Independent Communications Authority of South Africa

350 Witch-Hazel Avenue, Eco Point
Office Park Eco Park, Centurion.
Private Bag X10, Highveld Park 0169

ANNEXURE C – INTERNATIONAL VOICE GATEWAY

1. Purpose of ANNEXURE C

The purpose of Annexure C is to highlight the technical and functional requirements and specifications for the International Voice Gateway that the Independent Communications Authority of South Africa (hereinafter referred to as "the Authority") is seeking to acquire as per the terms and conditions outlined herein.

Considering the adverse impact of the covid19 pandemic on the economy, the National Treasury has requested the Authority – amongst other economic regulators – to explore additional opportunities to generate additional income for the fiscus. As part of its exploration, certain conduct – colloquially classified as interconnect bypass activities – has been highlighted. The effect of this conduct is to bypass, refile and or mask 'internationally originating traffic' destined for termination on South African networks 'as local traffic' with the consequence that:

(a) it results in significantly reduced revenue being recovered by the fiscus[1], and

(b) it undermines infrastructure investments as it diverts revenue from legitimate licensees.

The interconnect bypass activities are in breach of the Call Termination Regulations, 2018. Though the extent of the prevalence of these conduct / activities is not fully

[1] Instead of SARS recovering tax revenue on the basis of an international termination rate of USD0.15 per minute, it is recovering revenue on revenue at the domestic rate of less than USD0.01 per minute, given that where interconnect bypass activities have occurred the originating number reflected is a domestic number, and domestic rates are accordingly charged for the call

quantified, preliminary data demonstrates that it is not insignificant[2]. This is particularly the case given that in addition to undermining revenue collection efforts, the practice has other undesirable consequences such as unlawful manipulation of caller line identification in breach of the Electronic Communications Act, 2005 and the Numbering Plan Regulations, 2016. Furthermore, it has the potential to undermine national security by negating permissible intercept measures which are required to be implemented in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.

2. Background

2.1.1. An international Voice Gateway is the exclusive Gateway for all incoming and outgoing international voice traffic; it can monitor the international gateway climate within South Africa.

2.1.2. Telecom Operators and Governments are losing revenues from international interconnect fees due to uncontrolled leaks. There are many cases in which incoming international traffic is being bypassed and the Command Line Interface (CLI) of incoming international calls are being manipulated to a local CLI before routing the calls.

2.1.3. This highlights the need for reliable monitoring systems to address such losses, ensure effective revenue mobilization and ensure continuous monitoring to avoid further losses. An effective Revenue Assurance system verifying the international voice revenue is therefore critical for achieving high levels of effectiveness at collecting revenue from the telecom industry.

2.1.4. This should apply equally to local and international calls on mobile and fixed networks as well as to anti-fraud services. This requires deploying special technology and infrastructure to ensure the success of such a project. Proper deployment of this technology eliminates the concept of “single point of failure” and all the disadvantages of introducing a point of failure into the Revenue Assurance network through critical applications.

[2] Anecdotal data estimates the loss to the fiscus at R100 million per annum based on data from only on one licensee.

2.1.5. The purpose is to have real-time aggregation and monitoring of all international calls to serve the following objectives:

2.1.6. Provide the Authority with a clear and independent view to monitor the telecom industry.

2.1.7. Allow the ministry in charge of finance, the ministry in charge of communications and digital technologies and the regulator to access credible data from the telecom sector - monitored independently for the purposes of formulating policy - for the benefit of consumers and the economy.

2.1.8. Serve as an independent benchmark for auditing telephone operators and for cross-checking their income declarations and remittance of taxes.

2.1.9. Detect unwanted loss of revenue and maximise revenue collection for the fiscus.

2.1.10. The International Voice Gateway should be equipped with a set of functionalities that enable Subscribers to receive better service quality, the Government to regain lost revenue at zero cost, and the Operators to properly manage their revenue streams. The benefits can be summarised as following:

2.1.11. Better quality of international calls to and from mobile and fixed networks that will satisfy the subscribers’ needs and expectations, and a higher capacity for international traffic which allows for more inbound and outbound calls;

2.1.12. Monitoring and controlling all VoIP, grey routes and illegal traffic through SIM-Boxes, call centres and CLI manipulation, which results in better security and more control over security issues;

2.1.13. Prevent any hidden revenues not declared by operators, stop tax evasion and restore substantial lost revenues using good management, with the billing and collection of all taxes from voice traffic reported by operators, mitigate against fraudulent traffic management and offer full transparency.

2.1.14. Provide a Net settlement service for international voice traffic, local operators and carriers.

3. Functional Specifications

The Authority intends to appoint a service provider to supply, install and support a centralised and complete International Voice Gateway which can manage and monitor all international calls (incoming and outgoing). It should be designed in a modular way with multiple technical and security features to maximise revenue and minimise fraud.

Bidders must submit proof (e.g. datasheets, product manuals, catalogues, etc.) to confirm/verify that the proposed system conforms to the Architecture, Requirements, Technical Parameters, Special Reporting Requirements listed below:

3.1. Hardware, Documents and Training

The scope of work includes the following deliverables:

Table 1 Project Deliverables

ITEM NUMBER	BRIEF DESCRIPTION
	International Voice Gateway System
3.1.1.	Service provider/Vendor's side International Voice Gateway (with all supporting hardware, software, licenses and databases). Breakdown as follows: 1. Centralised voice gateway module 2. Revenue Assurance Module 3. OTT Bypass Module 4. Sim Box detection Module **Note:** *a) The supplier shall provide International Voice Gateway hardware requirements and specifications to ICASA.*

	b) The supplier shall integrate and setup the proposed solution.
	Documentation
3.1.2.	Electronic copy of the International Voice Gateway System operational manuals
3.1.3.	Electronic copy of the International Voice Gateway System design documents
	Support
3.1.4.	Provide support for the module for five years. Support to kick-off immediately after implementation (on acceptance). Service Level Agreement (SLA) to be implemented between the parties within one month of delivery and acceptance of the system.
	Training
3.1.5.	Full training must be provided to staff members of the Authority. A minimum of twenty-five (25) employees of ICASA must be trained at no additional cost to ICASA. Provide additional refresher training during the maintenance and support period upon system enhancements release or whenever needed.

3.2. Centralised Voice Gateway

3.2.1. The International Voice Gateway shall:

3.2.2. Aggregate all international incoming and outgoing call traffic and terminate it towards local or international mobile operators.

3.2.3. Analyse, detect, and block all unwanted traffic.

3.2.4. Provide Performance Reports and traffic analysis reports.

3.2.5. The system needs to be configured with performance-management alarms in response to service degradation. The system should be able to:

3.2.6. Customise reporting: Configure automatic email alerts for network events (align with service-affecting incidents).

3.2.7. Allow access control configurations (administrator profile and general users' profile (priority and non-priority) to ensure maximum security.

3.2.8. The Authority and the service provider will conduct Provisional Acceptance

Testing (PAT) of the system. PAT is conducted to determine if the requirements specified by the contract are fulfilled after each implementation milestone.

3.3. Revenue Assurance

3.3.1. The Revenue Assurance module should enable the Authority to provide assurance to the National Treasury and South African Revenue Service (SARS) that revenue generated by licensees from international calls is properly billed and accounted for and that processes designed to ensure revenue assurance are functioning in the most efficient possible way. The technology needs to collect data from various sources to address a variety of income assurance challenges.

3.3.2. The proposed solution should cover the following aspects:

3.3.3. Unrated Usage: Analyses network traffic and provides predefined dashboards. This can be supplemented by the Usage Segment module to calculate the customer base (subscribers) of all operators in a consistent manner. Covers call profiles and endpoint analysis.

3.3.4. International Usage: Analyses international traffic and provides predefined dashboards.

3.3.5. Interconnection Usage: Analyses the traffic of interconnection gateways and provides predefined dashboards.

3.3.6. Roaming Usage: Analyses customer traffic of the Operator while roaming abroad

3.3.7. Mobile Wallet: Analyses mobile (electronic) wallet transactions and associated controls.

3.3.8. The proposed solution should also cover the following aspects of income assurance and fraud detection:

3.3.9. Usage: Analyses the consistency of several CDR sources (local / international Interconnection, MO / MT, Rating / IN, TAP files, Probes). Consistency checks are carried out at macro and micro levels (reconciliation at CDR level) and compared with detected live data traffic

3.3.10. Interconnect: Analyses the quality of the interconnection.

3.4. OTT Bypass

3.4.1. The solution should enable the Authority to efficiently identify OTT interconnect bypass losses in an efficient manner using end-to-end testing on an unlimited number of international routes, all in a fully managed service. The OTT bypass solution should also support the following:

3.4.2. Management and execution of test calls

3.4.3. Complete configuration of the Platform

3.4.4. Supervision and monitoring of test results

3.4.5. CLI verification analysis

3.4.6. Filtering and identification of OTT Bypass cases

3.4.7. Generation of notifications for detected OTT Bypass

3.4.8. Automatic generation of reports

3.4.9. Detailed monthly reports

3.4.10. Remote maintenance of the Platform

3.4.11. Facilities for monitoring and reporting

3.5. Fraud detection

3.5.1. The Fraud detection (detection, profiling) service should be fully managed and should efficiently identify SIM Box usage with extrapolation using profiling and CDR fingerprints.

3.5.2. The Fraud detection service should offer precise geolocation of the SIM Box.

3.5.3. The Fraud detection service should include the following elements and deliverables:

3.5.4. Definition of the test scenario

3.5.5. Management and execution of test calls: The system should originate test calls from probes worldwide and terminate them on a local unit.

3.5.6. Detection, tracking and localization of all forms of traffic bypass or traffic refiling into networks in South Africa.

3.5.7. Control and monitoring of test results

3.5.8. CLI verification analysis

3.5.9. Filtration and identification of SIM Boxes

3.5.10. Full configuration of the Platform

3.5.11. Creation of alerts and notifications in case of detected SIM Boxes

3.5.12. Creation of automated reports

3.5.13. Detailed monthly summaries

3.5.14. Remote maintenance of the Platform

3.5.15. Reporting systems

3.5.16. Dedicated customer service

4. Product Support and Licensing

4.1 The supplier must have capacity to maintain, repair and replace all components of the system in a timely manner.

4.2 Local presence in South Africa is critical, as the Authority requires service with short lead times.

4.3 The supplier must have an online portal for logging failures and complaints and may supplement this portal with other reporting platforms.

4.4 The bidder must state the manufacturer’s end of support for this solution, which shall not be less than 5 years from final acceptance of the system.

4.5 The bidder shall provide the licenses to be used, remote upgrades of software and any installation of software patches. Licenses must be valid for at least 5 years from installation of the system.

4.6 The bidders must state any third party or supplier they are involved with in supplying the solution.

4.7 The bidder shall provide the product roadmap for the proposed solution.

4. Period of assignment

All work is to be carried out in accordance with the timeline as agreed with the Authority. The Authority will not be responsible for any cost incurred due to an extension of the project resulting from delays by the Supplier.

ANNEXURE C1: INTERNATIONAL A2P GATEWAY

1. Purpose of ANNEXURE C1

1.1 The purpose of Annexure C1 is to highlight the technical and functional requirements and specifications of the International A2P Gateway which the Independent Communications Authority of South Africa (hereinafter referred to as ("the Authority") is seeking to acquire as per the terms and conditions outlined herein.

2. Background

1.2 International A2P SMS is the process of sending mobile messages from an application to a mobile user. Businesses can use it in several technical modes to communicate with consumers, authenticate users of online services, or deliver time-sensitive alerts.

1.3 Typical examples of A2P SMS include banking notifications, critical alerts, SMS-based two-factor authentication, automatic booking confirmations, loyalty programs, and marketing notifications, etc. Online reservation systems, different corporate platforms, and support services have deployed A2P SMS to increase efficiency and improve communication.

1.4 The A2P International Gateway is a module that aims to establish a central automated system with the best specifications, technical and security services, to collect all international A2P traffic and terminate it towards local subscribers through local operators, in addition, to analyse, detect and block all unwanted traffic.

3. Functional Specifications

3.1. The Authority intends to appoint a service provider to supply, install and support a centralised and complete International A2P SMS Gateway to collect, monetise and monitor all international A2P Traffic and deliver it towards local subscribers through local operators while maintaining local MNOs revenues.

3.1.1. The system shall provide content analysis mechanisms for SMS messages, including keyword triggers by the system automatically.

3.1.2. The system shall be able to quarantine, screen, block, and/or drop SMS messages based on pattern and content analysis by the system automatically.

3.1.3. The system shall support a Grey Route detection, to identify International A2P traffic which is arriving from other networks other than the operators set as trusted.

3.1.4. The system shall include a spam/fraud database, which shall collect data from suspicious A-numbers, Global Titles, URLs, etc.

3.1.5. The system shall support Text Filtering, which is filtering a message by specific content (if the content is including a known A-number when compared to the spam/fraud database, if the content is including a known URI/URL when compared to spam/fraud database).

3.1.6. The system shall support a reputation filter, which is comparing A-number for sender history in a spam/fraud database.

3.1.7. The system shall support a real-time graphical view of international A2P SMS flow traffic. A2P platform should have a flexible tool to provide an instant, graphical overview of the volumes of traffic being allowed and filtered on a network. Completed reports should be sent to responsible persons daily. The detailed report must contain mandatory fields such as Date, GT content-provider’s name, sender name (alpha number), the quantity of local A2P, the quantity of international A2P, services division (Facebook, Apple, Google, etc.)

3.1.8. The system shall be able to identify A2P international traffic.

3.1.9. The system shall have a blacklist of GTs and sender (MSISDNs and alpha-name)

3.1.10. The system shall provide statuses of all traffic online (real-time, delivered, not delivered)

3.1.11. The System should have the possibility to block traffic for client/providers who are sending International A2P SMS using different content criteria (absence of brands, digits, any keyword, and so on).

3.1.12. The system should include a built-in alert system with automatic sending of notifications (by mail) to the concerned person/s.

3.1.13. The system should handle not less than 1000 connects (SMPP, SIGTRAN, HTTP)

3.1.14. The system shall store SMS content, MSISDN, sender name in DB. It should be able to replace secure/critical information with symbols.

Bidders must submit proof (e.g. datasheets, product manuals, catalogues.) to confirm/verify that the proposed system conforms to the Architecture, Requirements, Technical Parameters, Special Reporting Requirements listed below:

3.2. Hardware, Documents, and Training

The scope of work includes the following deliverables:

Table 1 Project Deliverables

ITEM NUMBER	BRIEF DESCRIPTION
	International A2P SMS Gateway
	Service provider/Vendor's side International A2P firewall Gateway (with all supporting hardware, software, licenses, and databases). Break down as follows: 5. Firewall Application Software 6. Firewall requisite Hardware 7. Software licenses 8. Database prerequisite 9. Various Pricing options (inclusive of the hardware or excluding it) ICASA's side 1. Centralised Gateway and firewall Application software 2. Centralised Gateway and firewall requisite Hardware 3. SMPP and HTTPS connectivity to the 4 operators **Note:** c) *The supplier shall provide international SMS Gateway hardware requirements and specifications to ICASA.* d) *The supplier shall integrate and set up the proposed solution.* e) *ICASA will provide virtual dedicated links (e.g. SMPP sufficient link between Operators and ICASA Head Office)*
	Documentation
	The documentation shall be available in electronic form. Product documents, feature descriptions, and release notes of the ordered product shall be provided. The documentation of the delivered system shall be available online via support web pages.

	The documentation shall include all components of the system, in necessary detail, including IP addresses, physicals ports, configurations, connections, links to external systems, etc.
	The system to be delivered had to be documented so that all components and software releases are listed.
	The documentation shall be up to date, clear, and easy to understand and covers the delivered components (delivery documentation) from the product level down to the individual component level. Product codes and serial numbers shall be included.
	Documentation shall describe the management architecture (SS7 management, IP management, node management and describe also management rights if there are different user rights to manage these features)
	The vendor shall provide system documentation for alarm handling and other related issues.
	The vendor shall provide separate technical solution description document containing all relevant information on the purchased system with purchaser specific configurations (i.e. architecture, network elements, connections, availability, fail-over scenarios, back-ups)
	Support
	The vendor shall provide a proposal for technical support and maintenance, including initial installation, planned SW upgrades, trouble reporting, and responsive actions of received trouble reports, in addition to 24/7 prioritised emergency support.
	Training
	The vendor shall provide full training to staff members of the Authority. A minimum of twenty-five (25) employees of ICASA must be trained at no additional cost to ICASA. The vendor shall provide additional refresher training

	during the maintenance and support period upon releasing system enhancements or whenever needed.

3.3. Network Architecture and configuration

The network architecture must be able to accommodate more operators over and above the ones stated in Figure 1 below.

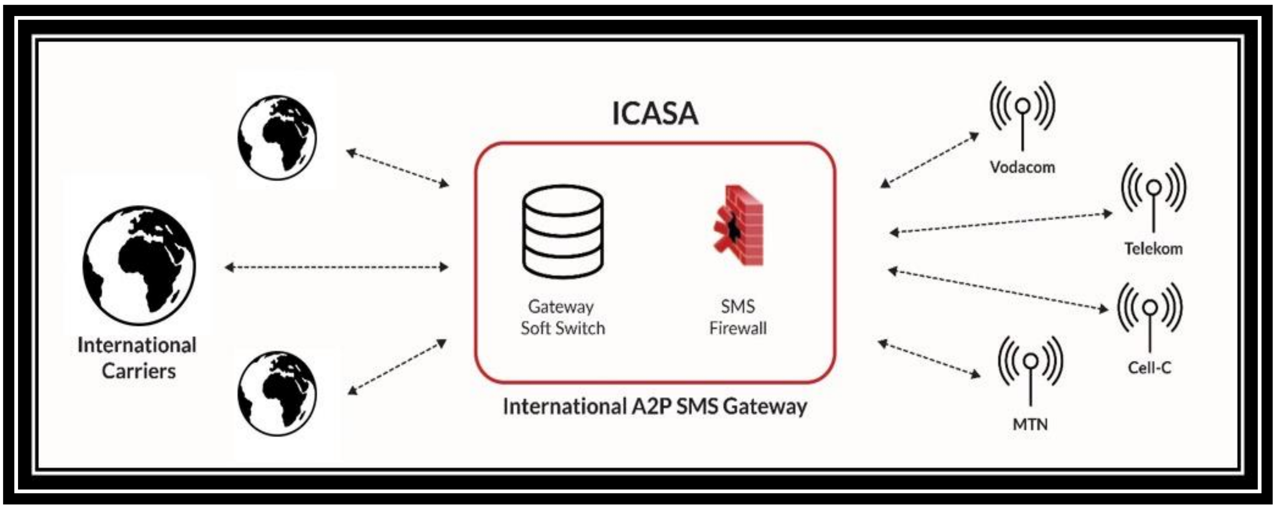

Figure 1: International SMS Gateway Topology

3.3.1. The required international A2P SMS Gateway shall:

3.3.1.1. Collect all international A2P traffic and terminate it towards local subscribers through local operators.

3.3.1.2. Analyse, detect, and block all unwanted traffic.

3.3.1.3. Control all remote firewalls at the operator level.

3.3.1.4. Control SMS traffic and stop SMS leakage from unauthorised sources.

3.3.1.5. Provide Performance Reports and traffic analysis reports.

3.3.1.6. Shall be expandable, to accommodate more entrants (licensees) in the future.

3.3.2. The system needs to be configured with performance-management alerts in response to service degradation. The system should be able to:

3.3.2.1. Customise reports: Configure automatic email alerts on network events (align with service-affecting incidences).

3.3.2.2. Perform access control configurations (administrator profile and general users' profile (priority and non-priority) to ensure maximum security.

3.3.3. The Authority and the service provider will conduct Provisional Acceptance Testing (PAT) of the system. PAT is conducted to determine if the requirements of a specification or contract are fulfilled after each implementation milestone.

3.4. Product Support and Licensing

3.4.1. The supplier must have the capacity to maintain, repair, and replace all components of the system in a timely manner.

3.4.2. Local presence in South Africa is critical, as the Authority requires service with short lead times.

3.4.3. The supplier must have an online portal for logging failures and complaints and may supplement this portal with other reporting platforms.

3.4.4. The bidder must state the manufacturer's end of support for this solution, which shall not be less than 5 years from the installation of the system.

3.4.5. The bidder shall provide the licenses to be used, remote upgrades of software, and any installation of software patches. Licenses must be valid for at least 5 years from the installation of the system.

3.4.6. The bidders must state any third party or supplier they are involved with in supplying the solution.

3.4.7. The bidder shall provide the product roadmap for the proposed solution.

3.5. General Requirements

3.5.1. The International A2P SMS Gateway has the following general requirements:

3.5.1.1. The proposed solution shall be a fully redundant system and redundancy shall apply to all application modules.

3.5.1.2. The platform should have a free SW licensed model and be limited only by computing (HW) resources.

3.5.1.3. The platform shouldn't use any 3rd party license-dependent software.

3.5.1.4. If the platform has embedded or otherwise uses any 3rd party software (e.g. database), Bidder shall submit an authorization letter from Licensee.

3.5.1.5. The platform shall support virtualization technology to allow optimal usage of hardware resources, considerably reduce footprint, power consumption, and required maintenance.

3.5.1.6. The Virtualization technology shall allow seamless allocation of new resources (i.e. virtual environment resources) to be assigned to any of the existing applications on Platform. It shall have no impact on the application being expanded and the other running modules

3.5.1.7. The platform shall provide a Web-based GUI tool to perform application/services administration and configuration changes by user admins.

3.5.1.8. The platform shall be easily scalable and have a modular architecture so that new capacity and features can be easily added by adding new computing resources and SW modules.

3.5.1.9. The platform should support changes with no service interruption

3.5.1.10. Participant shall provide complete sizing/dimensions of the platform

3.5.1.11. The platform shall provide configuration WS (WebService) APIs

3.5.1.12. The platform shall allow for configurations to be updated remotely.

3.5.1.13. The platform shall support the management of all alerts issued by all products through a single alarm management system.

3.5.1.14. The platform shall support GUI-based alert monitoring tool for active and previously stored alerts

3.5.1.15. Platform alerts can be filtered per application in addition to Host, Module, Alarm Level, Alarm Severity, Alarm Type, Alert Category (error, event), Start Time, and End Time.

3.5.1.16. The platform shall support access & rights management both for the whole platform and per application.

3.5.1.17. The platform shall provide historical records for each application. (6 months)

3.5.1.18. The platform shall support monitoring historical records on the provided Web-based GUI tool per application. (6 months)

3.5.1.19. Old data should be stored in an online or offline mode according to requestor’s requirement

3.5.1.20. The platform shall support API integration

3.5.1.21. The system shall support the NTP protocol for time synchronization.

3.5.1.22. The platform shall support SMPP v3.4

3.5.1.23. The system should be integrated with CODA (SOAP) via API to get different subscribers' info

3.5.1.24. The system shall be integrated with the network via Sigtran and shall receive the whole SIGTRAN traffic. The system should route back traffic not related to SMS in the same order as it was delivered to the platform.

3.5.1.25. The platform shall support number portability (MNP).

3.5.1.26. SIGTRAN connection should be protected and separated from usual IP traffic

3.5.1.27. Supplier shall submit preliminary execution plan (activities, timing)

3.5.1.28. The supplier must indicate all terms of third-party equipment – SLA, warranty, etc. if applicable

3.5.1.29. Bidder should have a clear roadmap and have a solution for the digitalization of OTT authentication and verification

3.6. Special Reporting requirements

3.6.1. The system should allow the building of new reports and changes to **the ready-made and regular reports** with ease.

3.6.2. Display customization

3.6.3. Dashboard Customization

3.6.4. Automated reporting

3.6.5. Support of multiple output reports, such as PDF and Excel reports

3.7. Technical Parameters/ Key performance indicators (KPIs):

3.8. The System shall have the capability to monitor significant events related to gateway KPIs, not limited to the following:

3.8.1. ***<u>Generic KPIs:</u>***

3.8.1.1. SMS Transit Service Availability

3.8.1.2. SMS Transit Service Availability Per Destination

3.8.1.3. Maximum Time To restore Service

3.8.1.4. Service Provisioning Time Frame

3.8.2. ***<u>KPIs per Connection Type:</u>***

3.8.2.1. SS7 Connection Type:

3.8.2.1.1. SRI Message Failure Ratio

3.8.2.1.2. SRI Message Process Time

3.8.2.1.3. SMS Message Failure Ratio

3.8.2.1.4. SMS Message Process Time

3.8.2.1.5. SMS Transmission Time

3.8.2.2. SMPP Connection Type:

3.8.2.2.1. SM Message Failure Ratio

3.8.2.2.2. SM Message Process Time

3.8.2.3. Hybrid SS7 to SMPP Connection Type:

3.8.2.3.1. SMS Message Failure Ratio

3.8.2.3.2. SMS Message Process Time

3.8.2.4. Hybrid SMPP to SS7 Connection Type:

3.8.2.4.1. SMS Message Failure Ratio

3.8.2.4.2. SMS Message Process Time

4. Period of assignment

All work is to be carried out in accordance with the timeline as agreed with the Authority. The Authority will not be responsible for any cost incurred due to an extension of the project resulting from delays by the Supplier.

ANNEXURE C2: OTT & VOIP SYSTEM

1. Purpose of ANNEXURE C2

1.1. The purpose of Annexure C2 is to highlight the technical and functional requirements and specifications of the OTT & VOIP System which the Independent Communications Authority of South Africa (hereinafter referred to as "the Authority") is seeking to acquire as per the terms and conditions set out herein.

2. Background

2.1. The OTT & VOIP System is designed to detect data traffic of VOIP calls.

2.2. The purpose of the VOIP Calls Data rate differentiation is to monitor emergence of new revenue streams emanating from new technologies (especially OTTs) and to assess the extent of any revenue losses due to increased adoption of new technologies at the expense of traditional services (i.e. GSM calls).

2.3. The Authority is required to licence electronic communications services in the public interest and to this end to inter alia facilitate convergence of services, promote development of interoperable and interconnected electronic networks and create a technology neutral licensing regime.

2.4. The purpose of this sub-module is to enable the Authority to gather reliable data for purposes of executing its mandate. The project will serve the following objectives:

2.4.1. Monitoring new revenue streams emanating from new services and assessing lost revenue due to increased OTT usage at the expense of the GSM calls.

2.4.2. Monitoring and gathering data on VOIP traffic.

2.4.3. Fraud detection.

3. Functional Specifications

3.1. ICASA intends to appoint a service provider to supply, install and support a VOIP and OTT system which can manage and monitor all the international and local calls (incoming and outgoing) over IP. It should be designed in a modular way with multiple technical and security features to maximise revenue and minimise fraud.

3.2. The OTT & VOIP System is intended to:

3.2.1. Compensate for lost revenue caused by the drop in local and international GSM Voice calls without increasing taxes or adding any new tariffs on Operators

3.2.2. Set a dynamic centralised nationwide rate for National and International VOIP calls based on volume of call minutes

3.2.3. Differentiate VOIP traffic to enable reporting of statistics on application, usage and performance; allow for the establishment of different rates for different OTT applications (e.g.: charging WhatsApp calls at a different rate than Viber calls)

3.2.4. Unlock additional revenues by increasing end-user data consumption generated from VOIP Calls, without obviously or heavily impacting users.

Bidders must submit proof (e.g. datasheets, product manuals, catalogues, etc.) to confirm/verify that the proposed system conforms to the Architecture, Requirements, Technical Parameters, Special Reporting Requirements listed below:

3.3. Hardware, Documents and Training

The scope of work includes the following deliverables:

Table 1 Project Deliverables

ITEM NUMBER	BRIEF DESCRIPTION
	International Voice Gateway System
	OTT & VOIP Charging system (with all supporting hardware, software, licenses and databases). Breakdown as follows: 0. VOIP call charging 1. Data centralization & Synchronization 2. VOIP Quality of Service **Note:** *f) The supplier shall provide OTT & VOIP Charging system hardware requirements and specifications to ICASA.* *g) The supplier shall integrate and setup the proposed solution.*
	Documentation
	Electronic copy of the OTT & VOIP Charging system operational manuals
	Electronic copy of the OTT & VOIP Charging System design documents
	Support
	Provide support for the module for a period of five years. Support to kick-off immediately after implementation (on Acceptance). Service Level Agreement (SLA) to be implemented between the parties within one month of delivery and acceptance of the system.
	Training
	Provide full training to staff members of ICASA. A minimum of twenty-five (25) employees of ICASA must be trained at no additional cost to ICASA. Provide additional refresher training during the maintenance and support period upon system enhancements release or whenever needed.

3.4. Network Architecture and configuration

Figure 1 below shows the network architecture and configuration with four main operators in the South African ICT market but the module must be able to accommodate more operators that will join the market in future.

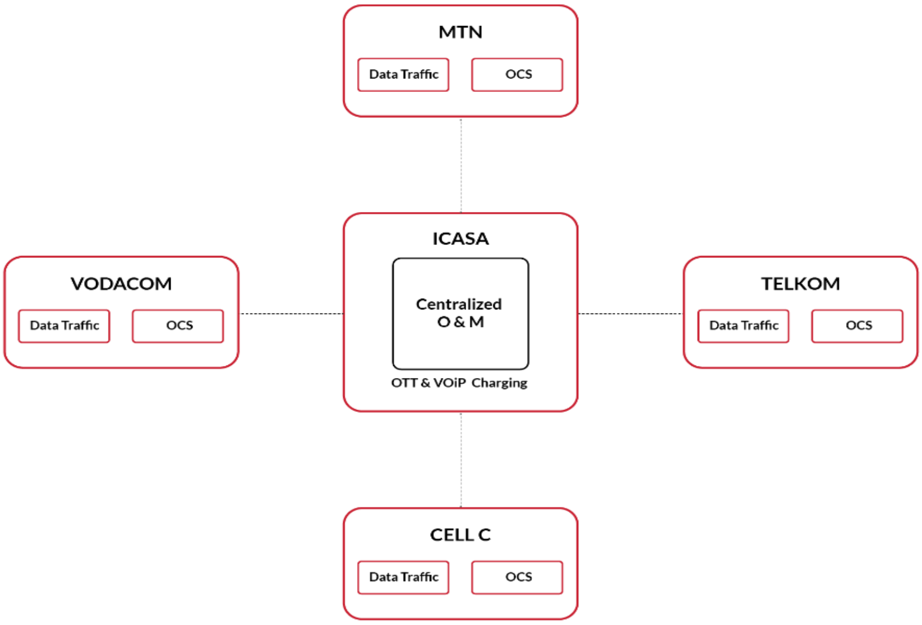

Figure 1: Set up and connection of OTT & VOIP charging system

3.4.1. ***VOIP Call Charging***

3.4.1.1. The proposed system should support charging for VOIP calls through different models:

3.4.1.1.1. Prepaid vouchers: a subscriber could purchase a VOIP voucher and recharge his/her account, allowing him/her to make or receive calls for a specific number of minutes or during a specific period.

3.4.1.1.2. Real-time call charging: the VOIP calls will be charged like any GSM calls in real time. Call rates should be configurable.

3.4.1.1.3. Postpaid charging: this charging feature requires a profiling engine which will define the eligibility to access postpaid VOIP charging or not depending on an assessment of payment failure risk.

3.4.1.1.4. Integrated charging from the regular data bundles with a different consumption rate

3.4.2. ***Data Centralization & Synchronization***

3.4.2.1. The proposed system should have a centralised system located on ICASA's premises or any other authorised location which should be connected to all mobile operators or data providers.

3.4.2.2. The purpose of the centralization is to have a real-time synchronization between the local entities from one end and central entity to another end, providing the following capabilities:

3.4.2.3. Synchronization of call event records

3.4.2.4. Synchronization of all charging activities in real time

3.4.2.5. Pushing voucher and charging configuration from central to local systems

3.4.3. ***Quality of service***

3.4.3.1. The proposed system should guarantee a high level of quality of service and ensure that the added charging concept and the platform behaviour are not impacting the user experience.

3.4.3.2. The system should provide a high availability and offer uninterrupted service.

4. Product Support and Licensing

4.1. The supplier must have capacity to maintain, repair and replace all components of the system in a timely manner.

4.2. Local presence in South Africa is critical, as the Authority requires service with short lead times.

4.3. The supplier must have an online portal for logging failures and complaints and may supplement this portal with other reporting platforms.

4.4. The bidder must state the manufacturer's end of support for this solution, which shall not be less than 5 years from final acceptance of the system.

4.5. The bidder shall provide the licenses to be used, remote upgrades of software and any installation of software patches. Licenses must be valid for at least 5 years from installation of the system.

4.6. The bidders must state any third party or supplier they are involved with in supplying the solution.

4.7. The bidder shall provide the product roadmap for the proposed solution.

5. Period of assignment

All work is to be carried out in accordance with the timeline as agreed with the Authority. The Authority will not be responsible for any cost incurred due to an extension of the project resulting from delays by the Supplier.