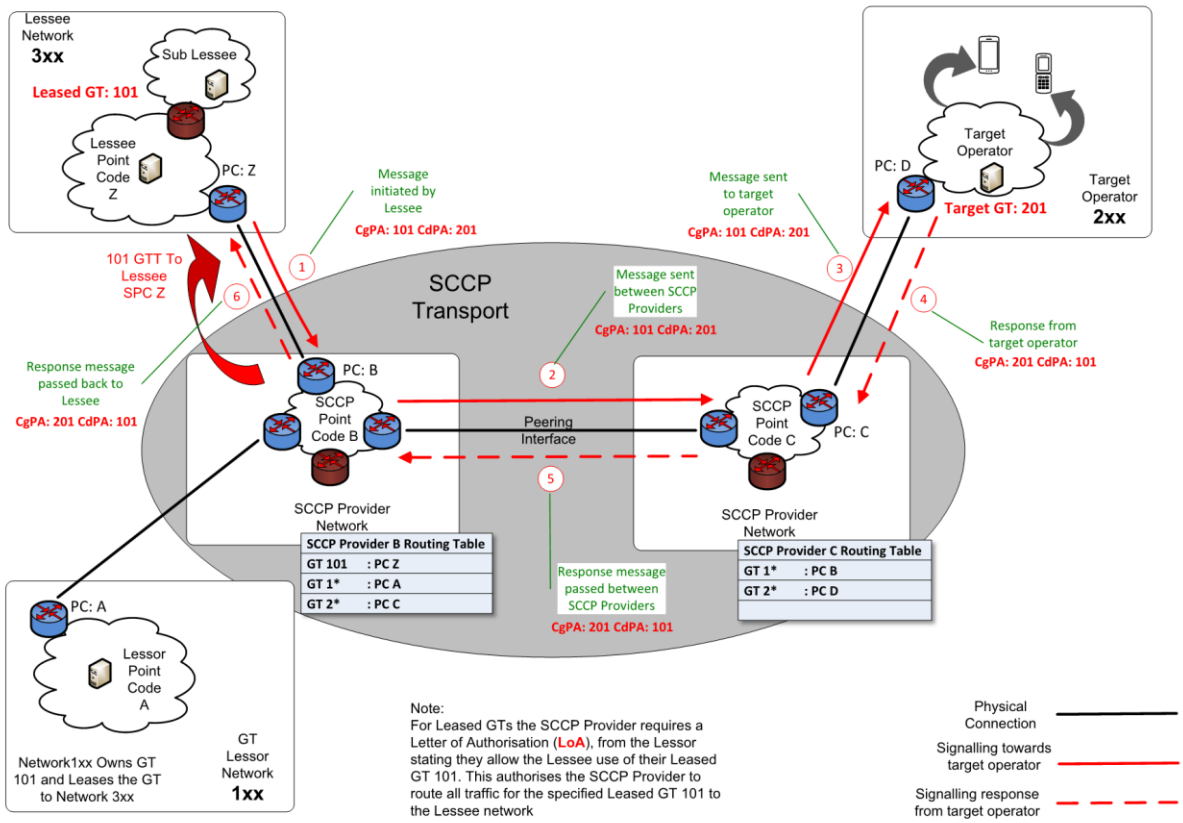

Figure 4 – Routing via Lessee Only Signalling Flow

Annex B Appropriate IR.21 Management

It is important that MNOs fully break out number ranges down to the individual ranges assigned to all individual operators. An example of this is contained in Table 1 below:

Range	GT
100	Operator A
101	Operator A
102	Operator A
103	Operator A
104	Operator B
105	Operator A
106	Operator A
107	Operator A
108	Operator A
109	Operator A
110	Operator A

Table 1 – Example of Number Range Break-Out

In Table 1 GT 104 is assigned to Operator B, whereas all other GTs beginning with 10 belong to Operator A. It is therefore important that MNOs configure each GT separately to ensure that Operator B is correctly identified. If MNOs assume that all GTs commencing with 10 belong to Operator A, then any traffic originating from Operator B will not be correctly attributed.

When configuring their systems, it is important for MNOs to breakout IR.21 defined GT ranges to a level of detail necessary to unambiguously identify the appropriate operator and exclude ranges that are not within the IR.21 data. There should not be a scenario where a GT range is allocated to multiple operators.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	28 Mar 2023	First version.	ISAG	Stephen Ornadel, Mobileum.

C.2 Other Information

Type	Description
Document Owner	FASG
Editor / Company	Stephen Ornadel, Mobileum

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.