

# 

##### 

**A&E Specifications**

ZIPS-H - 1023321311

# GENERAL

## SYSTEM DESCRIPTION

### General Requirements

#### The specified unit shall be of manufacturer’s official product line, designed for commercial and/or industrial 24/7/365 use.

#### The specified unit shall be based upon standard components and proven technology using open and published protocols.

#### All installation, configuration, setup, program, and related work shall be performed by electronic technicians thoroughly trained by the manufacturer in the installation and service of the equipment provided.

#### All the security system components provided shall be backed by a two (2) year manufacturer warranty. The manufacturer shall provide warranty and optional extended warranty for the unit for a total period of maximum five (5) years. If stipulated as part of the contract, the Contractor shall repair or replace parts and/or labor per the warranty for the length of this warranty at no cost to the client.

## CERTIFICATIONS AND STANDARDS

### Sustainability:

#### Manufactured in accordance with ISO 14001.

#### Compliant with the EU directives 2011/65/EU (RoHS) and 2015/863/EU (WEEE).

#### Compliant with the EU regulation 1907/2006 (REACH).

### The specified unit shall meet the requirements of the following EU directives:

#### 2014/30/EU

#### 2014/53/EU

#### 2011/65/EU

### The specified unit shall meet the requirements of the following electrical product safety standards:

#### EN IEC 62368-1

### The specified unit shall meet the requirements of the following EMC standards:

#### EN 61000-6-1

#### EN 61000-6-2

#### EN 61000-6-3

#### EN 61000-6-4

### The specified unit shall meet the requirements of the following EMC classifications:

#### FCC Part15

### The specified unit shall meet the following standards:

#### Audio:

##### G.711

##### G.722 (wideband)

##### G.729

##### L16x48D

#### Network requirements:

##### IEEE 802.3 af (PoE)

##### IEEE 802.1x (Authentication)

##### IPv4 (RFC 791)

#### Mechanical Environment:

##### IEC/EN 60529 IP66

##### IEC/EN 62262 IK08

# PRODUCT

## Equipment

### Manufacturer: Zenitel Norway AS

Myrens Verksted 3A

0473 Oslo, Norway

Phone: +47 40 00 27 00

[www.zenitel.com](http://www.zenitel.com)

### Model: Zenitel IP Speaker – Horn, ZIPS-H. Item number: 1023321311

## GENERAL Requirements

### Speakers shall be IP-based and comply with established network and video standards.

### Speakers shall be powered by the switch utilizing the network cable.

### Speakers shall include a built-in web server and/or web interface.

## Speaker

### IP Speaker

#### The speaker shall meet or exceed the following performance specifications:

##### Audio

###### The speaker shall support half duplex audio - PTT:

Internal microphone (Speaker-as-Mic)

30 W Output Power

Line out to secondary speaker (8 Ohm)

Line in for secondary microphone

###### The speaker shall support automatic volume control, AVC.

###### The speaker shall support automatic gain control, AGC.

###### The speaker shall provide a continuous sound pressure level (SPL) of 115 dBA (6dB Crest factor)

###### The speaker shall provide a maximum sound pressure level (SPL) of 120 dBA @ 1kHz/1m

###### The speaker shall provide a frequency range (G.722 Codec) of 275 Hz – 7000 Hz

###### The speaker shall provide 7.5W continuous output power

###### The speaker shall provide 30W peak output power

###### The speaker shall be equipped with Speaker as Microphone technology

##### User Interface

###### Web Server

The speaker shall contain a built-in web server making functionality and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.

###### IP addresses

The speaker shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.

The speaker shall allow for automatic detection of the intercom based on WS Discovery when using a computer with an operating system supporting this feature.

The speaker shall provide support for IPv4.

The speaker shall speak the IP address after system boot (requires connected speaker)

##### Protocol

###### The speaker shall support at least IPv4 (with DiffServ), SIP, TCP, UDP, HTTPS, TFTP, RTP, DHCP, SNMP, Vingtor-Stentofon CCoIP®, NTP, ONVIF

##### Security

###### The speaker shall support the use of HTTPS and TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication administration data.

###### The speaker shall provide centralized certificate management, with the ability to upload CA certificates. The certificates shall be signed by an organization providing digital trust services.

###### The speaker shall support IEEE 802.1X authentication.

###### The speaker shall restrict access to the built-in web server by username and password. Length: 8 – max 32 characters, and at least 3 of the following 4: 1 Digit, 1 Capital letter, 1 Small letter, and 1 Special character (?!@$%\*,-).

##### API support

###### The speaker shall conform to ONVIF profile S as defined by the ONVIF Organization.

##### Networking and Protocols

###### The speaker shall support secure configuration using HTTPS.

###### The speaker shall support the use of SNMP-based management tools according to SNMP v2c and v3.

###### The speaker shall allow for software (firmware) updates over the network, using HTTP/ HTTPS or the web interface.

###### The speaker shall accept external time synchronization from an NTP (Network Time Protocol) server.

###### The speaker shall support back-up and restore of configuration.

###### The speaker shall store all customer-specific settings in a non-volatile memory that shall not be lost during power cuts or soft reset.

##### SNMP g. Event Log

###### The speaker shall have the capability to log all triggered events as part of a detailed event log.

###### The administrator shall be able to configure whether specific messages are sent immediately upon the occurrence of an event (e.g., as an SNMP Trap or ONVIF Event) or whether the operator subscribes to the event log and retrieves a comprehensive report of all logged events since the last subscription.

###### The operator shall be able to select which types of messages are to be reported from the event log.

##### Speaker Diagnostics

###### The speaker shall be monitored by a Watchdog functionality, which automatically re-initiates the processes or restart the unit if a malfunction is detected.

##### Hardware Interfaces

###### Network Interface

The speaker shall be equipped with one 10/100Mbps Ethernet-port, using a standard RJ45 connector and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).

###### Audio

The speaker shall be equipped with balanced 8 Ohm audio line output.

The speaker shall be equipped with secondary mic/line input.

The speaker shall be equipped a built-in Class D amplifier

###### Multifunctional connector

The speaker shall be equipped with 1 general purpose I/O~~s~~. TheI/O can be configured either as an input or 12mA LED driver output.

###### Relay

The speaker shall be fitted with a single throw relay with 16W switching power. COM, NO contacts. 48V nominal. Max: 100VDC, 70VAC (160 mA nominal).

##### Enclosure

###### The speaker shall:

Be designed for on-wall installations for indoor and outdoor use.

Be fitted with ASA encapsulation material.

Be fitted with a stainless-steel grade 304 U-shaped mounting bracket.

Have the dimensions 254mm / 10” (width) x 146mm / 5.75” (height) x 299mm / 11.77” (depth).

Be supplied with IP66 and IK08 protection.

##### Power supply

###### Power over Ethernet IEEE 802.3af standard, Class 3 (6.49 – 12.95 W)

##### Environmental

###### The speaker shall:

Operate in a temperature range of -40°C to +70°C / -40°F to 158°F.

Operate in a humidity range of < 95% (non-condensing).

# 3. EXECUTION

## 3.01 Installation

### The Contractor shall carefully follow the instructions included in the documentation provided by the manufacturer to ensure that all steps are taken to create a reliable and easy-to-operate system.

### All the equipment shall be tested and configured in accordance with the instructions provided by the manufacturer prior to installation.

### The firmware installed in the products shall always be the latest and most up-to-date version provided by the manufacturer.

### All the equipment that requires the users to log in using a password shall be configured with user/site-specific password/passwords. No system/product default passwords shall be allowed.