K105165/02
Process certificate

CERTIFICATE

Issued	*15-12-2021*
Replaces	*K105165/01*
Page	*1 of 6*

Wireless Silent Alarm Systems

STATEMENT BY KIWA
Based on pre-certification tests as well as periodic inspections by Kiwa, the products referred to in this certificate and marked with the Kiwa-mark as indicated under 'Marking', supplied by

MultiBel B.V.

may, on delivery, be relied upon to comply with the Kiwa certification scheme K21047/02 dated. June 10th, 2020 “Wireless Silent Alarm Systems”.
☒ System Provider
☐ Installation & Maintenance Provider

Ron Scheepers
Kiwa

Publication of this certificate is allowed.
Advice: consult www.kiwa.nl or www.kiwafss.nl in order to ensure that this certificate is still valid.

294171015

Kiwa Nederland B.V.
Fire Safety & Security Certification
Dwarsweg 10
5301 KT Zaltbommel
The Netherlands
Tel. +31 88 9985100
www.kiwa.com

WSAS System Provider
MultiBel B.V.
Veemarktkade 8
5222 AE 's-Hertogenbosch
Netherlands
Tel. +31 88 141 0300
E-mail info@multibel.nl
www.multibel.eu

Network
According to certification scheme K21030 (EN 50136-1/A1) with 2 data centres in the Netherlands

Certification process consists of initial and at minimum yearly inspection of:
- **quality system**
- **processes**
- **technical requirements**

TECHNICAL SPECIFICATION

General specification of the process
This certificate confirms the compliance of the processes and services and its enabling chain of entities to the requirements in the certification scheme K21047 "Wireless Silent Alarm Systems".
These requirements include a general level of safety, security and prevalent stipulations for the connections of the entities, access mechanisms of the involved entities, accessory mobile application and accompanying development and functional peripherals, setting alteration management, uptime – availability -business continuity, authenticity, accountability, time restrictions, processes and quality systems and processes of the manufacturer.

The basic framework for this scheme has been standard NEN 2575-4; Fire safety of buildings - Evacuation alarm installations - System and quality requirements and guidelines for locating of alarm devices - Part 4: Wireless silent alarm installation.
The framework in this scheme is covering all the functions and performances requirements of standard NEN 2575-4 based on international reference standards such as EN 50136-1/A1 / IEC 60839-5-1, EN 50131-1, ISO/IEC 11770-1/2/3, ISO/IEC 18033 & ISO/IEC 29115. Additionally are the requirements on logging, reporting, uptime, alarm transmission and software control more strict. It also has an additional function on positioning and counting of staff in the designated areas and in the surrounding of the designated areas.

Process specification and demarcation

Demarcation within scope
The wireless silent alarm system WSAS is intended to be used in buildings and/or on sites to relay the information of the fire detection and fire alarm system (FDFAS) in a building and/or on a site to for example the emergency response team (ERT) of the building and/or site. The WSAS can be used in a hosted situation.
The goal of the product is to inform and alarm the emergency response team in the building and/or site in a timely and secured way of the status of the fire detection system or other alarm systems. In that way, the users of mobile devices such as emergency response officers (ERO) at a location are able to start the emergency response and/or evacuation process. The reliability and availability of the system is essential.
The following elements in the demarcation are within scope:

- The Control and Indicating Equipment (CIE) of the Wireless Silent Alarm System;
- The critical alarm transmission between the Control and Indicating Equipment (CIE) of the fire detection system and the CIE of the WSAS;
- The critical connection to the power supply for the WSAS;
- The critical alarm transmission between the central equipment of the WSAS and the server in the secure location.
- The critical alarm transmission between the server in the secure location and the mobile devices (MD).
- The application performing on the mobile device with its functions to support the users on site.
- The positioning function of the WSAS for determining the number of present mobile device users.

Additionally, the critical transmission between the server in the secure location and the Monitoring Centre (MC) is in scope for at least the reporting of the faults of the WSAS.

Functions of the WSAS
The functions of the WSAS are:

- Supervised alarm transmission of the fire detection system and the mobile devices of the emergency response team at the location;
- Informing of the WSAS-user about faults in the system;
- Reporting on the availability of the system;
- Reporting on the availability of the connected number of emergency response officers within the designated area of the emergency response team;
- Optional: Reporting on the availability of the connected number of emergency response officers off site.

System requirements
The supervised alarm transmission between the central equipment of the WSAS and the server in the secure location have to comply with the requirements in EN 50136-1/A1 / IEC 60839-5-1; Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements; based on certification scheme K21030 for the scope critical transmission.
The level of the secure alarm transmission is Dual Path 4 (DP 4). See EN 50136-1/A1.
The supervised alarm transmission between the mobile devices of the WSAS and the server in the secure location have to comply with the requirements in EN 50136-1/A1 / IEC 60839-5-1; Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements;

The level of the secure alarm transmission is Dual Path 2 (DP 2) or Single Path 3 (SP 3) see EN 50136-1/A1.
The reporting is accessible for the user of the system and inspection bodies.
Remark: The possible radio transmission bands are 2G, 3G, 4G, 5G and Wi-Fi. SMS can be used as transmission layer.
SMS is only used as a backup when data transmission is not available.
The capacity of the used network shall be such that it has sufficient capacity in a normal and in an incident situation to interact with all the users.
The positioning function (GPS) of the WSAS per mobile device user has to meet the following specifics:
• In the building and/or site are devices (such as Wi-Fi transmitters) needed to facilitate the communication of the system of the users of the emergency response team.
• Accuracy positioning on a surface level: this has to be specified by the supplier, it needs to have a minimal accuracy of 100 meter and be determined using at least two methods of location positioning. In case of inaccurate Wi-Fi and GPS positioning there needs to be a manual input for users. The positioning function has a relation with alarm zone in the basic design of the WSAS.
• A designing and verification function tool for the determination of the number of local devices for the position function per building / floor and the verification of the function when installed. The basic criteria for this tool are accuracy positioning, adequate speed of transmission and adequate availability of transmission.
Note: The positioning function to be used off site is the same as on site.

Loggings of the system
According to EN 50136-1 / IEC 60839-5-1 loggings are made of the functions of all the devices within the system. The system shall have a capacity of at least 3 months to store this data.

CIE WSAS
The wireless silent alarm system must have an operating possibility (control panel) which, in case of fire or other emergency, can call silent alarm groups manually.

Server WSAS– system requirements
All transmission paths of wireless silent alarm systems are intended for use by wireless silent alarm systems. Secondary application transmission pathways for wireless alarm systems must not have a negative influence on the primary purpose of the transmission paths for wireless silent alarm.
The equipment shall be a stand-alone application for alarm handling. The software application changes may only be made by trained and authorized personnel for this equipment.
The equipment shall handle a fire / evacuation alarm with the highest priority.
Note: the server of the WSAS can be at a premises (non-hosted) or at a secure location (hosted).

Building / site transmission devices supporting the WSAS
The local transmission devices supporting the WSAS shall provide sufficient coverage for the evacuation area. In case of failure in transmission, the reception of messages in an area may not become below the level of availability of the WSAS per week and year (based on EN 50136-1/A1) and being monitored for proper functioning and shall be controlled and indicated by the software tool of the WSAS.
The instruction of the WSAS shall specify that the local transmission devices for supporting of the WSAS shall:
- be suitable for the location where it is set up;
- comply with telecommunication legislation that applies to it.
The specifications for the building network are:
• GPS location of a smartphone must be accurate to at least 100 meter;
• Wi-Fi connection speed must be at least 40 Mbps, and must have a signal strength of at least -67 dBm;
• 4G signal strength should be at least -58 dBm;
• GPRS signal strength should be at least -50 dBm.

Mobile devices supporting the WSAS
The business continuity strategy of the WSAS is such that regular mobile devices can be used supporting the functioning of the WSAS. By enforcing this strategy on a location, the possibility is created that all staff from the organisation using the WSAS present on the designated location can use their regular mobile device obtaining a high percentage of users.
This high percentage of users creates the ability to have a more direct action of the emergency response team based on the emergency response plan for the location and a higher business continuity for the WSAS.
Note: If needed within the infrastructure of the building and/or site, dedicated WSAS devices can be used. This has to stipulated within the basic engineering WSAS - plan of the building / site.
Note: Due to obtaining a proper Confidentiality, Integrity and Availability (CIA) level in terms of information security, BYOD solutions in this WSAS infrastructure are not permitted.

Preconditions of mobile devices
The mobile devices have to been set in the following preconditions by the software tool of the WSAS on the device:

- the audible alarm signal on the receiving mobile device must be at least 65 dB (A) at 1 m and must be clearly distinguishable from other call signals. Is the sound pressure level of the ambient noise 59 dB (A) or more, the receiving mobile device must also be clearly felt through a vibrating signal.
- the acoustic signal in the event of an alarm may not interrupt the voice communication;
- the acoustic signal from the receiving device must remain active during a silent alarm call until it is manually confirmed or up to a maximum of 60 seconds if it is not manually confirmed;
- a receiving mobile device must give a text message with at least the room/location that should be evacuated (for example the alarm zone or area);
- the language of the text message must be aligned with the emergency response & evacuation team and shall be recorded in the basic engineering plan of the WSAS for the building/site;
- the text messages relating to an evacuation alarm must have the highest priority, recognizable as such and clearly distinguishable from other messages;
- the receiving mobile devices give an acoustic and visual warning when the battery capacity is too low. This warning is made when the battery capacity reaches 10% of its maximal capacity. The warning does not have to be reported to the CIE of the WSAS;
- the receiving mobile devices cannot be switched off without an acoustic and/or optical warning;
- the receiving mobile device gives "information about availability within the defined zone", no later than 15 minutes when out of range with the WSAS if this is a control setting in the basic engineering plan based of the emergency response (evacuation) plan;
- the selection of the mobile device is such that the energy supply must be sufficient for at least 12 hours of operation. The supplier shall specify this in its instruction for the software tool.

Mobile application and hosted web platform
This part contains the requirements that the application on the mobile device, CIE WSAS and the hosted web platform shall have to fulfil.

Use and access levels of the application
The mobile application is intended to be used on general mobile smart devices.
The mobile application shall connect direct by radio transmission to the WSAS.
The application requires a logical access level 2 on the smart mobile device according to EN 50131-1. The application shall enforce a new code after first installation.
The CIE WSAS shall connect to the hosted web platform. This requires a logical access level 3 according to EN 50131-1.

Connections of the application
The applications shall have a secure and confidential connection to the CIE of the WSAS and meet the key management requirement of TLS1.2.
Key management shall be arranged according ISO/IEC 11770-1/2/3
The integrity of this connection shall be arranged on cryptographic algorithms according to ISO/IEC 18033. The hash functions according to this shall also be applied for non-repudiation.
The cryptographic algorithms shall meet the updated list of SSL labs or better.
The CIE of the WSAS shall have a secure connection to a hosted web platform according to IEC 60839-5-1 (EN 50136-1/A1).

Acknowledgment un/setting
The setting made on the CIE shall be acknowledged by the CIE of the WSAS and the hosted web platform. These settings shall also be communicated to the mobile devices.
The setting made in the hosted web platform shall be acknowledged by the CIE of the WSAS and the application of the mobile device. By this the live situation is reflected by the application.
The process shall be fail-safe; that means that if during normal use the connection fails, the process is stopped and that the not completed changed settings shall fall back to the last completed settings.

Uptime – availability – business continuity
The availability of the hosted web platform shall meet the requirements DP4 according to IEC 60839-5-1 (EN 50136-1/A1).
The hosted web platform shall be hosted from a secure location complying with EN 50518 or EN 50600.

Authenticity
The definitions and processes of ISO/IEC 29115 shall be applied.
LoA3 shall be defined in the process of getting first access (onboarding) as a user to all applications.
The mobile application shall restrict a limited time within 2 factor authentication process.
The procedure of getting access to the mobile application on the mobile device shall be the same as access to the CIE WSAS.
The procedure giving more users entrance (on different levels) to the mobile application is the same as for the CIE WSAS.
The process of remote access by the installer / supplier shall require at least 2 factor authentication.
It is allowed to use biometrics according to the standardisation group ISO/IEC JTC 1 SC 37 on Biometrics.

Accountability
The hosted web platform and the mobile application shall apply logging.
The minimum storing time of the logs for the hosted web platform and the mobile application is 3 months.

Session time
A maximum session time shall be applied preventing unauthorised use for critical function(s) within the mobile application. For example: opening the mobile application function for (setting) the CIE WSAS.
Protection against hostile access (brute force) to the mobile application within the secure functions shall be tested by penetration testing in the developing stage of the application.

Instructions by the application towards the user
The mobile application shall warn and instruct the user to use the mobile application in a secure manner.

Secure development process for the code
This part contains the requirements that the secure development process for the code of the mobile application and the hosted web platform shall have to fulfil.
Remark; An approved process according to scheme K21048 fulfils also this requirement.

Process requirements
The process shall fulfil the requirements of "A.14.2 Security in development and support processes" of ISO 27001 or the secure development processes according to IEC 62443-4-1; Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements. The manufacturer shall have an accredited certificate according to this standard for this activity or this process and it shall be assessed by an expert of Kiwa.

Process requirement stages
The secure development process shall contain at least the following stages:
1. Planning with project management;
2. Analyses of the epics, user stories, use cases;
3. Design with architecture & user experience;
4. Building the code by the developers;
5. Testing of the code; testing is continuous process for control and verification of the functions and the threats / weaknes ses of the security;
6. Deploying of the code in a hosted solution;
7. Review of the process for improvement of the next development.

Marking for this process

RECOMMENDATIONS FOR CUSTOMERS

Check at the time of delivery whether:

- the supplier has delivered in accordance with the agreement;
- the mark and the marking method are correct;
- the products, process and services show no defects as a result of the delivery process etc;

If you should reject a product based on the above, please contact:

- MultiBel B.V.

and, if necessary,

- Kiwa Nederland B.V.

Consult the supplier's Design, Installation & Operation Manual (DIOM) for the proper methods.
After installation of the wireless silent alarm system, inspection based on ISO17020 of the system in conjunction with the building / site and organisation operating this system is advised.
With this inspection is determined that the wireless silent alarm system and organisation operating this system in the building / on the site are in compliance with applicable health and safety regulations such as NEN 2575-4 and scheme K21047.