Annex 1 to the Contract No. 138/2025/IS/076

Technical specification

for

**"ATIS LKCS
legacy/VoIP GateWay (GW)"**

LIST OF CONTENTS

1   GENERAL REQUIREMENTS

1.1   General requirements for the HW, SW and OS

All delivered equipment **shall** be designed for continuous operation, 24 hours per day and 365 days a year.

All hardware to be supplied **shall** be new, off-the-shelf and currently in production.

All electrical equipment **shall** be compatible with the Czech electrical norms according to APPENDIX 1 .

Any COTS operating system (if used) **shall** be supplied as the latest available software version released by manufacturer to ensure the full support can be provided as long as possible, unless specified otherwise.

To avoid all doubts, the Parties hereby state, that the provision of the System Development and the Training by the Contractor to the Customer according to the Contract **shall not** include any obligation or commitment of the Contractor as regards dismounting, liquidation, or any other handling with the current hardware, which is deployed in the premises of the Customer and will be partially renewed according to the Contract, or uninstallation of software currently installed on such hardware. Dismounting of the current hardware, uninstallation of the software currently installed on such hardware **shall** be the sole obligation of the Customer at its own costs.

1.2   *Applicable Documents*

The Contractor **shall** deliver the system in compliance with herein stated documents in their last available valid versions, including all amendments and supplements or recently discovered defects, errors or findings.

[1] ED-137B - Interoperability Standard for VOIP ATM Components – Volume 1: Radio", latest available version

[2] ED-137B "Interoperability Standard for VOIP ATM Components – Volume 5: Supervision", latest available version

[3] SIP: Session Initiation Protocol, RFC3261, latest available version

[4] RTP: Real-time Transport Protocol, RFC3550, latest available version

[5] ICAO Annex 10, Volume 2, Edition 7 (November 2020)

2   TECHNICAL REQUIREMENTS

Due to the technology progress and the expected run-time of the project, the **Contractor** shall deliver and install the "most recent" available platform from the brand proposed, for the price quoted and with a configuration (processing power, memory, disk capacity, communication adapters, etc.) equal or greater than the one in the offer. It is understood by "most recent" the latest model (in agreed category/generation/vendor) present on the market at the actual HW delivery date minus the normal delivery time. The same rule is applicable to the Operating Software version unless agreed otherwise.

2.1   HW configuration

The purpose of this chapter is to give detailed configuration and the list of the components in each node(s) of the system.

2.1.1   Servers / v-servers

Any management server(s), if needed, **shall** be delivered as Virtual server (v-server), virtualized on vmWare ESXi (virtualization) platform(s), version 7.0 or higher.

> _Note:_ The System can be delivered as a Virtual Appliance(s).

The virtualization platform(s) is already in place on current Purchaser's HW. Any potential new vmWare ESXi virtualization platform(s) **shall not** be part of the delivery.

2.1.2   Operator's workstations

--- Intentionally Left Blank ---

2.1.3   specific equipment

The HW and Operating System (OS) configuration of the delivered specific equipment – "legacy/VoIP GW" **shall** be:
- Dual Power Supply 230V AC
- Dual RJ45 connectivity
  - from/towards reception of legacy voice
  - from/towards ATC VoIP LAN (ATC VoIP traffic)
  - from/towards non-ATC VoIP LAN (non-ATC VoIP traffic)
  - from/towards LAN (management)
- rack mount
  - 1U size is preferred (not mandatory)

2.2   System security and Remote access

User access by means of the Operational system tools and functions **shall** be validated by unique personal id/username and password.

The program code version **shall** be clearly identified by version (not only date of issue), checksum of all binaries, scripts and/or other executable files.

The configuration files **shall** be clearly identified whether the configuration files are used for Operational or Test system.

All workstations and servers within ANS CR premises **are** protected against unauthorized access to its unused devices, such as CDROMs, UBS ports, LAN or CONSOLE ports (e.g. Ethernet port not used shall be disabled). The Contractor **shall** respect this ANS CR policy.

3 OPERATIONAL REQUIREMENTS

The purpose of this chapter is to define new required functions in all system (subsystem) parts.

The legacy/VoIP GW shall serve as equipment dealing with conversion from legacy to ATC VoIP and non-ATC VoIP voice (at the same time) while interconnected to ATIS system. At the same time, it shall implement functions to protect potential simultaneous transmission from both ATIS servers in case of their native malfunction.

3.1 SW functions of the "legacy/VoIP GateWay"

The Contractor **shall** deliver a legacy/VoIP GW as defined by following applicable documentation and standards: [1], [2], [3] and [4]
upgrade of the system where all existing (currently implemented) functionalities shall be maintained and unchanged by this upgrade. Modification of existing functionalities is possible only if such a change is requested and approved by the Customer.

The definition of the Software functions required for the legacy/VoIP GW is written in chapters 3.1.1 - 3.1.6.

3.1.1 Legacy voice [A1.1.1]

[A1.1.1.1] _reception of Legacy voice (audio input)_
- The legacy/VoIP GW **shall** allow reception from two alternative legacy voice sources.
  The alternative legacy voice sources are:
    o ATIS server Master
       transmitting/generating legacy audio
    o ATIS server standby
       ready to take role of the Master in case of failure.
- The legacy/VoIP GW **shall** follow the first come first serve principle (following the decisions of primary/secondary source of legacy voice from the voice source(s).
- The legacy/VoIP GW **shall** have the functionality of switchover to secondary source of legacy voice, after defined period of time – see [A1.1.2]
- The legacy/VoIP GW **shall** protect potential malfunction of ATIS server(s) and prevent / deny of simultaneous processing of legacy voice signal from both sources (ATIS server(s)) at the same time.
- The legacy/VoIP GW **shall** receive the legacy voice audio signal on audio jack 3,5' and/or RJ45
- The Contractor **shall** specify on which PINs of the RJ45 the analog audio signal from Customer's ATIS system is expected to be provided.
- The Contractor **shall** not deliver any audio 3.5' jack <> RJ45 LAN cable, it is responsibility of Customer to provide such cabling.

[A1.1.1.2] _switchover/protection timer_
- The legacy/VoIP GW **shall** implement configuration parameter – timer for switchover/protection between switchovers when primary source of legacy voice is detected as lost.
- The timer for switchover/protection between switchovers **shall** be configurable in ms (milli-seconds).

- Timer for switchover/protection between switchovers **shall** be from range between 550ms and 8000ms, with default setup at the time of delivery to 3500ms.

  Note: This parameter shall allow configuration of audio pause at the end of / before repetition of next ATIS session, without switching over to secondary legacy voice in due to expectations, the primary legacy audio source is lost.

3.1.2 ATC VoIP traffic [A1.1.2]

[A1.1.2.1] *ATC VoIP traffic (audio output - Critical)*
- The legacy/VoIP GW **shall** generate ATC VoIP traffic according to [1] and [2].
- The legacy/VoIP GW **shall** generate ATC VoIP traffic at the same time as non-ATC VoIP traffic, with same content.
- The legacy/VoIP GW **shall** allow definition of primary and secondary Tx (Transmitter(s)), accessible via routed AGVN network (not in the same network subnet).
- The legacy/VoIP GW **shall** monitor status and accessibility of primary and secondary Tx (Transmitter).
- When communication failure with primary Tx is detected, the legacy/VoIP GW **shall** automatically redirect the generated audio to secondary available Tx.
- When communication failure with one of Tx(s) is detected, an alarm **shall** be internally declared by the system. Such alarm shall be as well propagated to SNMP MIB, accessible via management LAN (not via ATC VoIP interface(s)).

- The legacy/VoIP GW **shall** allow configuration of gain (volume output) of ATC VoIP traffic, allowing finetuning of audio output towards the Tx(s). The adjustment of gain of ATC VoIP traffic and/or non-ATC VoIP traffic at the same time (by one parameter) is acceptable.

- The legacy/VoIP GW **shall** use separate RJ45 LAN ports to be connected directly into AGVN segment of the network.
- The legacy/VoIP GW **shall** allow bonding / teaming of those RJ45 LAN ports – logical LAN interface.
- The legacy/VoIP GW **shall** allow configuration of specific IP address above this logical bonded LAN interface, together with all other network configuration parameters (e.g. net-mask, default GW, etc.)

3.1.3 non-ATC VoIP [A1.1.3]

[A1.1.3.1] *non-ATC VoIP traffic (audio output – non-Critical)*
- The legacy/VoIP GW **shall** generate non-ATC VoIP traffic according to [3] and [4]
- The legacy/VoIP GW **shall** generate non-ATC VoIP traffic at the same time as ATC VoIP traffic, with same content.
- The legacy/VoIP GW **shall** act as SIP server where the non-ATC VoIP calls will be routed to by call manager (SIP telephony exchange server) of the Customer.
- The legacy/VoIP GW acting as SIP server **shall** handle at least 4 simultaneous incoming calls at the same time (conference call).

- The legacy/VoIP GW acting as SIP server **shall**:

- o allow only listening to the generated audio server by the calling party (audio output)
    - o deny any audio input from the calling party
- The legacy/VoIP GW **shall** allow configuration of call manager (SIP telephony exchange server) with following parameter(s) as minimum:
    - o IPv4
    - o Login name
    - o Password
    - o SIP number
- When a communication failure with call manager (SIP telephony exchange server) is detected, an alarm **shall** be internally declared by the system. Such alarm shall be as well propagated to SNMP MIB, accessible via management LAN (not via non-ATC VoIP interface(s)).

- The legacy/VoIP GW **shall** allow configuration of gain (volume output) of non-ATC VoIP traffic, allowing finetuning of audio output towards the Tx(s). The adjustment of gain of ATC VoIP traffic and/or non-ATC VoIP traffic at the same time (by one parameter) is acceptable.

- The legacy/VoIP GW **shall** use separate RJ45 LAN ports to be connected directly into segment of the network of regular (non-ATC) telephony
- The legacy/VoIP GW **shall** allow bonding / teaming of those RJ45 LAN ports – logical LAN interface.
- The legacy/VoIP GW **shall** allow configuration of specific IP address above this logical bonded LAN interface, together with all other network configuration parameters (e.g. net-mask, default GW, etc.)

3.1.4 management [A1.1.4]

[A1.1.4.1] *management LAN of the GW, SNMP, user access*
- The legacy/VoIP GW **shall** use separate RJ45 LAN ports to be connected directly into LAN segment of the network for non-critical, non-voice related data communication, i.e. management of the legacy/VoIP GW.
- The legacy/VoIP GW **shall** allow bonding / teaming of those RJ45 LAN ports – logical LAN interface.
- The legacy/VoIP GW **shall** allow configuration of specific IP address above this logical bonded LAN interface, together with all other network configuration parameters (e.g. net-mask, default GW, etc.)
- When internal alarm is set within the system, management LAN **shall** be used as the only interface for communication with Customer's CMOS SNMP monitoring.

- User access by means of the system tools, administration GUI and functions **shall** be validated by unique personal id/username and password.
- The system **shall** allow definition of user access rights (e.g. setting read-write or read-only policy, etc.) and user roles (e.g. Administrator, Technical Operator).
- The user(s) with the same access rights shall be allowed to be grouped (e.g. setting up the rights to the group(s) and assigning user(s) to one user group or multiple user groups.

- The system **shall** log for purposes of Legal recording and Investigation all relevant configuration changes, logs and activities.
- The system **shall** allow configuration period for Legal recording and Investigation.
- The configurable period **shall** not be lower than 30 days for the purpose of Legal Recording and Investigation as specified in [5].

3.1.5　VMware image deliverable(s) [A1.1.5]

[A1.1.5.1] ***VMware image deliverable(s) – management v-server***

- The Contractor **shall** deliver the management server/cluster as follows:
  - VMware images of one management Web servers for management of the configuration of "legacy/VoIP GW";

  based on provided technical information on target internal network environment of Customer and CMOS SNMP monitoring.
- The Customer **shall** provide technical information on target internal network environment and CMOS SNMP monitoring.
- SNMP community name **shall** be defined in configuration file(s).
- SNMP agent **shall** be accessible or shall respond only when called from IP addresses defined in configuration file(s).
- The SNMP interface data provision via SNMP interface **shall** be coded according to APPENDIX 2 .
- The Contractor **shall not** deliver the VMware software or the license key(s) for the VMware virtualization platform. The Customer will host the provided VMware machines on Customer's VMware virtualization platform.

3.1.6　Configuration of the system [A1.1.6]

[A1.1.6.1] ***Contractor's assistance***

- The Contractor **shall** assist during the process of configuration of the system upon Customer request.
- The Contractor **shall** assist during the process bringing the System into Operations upon Customer request.
- In case Customer would request on-site assistance by Contractor's personnel, the Contractor **shall** provide sufficient experience personnel to assist Customer with bringing the System into Operations.

[A1.1.6.2] ***Security policy***

- The System **shall not** have access to the internet (e.g. Operating system updates, Antivirus and software FW updates (if installed), etc.);
- The Customer created and uses proxy servers for "indirect" updates of the software components of the system. The Customer will provide IP addresses of Purchaser's proxy servers. The proxy servers of Customer **shall** be used by the system to enable update function on the level of Operating system, Antivirus and software FW (if FW installed) and other.
- The Contractor **shall** define a list of applications, services and operating system that shall be covered by Purchaser's proxy servers, if applicable.

APPENDIX 1   GENERAL TECHNICAL REQUIREMENTS CONCERNING ELECTRICAL INSTALLATIONS IN THE CZECH REPUBLIC

1.   Technical Conditions for the Electrical Installation

a) An isolator transformer (230/24 V, 230/48 V, or equivalent) shall be part of the delivery if any other voltage for monitoring and control than 230V (single-phase with Neutral) is used.

b) Special cables and conductors shall be part of the delivery.

c) Flexible wiring (e.g. cables or wires in tubes or conduits) with a voltage higher than 50 V shall contain an earthing wire. The outer sheath of tubes shall consist of an insulating synthetic material, whereas metallic tubes shall be equipped with an insulating spacer.

d) Mains connection of machines etc. shall be made by means of 3 cable clamps (within the Mains termination box) as follows:
  1 clamp for Phase (brown)
  1 clamp for Earth (yellow-green)
  1 clamp for Neutral (light blue)

e) All machines, etc.. and every separate wiring cabinet, pump etc.. shall further be provided with an external earthing contact.

f) Insulated wires, cables for monitoring and control circuits shall be clearly identified and separated from the mains (operative) circuits.

g) Insulated wires on metallic parts of the control panels shall be separated from this fixing point by an insulating underlayer to prevent mechanical damage to the wire.

h) The passage of wires, cables etc.. through metallic walls shall be by means of humidity resistant (mastic or other product) insulating lead-through materials.

i) The whole electrical installation shall be protected from accidental mechanical damage.

j) If the cable clamps are fixed within the case of the switchboard they shall be protected against human contact by means of an insulating material.

k) The termination box of an installation that is supplied from a low-voltage 3-phase mains shall contain five cable clamps which are marked with idents marked L1, L2, L3 (N, E).

l) Individual conductors of a 4-wire line shall have the following colors:
  3 phase conductors: black or brown or 3-phase conductor combination brown, black.
  1 earthing conductor: green-yellow striped

m) Individual conductors of a 5-wire line shall have the following colors:
  3 phase conductors: black or brown or grey or 3-phase conductor combination brown, black, grey.
  1 earthing conductor: green-yellow striped
  1 neutral conductor: light blue

n) The following colors are stipulated for bus-bars:
- Phase bars: orange with black strips, L1, L2, L3 - 1, 2 or 3 strips at one end of the track.
- Earthing bars: green-yellow stripped.
- Neutral bar: light blue.

o) The color of the wiring cables of the distribution cabinet shall be black.

p) Mandatory color for the indicator lamps (signal lamps).
- green indicator: station normal, non operational/shut-down
- white indicator: station in normal operation
- yellow indicator: warning - station in abnormal operation
- red indicator: dangerous or critical situation
- blue indicator: other signals or messages.

q) Mandatory colors of the control buttons:
- button for switch-on: green
- button for emergency switch-off: red
- button for switch-off: white

If the same button is used step by step for switch-on and off neither the green nor the red colors shall be used. In that case the black color is recommended.

2. General Technical and Qualitative Conditions

a) The complete delivery shall be made in accordance with metric units. The scales of any analogue measuring devices shall also be calibrated in the metric system (SI-system).

b) All machines and facilities or parts of them, which are not resistant to corrosion, shall be provided with one basic coat of paint and two protective coatings: the color shade will be agreed between the Contractor and the Customer later on.

c) All working surfaces shall have a protective coating. The information on a suitable means for removal of that coating shall be supplied two months before the unit assembly.

d) The safety-technical design of all machines shall be conform to Czech standards in principle.

e) All inscriptions on the machines and facilities shall be in the Czech or/and English language.

f) All lubrication points shall be marked with red color and shall correspond with the names in the lubrication plan.

g) Distributors, control cabinets and control elements (color of the indicator lights, control buttons, wires) shall correspond to STN 33 22 00 which is equivalent to the standard IEC 204-1-1981.

APPENDIX 2 SNMP AGENT REQUIREMENTS SPECIFICATION

1. Acronyms, abbreviations and definitions

ANS CR	Air Navigation Services of the Czech Republic
ASN.1	Abstract Syntax Notation is a standard and flexible notation that describes data structures for representing, encoding, transmitting, and decoding data. It provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques and is a precise, formal notation that removes ambiguities.
CADIN IP	Czech Aeronautical Data Interchange Network
CMOS	Central Monitoring System
MIB	Management Information Base. A schema, blueprint or roadmap of managed objects in a network.
OID	Object Identifier. In computer networking, an OID, in the context of the Simple Network Management Protocol (SNMP), consists of the object identifier for an object in a Management Information Base (MIB).
SNMP	Simple Network Management Protocol. A communications protocol specifically designed for the monitoring and control of computer networks.

2. System interface

For seamless integration into the CMOS system has to provide SNMP agent version 2C.

As a last resort, if the SNMP agent is not part of the system, the system must provide at least a suitable interface for external control and monitoring system, which should be suitable for creating the SNMP agent. This interface has to be fully documented.

3. Data organization

Data provided by the SNMP agent (its MIB base) must be detailed and adequately described (the best is to use ASN.1 language). Data in MIB agent base should be organized in the logical entities organized by parts of the system. Besides detail description of each subsystem, each part should be described by the scalar (not table) value in MIB database - so called status word. For example suitable could be enumerated type or bit-coded integer value.

Data in MIB base should reflect how the system is built and for each object should be selected as precise types of ASN.1 as possible. It is important to take into account that data in MIB base are used by machine and not by human and therefore each OID with unique and concise name indicate value directly.
If it is possible, it is preferred to keep following convention for the states of monitored variables / subsystem:

- 0 – Unknown
- 1 – OK
- 2 – Warning
- 3 – Alarm
- 4 – Purposely turn off (OK Off)

If any part of system fail or there are no information about it, failing branch should still exist in MIB and its values should be set to appropriate value respectively to unknown value.
In case of service reconfiguration of system should not be no changes of addresses (OID) for specific values.

The agent should be able to response on request SNMP GET and SNMP GETNEXT in accordance with appropriate documentation of SNMP protocol so, it would be possible to use utility snmpwalk or other application runs as MIB browser for obtaining data.

In case that sources data for CMOS (SNMP agents) are doubled (redundant systems), structure of MIB and values on specific OID should be the same on all redundant servers.

If the system contains more parts either identical or significantly similar it is suitable to represent data in MIB using the table. It is absolutely improper to unfold such table in to the scalar values.

The System must be connected directly or by some proxy part to data net CADIN/IP ANS CR.

4. System monitoring

If MIB base is well designed - system monitoring is sufficient only by pooling status word in MIB base in low frequency. Low frequency status word pooling is important to identify malfunctioning agent. The System CMOS is periodically requests state of values of the monitored system, which are returned in response. Frequency of request is for each system adjustable.

5. System control

Currently CMOS does not use SNMP interface for controlling. CitectSCADA software, which is based and developed on CMOS, does support controlling by SNMP. Controlling system by SNMP agent is absolutely necessary only in case that system does not have its own remote for detail controlling.

6. SNMP agent configuration

The SNMP agent detailed configuration capability is the significant advantage. Part of configuration must be security set-up, especially in case when the agent allows the control. Besides that the part of the configuration should be parameters like agent reaction times, login parameters, etc. The same requirements shall be applied for proprietary system interface, when system does not have SNMP agent.

7. Activities logging

SNMP agent should be capable of the recording of its own activity and data flows if so configured. The same applies for data flow on proprietary interface when the SNMP agent is not a part of the system. The information recorded this way makes integration in the CMOS system easier and also are useful to trace responsibility when the system functionality is broken.