# 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.

### Sustainability

#### The specified unit shall be manufactured in accordance with ISO 14001.

#### The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).

#### The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).

## CERTIFICATIONS AND STANDARDS

### General abbreviations and acronyms

#### AES: Advanced Encryption Standard

#### API: Application Programming Interface

#### Bit Rate: The number of bits/time unit sent over a network

#### DHCP: Dynamic Host Configuration Protocol

#### DNS: Domain Name System

#### FPS: Frames per Second

#### FTP: File Transfer Protocol

#### H.264 (Video Compression Format)

#### IEEE 802.1x: Authentication framework for network devices

#### IP: Internet Protocol

#### IR light: Infrared light

#### ISO: International Standards Organization

#### JPEG: Joint Photographic Experts Group (image format)

#### LAN: Local Area Network

#### LED: Light Emitting Diode

#### MPEG: Moving Picture Experts Group

#### Multicast: Communication between a single sender and multiple receivers on a network

#### NTP: Network Time Protocol

#### ONVIF: Global standard for the interface of IP-based physical security products

#### PACS: Physical Access Control System

#### PoE: Power over Ethernet (IEEE 802.3af/at) standard for providing power over network cable

#### Progressive scan: An image scanning technology which scans the entire picture

#### QoS: Quality of Service

#### RPC: Remote Procedure Call

#### SIP: Session Initiation Protocol

#### SMTP: Simple Mail Transfer Protocol

#### SNMP: Simple Network Management Protocol

#### SSL: Secure Sockets Layer

#### TCP: Transmission Control Protocol

#### TLS: Transport Layer Security

#### Unicast: Communication between a single sender and single receiver on a network

#### UPS: Uninterruptible Power Supply

#### VBR: Variable Bit Rate

#### VMS: Video Management System

#### WDR: Wide dynamic range

### The specified unit shall carry the following EMC approvals:

#### EN55032: 2015

#### EN55024: 2010

#### 2014/35/EU

#### 2014/30/EU

#### 2012/19/EU

#### 2011/65/EU

#### EN 55032 Class A

#### EN 55032 Class B

#### EN 55024

#### FCC Part 15 - Subpart B Class A

#### FCC Part 15 - Subpart B Class B

#### FCC Part 15 - Subpart B Class A + B

#### ICES-003 Class A

#### ICES-003 Class B

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

#### IEC/EN/UL 60950-1

### The specified unit shall meet the following standards

#### Audio:

##### G.711

##### G.729

##### G.722 (wideband)

##### L16 / 16kHz (wideband)

#### Video:

##### H.263+

##### H.263

##### H.264 (MPEG-4 AVC)

##### MPEG-4 Part 2

##### MJPEG

####

#### Networking:

##### IEEE 802.3af/802.3at (Power over Ethernet) [applies to products with PoE]

##### IEEE 802.1X (Authentication)

##### IPv4 (RFC 791)

##### QoS

#### Mechanical Environment:

##### EN90529 IP69K

##### IEC/EN 62262 IK10

## QUALITY ASSURANCE

### The Contractor or security sub-contractor shall be a licensed security Contractor with a minimum of five (5) years’ experience installing and servicing systems of similar scope and complexity and evidence that is completed at least three (3) projects of similar design and is currently engaged in the installation and maintenance of systems herein described.

### 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.

### The contractor or designated sub-contractor shall submit credentials of completed manufacturer certification, verified by a third-party organization, as proof of the knowledge.

### The Contractor shall provide four (4) current references from clients with systems of similar scope and complexity that became operational in the past three (3) years. At least three (3) of the references shall be utilizing the same system components, in a similar configuration as the proposed system

### The specified unit shall be manufactured in accordance with ISO9001.

## WARRANTY

### All security system components and labor furnished by the contractor including wiring, software, hardware and custom parts shall be fully warranted for parts, materials, labor and travel expenses for a minimum of three (3) years.

### The manufacturer shall provide warranty and optional extended warranty for the unit for a total period of maximum five years. If enacted as part of the contract, the contractor will repair or replace parts and/or labor per the warranty for the length of this warranty at no cost to the client.

# PRODUCTS

## General

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

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

### Intercoms shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.

## Intercom schedule

### Intercom types listed below describing various resolutions, form-factor and features shall be supplied by a single intercom manufacturer.

### The intercom manufacture and model numbers will be as follows:

#### IP intercom shall be 2N IP Force with one button and HD camera.

#### IP intercom shall be 2N IP Force with one button.

#### IP intercom shall be 2N IP Force with one button and keypad.

#### IP intercom shall be 2N IP Force with two buttons.

#### Modular IP intercom shall be 2N IP Force with camera.

#### IP intercom shall be 2N IP Force with four buttons.

#### IP intercom shall be 2N IP Force with four buttons and HD camera.

## Intercom

### IP intercom

#### The intercom shall meet or exceed the following design specifications:

##### The intercom shall include a built-in web server.

##### The intercom shall be able to perform defined local access control functionality without being connected to the network.

##### The intercom shall be of rugged design for tough outdoor environments.

##### The intercom shall be equipped with a HD camera utilizing an IR-sensitive progressive scan megapixel sensor and be able to provide images also under dark conditions.

##### The camera shall provide an automatic IR-cut filter, providing day/night functionality.

##### The intercom shall be equipped with built-in power adaptive IR-illumination/LED.

##### The intercom shall be equipped with one push button with embedded backlight and replaceable labels for call-up functionality.

##### The intercom shall be equipped with numeric keypad with separated keys with backlight.

##### The intercom shall support the option to add embedded RFID reader functionality.

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

##### Video

###### The intercom shall provide video streams in 640x480 at up to 30 frames per second using H.264, H.263, H.263+ or up to 15 frames per second using MJPEG.

###### The intercom camera shall provide images in resolutions up to 1280x960.

###### The intercom shall support the following video encoding algorithms:

H.263+

H.263

H.264

MPEG-4 Part 2

MJPEG

###### The intercom shall provide independently configured simultaneous H.264 and MJPEG streams.

###### The intercom shall in H.263, H.263, H.264 support Constant Bit Rate (CBR) to protect the network from unexpected bit rate peaks.

###### The intercom shall provide configurable compression levels.

###### Support standard baseline profile H.264 with motion estimation.

###### Support motion estimation in H.264/MPEG-4 Part 10/AVC.

###### The intercom shall allow for video to be transported over:

HTTP (Unicast)

HTTPS (Unicast)

RTP (Unicast & Multicast)

RTP over RTSP (Unicast)

RTP over RTSP over HTTP (Unicast)

###### The intercom shall support Quality of Service (QoS) to be able to prioritize traffic.

##### Image

###### The camera shall incorporate automatic white balance.

###### The camera shall support manually defined values for:

Color level

Brightness

##### Audio

###### The intercom shall support two-way full duplex audio:

Input sources

Two internal microphones

 Output sources

Built-in speaker, 10W

Line out

###### The intercom shall support separately adjustable volume levels for:

Call

Key

Ring tones

Preloaded audio clips

Warning tones

Paging

###### The intercom shall support adaptive gain control.

###### Encoding

The intercom shall support:

G.711

G.722 (wideband)

G.729

L16 / 16kHz (wideband)

###### The intercom shall provide a sound pressure level of at least 94dB at 1kHz at 1m.

###### The intercom shall be equipped with active echo cancellation.

###### The intercom shall allow for audio to be transported over:

RTP (Unicast & Multicast)

RTP over RTSP (Unicast)

RTP over RTSP over HTTP (Unicast)

###### The intercom shall support Quality of Service (QoS) to be able to prioritize traffic.

##### Call functionality

###### The intercom shall support SIP for integration with VoIP, peer-to-peer or integrated into SIP/PBX.

###### The intercom shall support the use of SIP Proxy, which can be the same as the SIP registrar for outgoing calls.

###### The intercom shall support dialing up to twelve separate numbers in sequence or as ring group.

##### Access control functionality

###### The intercoms’ outputs shall support remote control using DTMF codes.

###### Each user shall have unique access codes for each electrical output.

##### User Interface

###### Web server

The intercom 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.

###### Language Specification

The intercom shall provide a function for altering the language of the user interface, and shall include support for at least 7 different languages and include an ability to support an additional language through customization.

###### IP addresses

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

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

The intercom shall provide support IPv4.

##### Event functionality

###### The intercom shall be equipped with an integrated event functionality, which can be trigged by:

Tamper / case open

SIP Call state incl. incoming call

Change of SIP registration status

Video Motion Detection

Noise Detection

SIP DTMF sequences

External input

Access control events such as code, card, fingerprint entered

Predefined time

###### Response to triggers shall include:

Send notification, using HTTP or email

Activate sound alarm

Make or end call

Send notification, using HTTP, HTTPS, Wiegand or email

Send images, using FTP or email

Activating external output

Play audio clip

##### Protocol

###### The intercom shall incorporate support for at least HTTP, HTTPS, SIP 2.0, TFTP, RTSP, RTP, SMTP, DHCP opt 66, NTP, Syslog.

###### The SMTP implementation shall include support for SMTP authentication.

###### The intercom shall incorporate support for at least IPv4, HTTP, HTTPS, SIP, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv2c, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, ARP, DNS, NTP,

##### Security

###### The intercom shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data, video and audio streams.

###### The intercom shall block its login page for 30 seconds after three faulty passwords has been submitted.

###### The intercom shall force user to change admin password upon first installation.

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

###### Selected services, such as RTSP or web config shall be configurable to only allow access from local devices.

###### The intercom shall restrict access to the built-in web server by username and password.

###### The intercom shall be equipped with tamper detection.

##### API support

###### The intercom shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.

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

###### The intercom shall be interoperable/certified with major PBX and gateway manufacturers, including:

Cisco

Avaya

Broadsoft

##### Installation and maintenance

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

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

###### The intercom shall allow updates of the software (firmware) over the network, using TFTP, HTTP or web interface.

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

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

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

##### Access log

###### The intercom shall be able to log events such as codes, phone calls, and provide them using HTTP interface for monitoring.

###### The administrator shall be able to set whether the particular messages are sent by the intercom immediately after any event occurs, or if the client registers for event logging and then asks for full report since last registration, all events at once.

###### The client shall be able to select which messages are reported from event log.

##### Intercom diagnostics

###### The intercom shall be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the intercom’s operational status and provide information about power, the network status and the intercom status.

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

##### Hardware interfaces

###### Network interface

The intercom shall be equipped with one 10BASE-T/100BASE-TX Fast 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).

###### Doors

The intercom shall be equipped with two independent outputs for door control. One active providing at least 8VDC / 600mA and one NO/NC relay supporting up to 30V AC/DC 1A.

###### Audio

The intercom shall be equipped with line output.

###### Power

The intercom shall be equipped with a terminal block providing connectivity for external power.

##### Enclosure

###### The intercom shall:

Be manufactured with IP69K rated housing, and be IK10

Be fitted with a tamper switch.

Be of ruggedized construction.

Be available in black surface finish

##### Power

###### Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 0

###### 12 V DC

Max: 2A

##### Environmental

###### The intercom shall:

Operate in a temperature range of -40 °C to +55 °C (-40 °F to 131 °F)

Operate in a humidity range of 10–95% RH (non-condensing).

# execution

## installation

### The Contractor shall carefully follow instructions in documentation provided by the manufacturer to ensure all steps have been taken to provide a reliable, easy-to-operate system.

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

### All firmware found in products shall be the latest and most up-to-date provided by the manufacturer.

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

END OF SECTION