# PARTIE 1 GÉNÉRAL

## DESCRIPTION DU SYSTÈME

### Exigences générales

#### L'unité spécifiés doivent appartenir à la gamme de produits officielle du fabricant et être conçus pour une utilisation commerciale et/ou industrielle 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

#### L'unité spécifiée doit être basée sur des composants standard et une technologie éprouvée utilisant des protocoles ouverts et publiés.

### Durabilité

#### L'unité spécifiée doit être fabriquée conformément à la norme ISO 14001.

#### L'unité spécifiée doit être conforme aux directives européennes 2011/65/UE (RoHS) et 2012/19/UE (DEEE).

#### L'unité spécifiée doit être conforme au règlement 1907/2006 de l'UE (REACH).

## CERTIFICATIONS ET NORMES

### Abréviations et acronymes généraux

#### AES : Norme de cryptage avancée

#### API : Interface de programmation d'applications

#### Bit Rate : Le nombre de bits/unité de temps envoyés sur un réseau

#### DHCP : Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte)

#### DNS : Système de noms de domaine

#### SFP : Images par seconde

#### FTP : Protocole de transfert de fichiers

#### H.264 (format de compression vidéo)

#### IEEE 802.1x : Cadre d'authentification pour les appareils de réseau

#### IP : protocole Internet

#### IR : Lumière infrarouge

#### ISO : Organisation internationale de normalisation

#### JPEG : Groupe mixte d'experts en photographie (format image)

#### LAN : Réseau local

#### LED : Diode électroluminescente

#### MPEG : Groupe d'experts sur les images animées

#### Multicast : Communication entre un seul émetteur et plusieurs récepteurs sur un réseau

#### NTP : Network Time Protocol

#### ONVIF : Norme mondiale pour l'interface des produits de sécurité physique basés sur IP

#### PACS : Système de contrôle d'accès physique

#### PoE : Norme d'alimentation par Ethernet (IEEE 802.3af/at) pour l'alimentation par câble réseau

#### Analyse progressive : Une technologie de balayage d'image qui balaie l'ensemble de l'image

#### QoS : Qualité de service

#### RPC : Appel de procédure à distance

#### SIP : Protocole d'ouverture de session

#### SMTP : Simple Mail Transfer Protocol (protocole de transfert de courrier simple)

#### SNMP : Simple Network Management Protocol (protocole de gestion de réseau simple)

#### SSL : Secure Sockets Layer

#### TCP : Transmission Control Protocol (protocole de contrôle de transmission)

#### TLS : Sécurité de la couche transport

#### Unicast : Communication entre un seul émetteur et un seul récepteur sur un réseau

#### UPS : Alimentation électrique sans coupure

#### VBR : Débit binaire variable

#### VMS : Système de gestion vidéo

#### WDR : Large gamme dynamique

### L'unité spécifiés doivent porter les agréments CEM suivants :

#### EN55032 : 2015

#### EN55024 : 2010

#### 2014/35/UE

#### 2014/30/UE

#### 2012/19/UE

#### 2011/65/UE

#### EN 55032 Classe A

#### EN 55032 Classe B

#### EN 55024

#### FCC Partie 15 - Sous-partie B Classe A

#### FCC Partie 15 - Sous-partie B Classe B

#### FCC Partie 15 - Sous-partie B Classe A + B

#### ICES-003 Classe A

#### ICES-003 Classe B

### L'unité spécifiés doivent satisfaire aux normes de sécurité des produits suivantes :

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

### L'unité spécifiés doivent répondre aux normes suivantes

#### Audio :

##### G.711

##### G.729

##### G.722 (large bande)

##### L16 / 16kHz (large bande)

#### Mise en réseau :

##### IEEE 802.3af/802.3at (Power over Ethernet) [s'applique aux produits avec PoE]

##### IEEE 802.1X (Authentification)

##### IPv4 (RFC 791)

##### QoS

#### Environnement mécanique :

##### EN90529 IP69K

##### IEC/EN 62262 IK10

## ASSURANCE DE LA QUALITÉ

### Le contractant ou le sous-traitant en sécurité doit être un contractant en sécurité agréé ayant au moins cinq (5) ans d'expérience dans l'installation et l'entretien de systèmes de portée et de complexité similaires et justifier d'avoir réalisé au moins trois (3) projets de conception similaire et être actuellement chargé de l'installation et de la maintenance des systèmes décrits dans le présent document.

### Toutes les opérations d'installation, de configuration, de programmation et les travaux connexes doivent être effectués par des techniciens en électronique ayant reçu une formation approfondie du fabricant en ce qui concerne l'installation et l'entretien du matériel fourni.

### Le contractant ou le sous-traitant désigné doit présenter des attestations de certification du fabricant, vérifiées par un organisme tiers, comme preuve de ses connaissances.

### Le contractant doit fournir quatre (4) références actuelles de clients ayant des systèmes de portée et de complexité similaires, devenus opérationnels au cours des trois (3) dernières années. Au moins trois (3) de ces références doivent utiliser les mêmes composants du système, dans une configuration similaire à celle du système proposé

### L'unité spécifiés doivent être fabriqués conformément à la norme ISO9001.

## GARANTIE

### Tous les composants du système de sécurité et la main-d'œuvre fournis par le contractant, y compris le câblage, les logiciels, le matériel et les pièces sur mesure, sont entièrement garantis pour les pièces, les matériaux, la main-d'œuvre et les frais de déplacement pendant une période minimale de trois (3) ans.

### Le fabricant doit fournir une garantie et une extension de garantie facultative pour l'appareil pour une période totale de cinq ans maximum. S'il est adopté dans le cadre du contrat, l'entrepreneur réparera ou remplacera les pièces et/ou la main-d'œuvre selon la garantie pour la durée de cette garantie, sans frais pour le client.

# PARTIE 2 PRODUITS

## Général

### Les interphones doivent être basés sur l’IP et respecter les normes établies en matière de reseau.

### Les interphones sont alimentés par le commutateur utilisant le câble du réseau.

### Les interphones sont entièrement pris en charge par une API (Application Programmers Interface) ouverte et publiée, qui fournit les informations nécessaires à l'intégration de fonctionnalités dans des applications tierces.

## PROGRAMMATION DE L’INTERPHONE

### Les types d'interphones énumérés ci-dessous, qui décrivent diverses résolutions, facteurs de forme et caractéristiques, doivent être fournis par un seul fabricant d'interphones.

### Les numéros de fabrication et de modèle des interphones seront les suivants :

#### L'interphone IP doit être le 2N IP Safety avec un seul bouton.

#### L'interphone IP doit être le 2N IP Safety avec un bouton d'urgence.

#### L'interphone IP doit être le 2N IP Safety avec deux boutons.

## InterPHONE

### Interphone IP

#### L'interphone doit respecter ou dépasser les caractéristiques de conception suivantes :

##### L'interphone doit comporter un serveur web intégré.

##### L'interphone doit être de conception robuste pour les environnements extérieurs difficiles.

##### L'interphone doit être équipé d'un bouton-poussoir industriel étanche, en acier inoxydable et résistant au vandalisme, avec rétro-éclairage intégré pour la fonction d'appel.

##### L'interphone doit être équipé d'un bouton d'urgence rouge – à tête bombée.

##### L'interphone doit être équipé de deux boutons poussoirs industriels étanches, en acier inoxydable et résistants au vandalisme, portant les étiquettes "INFO" et "SOS" avec rétro-éclairage intégré pour la fonction d'appel.

#### L'interphone doit satisfaire ou dépasser les spécifications de performance suivantes :

##### Audio

###### L'interphone doit pouvoir supporter un son bidirectionnel en duplex intégral :

Sources d'entrée

Deux microphones internes

Sources de production

Haut-parleur intégré, 10W

Ligne de sortie

###### L'interphone doit pouvoir supporter des niveaux de volume réglables séparément pour :

Appel

Clé

Sonneries

Clips audio préchargés

Tonalités d'avertissement

Paging

###### L'interphone doit prendre en charge le contrôle de gain adaptatif.

###### Encodage

L'interphone doit prendre en charge :

G.711

G.722 (large bande)

G.729

L16 / 16kHz (large bande)

###### L'interphone doit fournir un niveau de pression acoustique d'au moins 94dB à 1kHz à 1m.

###### L'interphone doit être équipé d'une annulation active de l'écho.

###### L'interphone doit permettre le transport de l'audio :

RTP (Unicast & Multicast)

RTP sur RTSP (Unicast)

RTP sur RTSP sur HTTP (Unicast)

###### L'interphone doit prendre en charge la qualité de service (QoS) pour pouvoir donner la priorité au trafic.

##### Fonctionnalité des appels

###### L'interphone doit prendre en charge le SIP pour l'intégration avec le VoIP, le peer-to-peer ou intégré dans le SIP/PBX.

###### L'interphone doit permettre l'utilisation du SIP Proxy, qui peut être la même que le SIP Registrar pour les appels sortants.

###### L'interphone doit permettre de composer jusqu'à douze numéros séparés en séquence ou en groupe de sonneries.

##### Fonctionnalité de contrôle d'accès

###### Les sorties des interphones doivent pouvoir être commandées à distance à l'aide de codes DTMF.

###### Chaque utilisateur dispose d'un code d'accès unique pour chaque sortie électrique.

##### Interface utilisateur

###### Serveur web

L'interphone doit contenir un serveur web intégré rendant la fonctionnalité et la configuration disponibles à plusieurs clients dans un système d'exploitation et un environnement de navigation standard utilisant le protocole HTTP, sans qu'il soit nécessaire de recourir à un logiciel supplémentaire.

###### Spécification de la langue

L'interphone doit offrir une fonction permettant de modifier la langue de l'interface utilisateur, et doit pouvoir prendre en charge au moins 7 langues différentes et inclure la possibilité de prendre en charge une langue supplémentaire par le biais d'une personnalisation.

###### Adresses IP

L'interphone doit prendre en charge à la fois les adresses IP fixes et les adresses IP attribuées dynamiquement, fournies par un serveur DHCP (Dynamic Host Control Protocol).

L'interphone doit permettre une détection automatique de l'interphone basée sur WS Discovery lors de l'utilisation d'un ordinateur dont le système d'exploitation supporte cette fonction.

L'interphone doit fournir un support IPv4.

##### Fonctionnalité des événements

###### L'interphone doit être équipé d'une fonctionnalité intégrée d'événements, qui peut être déclenchée par

Falsification / dossier ouvert

État de l'appel SIP, y compris l'appel entrant

Changement du statut d'enregistrement du SIP

Détection du bruit

Séquences DTMF SIP

Entrée externe

Temps prédéfini

Pression sur les boutons

###### La réponse aux déclencheurs doit comprendre :

Envoyer une notification, en utilisant le protocole HTTP ou le courrier électronique

Activer l'alarme sonore

Passer ou terminer un appel

Envoyer une notification, en utilisant HTTP, HTTPS, Wiegand ou par courrier électronique

Activation de la production externe

Lire le clip audio

##### Protocole

###### L'interphone doit au moins prendre en charge HTTP, HTTPS, SIP 2.0, TFTP, RTSP, RTP, SMTP, DHCP opt 66, NTP, Syslog.

###### La mise en œuvre du SMTP doit inclure la prise en charge de l'authentification SMTP.

###### L'interphone doit prendre en charge au minimum les protocoles IPv4, HTTP, HTTPS, SIP, SSL/TLS, QoS Layer 3 DiffServ, TCP, ICMP, SNMPv2c, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, ARP, DNS, NTP,

##### Sécurité

###### L'interphone doit permettre l'utilisation des protocoles HTTPS et SSL/TLS, en offrant la possibilité de télécharger des certificats signés pour crypter et sécuriser l'authentification et la communication des données administratives et des flux audio.

###### L'interphone bloque sa page de connexion pendant 30 secondes après que trois mots de passe erronés aient été soumis.

###### L'interphone oblige l'utilisateur à changer le mot de passe admin par défaut lors de la première installation.

###### L'interphone doit permettre une gestion centralisée des certificats, avec la possibilité de télécharger les certificats de l'AC. Les certificats doivent être signés par une organisation fournissant des services de confiance numériques.

###### L'interphone doit prendre en charge l'authentification IEEE 802.1X.

###### Certains services, tels que le RTSP ou la configuration web, doivent être configurables pour permettre l'accès uniquement à partir d'appareils locaux.

###### L'interphone doit restreindre l'accès au serveur web intégré par un nom d'utilisateur et un mot de passe.

###### L'interphone doit être équipé d'un système de détection de sabotage.

##### Support API

###### L'interphone est entièrement pris en charge par une API (Application Programmers Interface) ouverte et publiée, qui fournit les informations nécessaires à l'intégration de fonctionnalités dans des applications tierces.

###### L'interphone doit être conforme au profil S de l'ONVIF tel que défini par l'Organisme ONVIF.

###### L'interphone doit être interopérable/certifié avec les principaux fabricants de PBX et de passerelles, y compris :

Cisco

Avaya

Broadsoft

##### Installation et maintenance

###### L'interphone doit permettre une configuration sécurisée utilisant le HTTPS.

###### L'interphone doit permettre l'utilisation d'outils de gestion basés sur le SNMP conformément au SNMP v2c.

###### L'interphone doit permettre la mise à jour du logiciel (micrologiciel) sur le réseau, en utilisant le protocole TFTP, HTTP ou une interface web.

###### L'interphone doit accepter la synchronisation temporelle externe à partir d'un serveur NTP (Network Time Protocol).

###### L'interphone doit permettre la sauvegarde et la restauration de la configuration.

###### L'interphone doit stocker tous les réglages spécifiques au client dans une mémoire non volatile qui ne doit pas être perdue en cas de coupure de courant ou de réinitialisation.

##### Journal d'accès

###### L'interphone doit pouvoir enregistrer des événements tels que des codes, des appels téléphoniques, et les fournir en utilisant une interface HTTP pour la surveillance.

###### L'administrateur doit pouvoir déterminer si les messages particuliers sont envoyés par l'interphone immédiatement après qu'un événement se soit produit, ou si le client s'inscrit pour l'enregistrement d'événements et demande ensuite un rapport complet depuis la dernière inscription, tous les événements à la fois.

###### Le client doit pouvoir sélectionner les messages qui sont signalés dans le journal des événements.

##### Diagnostic des interphones

###### L'interphone doit être équipé de LED, capables de fournir des informations d'état visibles. Les LED doivent indiquer l'état de fonctionnement de l'interphone et fournir des informations sur l'alimentation, l'état du réseau et l'état de l'interphone.

###### L'interphone est surveillé par une fonction Watchdog, qui réinitialise automatiquement les processus ou redémarre l'appareil si un dysfonctionnement est détecté.

##### Interfaces matérielles

###### Interface réseau

L'interphone doit être équipé d'un port 10BASE-T/100BASE-TX Fast Ethernet, utilisant un connecteur RJ45 standard et doit supporter l'auto-négociation de la vitesse du réseau (100 MBit/s et 10 MBit/s) et du mode de transfert (full et half duplex).

###### Portes

L'interphone doit être équipé de deux sorties indépendantes pour la commande de la porte. Une active fournissant au moins 8VDC / 600mA et un relais NO/NC supportant jusqu'à 30V AC/DC 1A.

###### Audio

L'interphone doit être équipé d'une sortie de ligne .

###### Alimentation

L'interphone doit être équipé d'un bornier permettant la connexion d'une alimentation externe.

##### Pièce jointe

###### L'interphone doit :

Être fabriqué avec un boîtier classé IP69K et être certifié IK10

Être équipé d'un interrupteur d'autoprotection.

Être de construction robuste.

Être disponible en finition de surface orange RAL 2004

##### Alimentation

###### Alimentation par Ethernet IEEE 802.3af/802.3at Type 1 Classe 0

###### 12 V DC

Max : 2A

##### Environnement

###### L'interphone doit :

Fonctionner dans une plage de température de -40° C à +55° C (-40° F à 131° F)

Fonctionner dans une plage d'humidité de 10 à 95 % HR (sans condensation).

# PARTIE 3 exécution

## installation

### Le contractant doit suivre attentivement les instructions figurant dans la documentation fournie par le fabricant afin de s'assurer que toutes les mesures ont été prises pour fournir un système fiable et facile à utiliser.

### Tous les équipements doivent être testés et configurés conformément aux instructions fournies par le fabricant avant leur installation.

### Tous les microprogrammes présents dans les produits doivent être les plus récents et les plus à jour fournis par le fabricant.

### Tous les équipements nécessitant que les utilisateurs se connectent à l'aide d'un mot de passe et doivent être configurés avec des mots de passe spécifiques à l'utilisateur/au site. Aucun mot de passe par défaut pour le système/produit ne doit être autorisé.

FIN DE SECTION