K21023/03
20200707

Mobile Security

for the certificate for Mobile Alarm Systems to protect vehicles, goods and persons

Trust
Quality
Progress

Preface

This European Certification Scheme has been accepted by the Kiwa Board of Experts Security, in which all the relevant parties in the field of Security are represented. This Board of Experts also supervises the certification activities and where necessary require the Certification Scheme to be revised. All references to Board of Experts in this Certification Scheme pertain to the above-mentioned Boards of Experts. This Certification Scheme will be used by Kiwa in conjunction with the Kiwa-Regulations for Certification, in which the general rules in case of certification are registered.

The purpose of this Certification Scheme is to clarify in which way a declaration of conformity is established regarding performance-, reliability- and security requirements of the assessed Mobile Alarm System (MAS). With this Mobile Alarm System vehicles, goods and persons can be protected. This certification scheme is based on the European standards in this field of application. This certification scheme reflects heavily to the standard EN 50518 and EN 50136-1/A1. This certification scheme arranges further the application of mobile security. For example the requirements of scope 1 have been established with the Dutch Police.

Kiwa Nederland B.V.
Kiwa Fire Safety & Security
Dwarsweg 10
5301 KT Zaltbommel
The Netherlands

Tel. +31 88 998 51 00
NL.info.ncp.fss@kiwa.com
www.kiwafss.nl

Validation
This certification scheme has been validated by the Director Certification and Inspection of Kiwa FSS on 7-7-2020.

5911810330

Contents

1 Introduction

1.1 General

This European certification scheme includes all relevant requirements which are employed by Kiwa when dealing with applications for the issue and maintenance of a certificate for products, (systems), processes and services used for mobile alarm systems.

For the performance of its certification work, Kiwa is bound to the requirements as included in EN-ISO/IEC 17065 “Conformity assessment - Requirements for bodies certifying products, processes and services”.

This certification scheme is drafted according EN-ISO/IEC 17067 “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes”. This scheme is a type 6 according to this standard.

This certification scheme replaces the following certification scheme:

Certification scheme	Title	Dated
K21023/02	Mobiele beveiliging - voor het Kiwa procescertificaat voor beveiliging mobiele objecten en personen	2016-10-03

This 3th version of the certification scheme translates the certification scheme in English to establish a broader applicability based on European Standards. The certification scheme can be used directly.

On 10-02-2021 an amendment for the scheme K21023 has been approved by the Board of Experts Security. The content of the amendment is the following table which replaces certain requirements. The scheme including amendment can be used directly.

Protection of persons K21023				
Scope	1	2	3	4
Risk level	High	Medium	Medium	Low
Configuration	GPS & ARC;	GPS & ARC;	ARC	N/A
Device	dedicated device	dedicated/smart device	dedicated/smart device	smart device
Paragraph	(paragraph 6.1)	(paragraph 6.2)	(paragraph 6.3)	(paragraph 6.4)
Internal GPS logging of the device	60 sec	90 sec	N/A	N/A
Data exchange (poll) frequency between device and server MAS	30 min and in event of an alarm	60 min and in event of an alarm	60 min and in event of an alarm	60 min and in event of an alarm
Intended usage	8-12 hours	8-12 hours	8-12 hours	N/A
Back-up transmission path	Obliged	N/A	N/A	N/A

Replace the text in paragraph 6.4: Touching the alarm activation function on the device (press and hold for at least 1.5 seconds to continue the alarm) or another activation mechanism with a low risk for false alarms).

With the following: Touching the alarm activating function on the personal alarm device shall activate the alarm

1.2 Field of application / scope

Figure 1 sets the demarcation of a mobile alarm system.

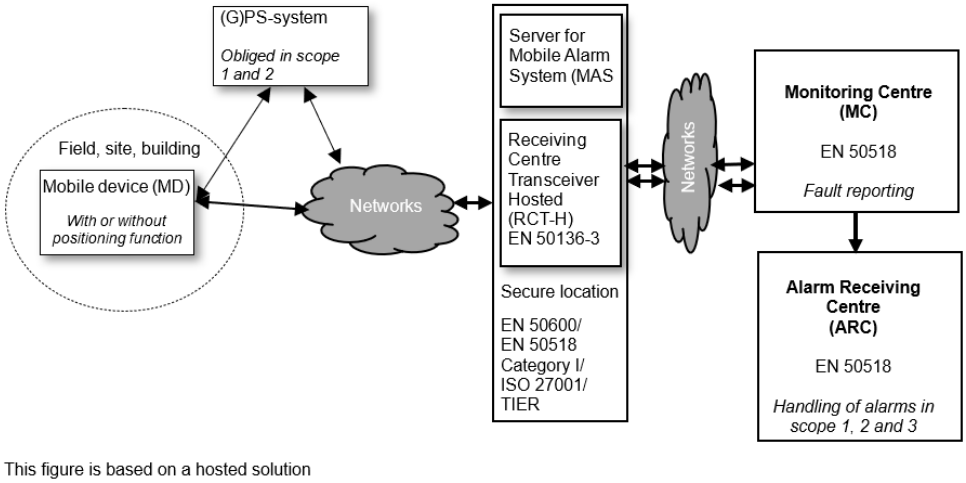


Figure 1 – infrastructure of the MAS

The goal of the product is to inform and alarm the (external) emergency organisation in a timely and secured way of the status of the good(s) or person(s) to be able to start the emergency process. The reliability and availability of the system is essential.

The product is intended to be used in the field, on sites and/or in appointed buildings as additional function to send information of the good(s) or person(s) in specific situations to the (external) emergency organisation if needed.
The infrastructure is the same for the protection of vehicles and goods and persons. The requirements for vehicles and goods (e.g. logistics) and persons are divided in separate chapters. For vehicles and goods many requirements are determined. That's why this certification scheme does not set extra requirements. The chapter about persons has a functional separation in four scopes.

The following elements of the infrastructure define the demarcation which are in scope:

- Server in the secure location;
- Mobile Device(s);
- The supervised alarm transmission between the server in the secure location and the mobile devices (MD) of the users;
- The application performing its functions on the mobile devices;
- The positioning function of the MD within the MAS.

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 faults. For the protection of vehicles and goods and the protection of persons in scope 1, 2 and 3 the connection the Alarm Receiving Centre is also in scope.

For more information regarding the transmission see certification scheme K21030 – Alarm Transmission Service Providers.

1.3 Functions of the MAS

The functions of the MAS are:

- Supervised alarm transmission between the mobile devices and the server of the MAS;
- Informing the user of the MAS about faults in the system;
- Reporting about the availability of the system;
- Reporting about the availability of the connected number of MD's.

1.4 Technical and organizational resources

To achieve certification of a wireless silent alarm system, the assessment contains the following:

- The adoption of the demarcation and the specifications of the MAS;
- The requirements of the product quality of relevant components;
- The requirements of the network architecture;
- The field inspection of the performance- & other requirements of the MAS;
- The requirements of the security controls of the MAS;
- The assessment of the statistical data which is generated by the hardware and software of the MAS;
- The requirements of the Monitoring & Alarm Receiving Centre who collects the data and processes this according to the specifications of the MAS;
- The requirements of the corrective actions by the MAS on failing communication by the system.
- The requirements of the Alarm and Receiving Centre which handles the alarms.

1.5 Acceptance of test reports provided by the supplier

If the supplier provides reports from test institutions or laboratories to prove that the products meet the requirements of this evaluation guideline, the supplier shall prove that these reports have been drawn up by an institution that complies with the applicable accreditation standards, namely:

- NEN-EN-ISO/IEC 17020 for inspection bodies;
- NEN-EN-ISO/IEC 17021-1 for certification bodies certifying systems;
- NEN-EN-ISO/IEC 17024 for certification bodies certifying persons;
- NEN-EN-ISO/IEC 17025 for laboratories;
- NEN-EN-ISO/IEC 17065 for certification bodies certifying products.

Remark:
This requirement is considered to be fulfilled when a certificate of accreditation can be shown, issued either by the Board of Accreditation (RvA) or by one of the institutions with which an agreement of mutual acceptance has been concluded by the RvA. The accreditation shall refer to the examinations as required in this evaluation guideline. When no certificate of accreditation can be shown, Kiwa shall verify whether the accreditation standard is fulfilled.

1.6 Quality declaration

The quality declaration to be issued by Kiwa is described as a:

- process certificate for the services for the delivery of maintenance of these systems.

A model of these certificate to be issued based on this scheme has been included for information as an annex.

1.7 Assessment method type 6

The normal assessment method per installation of this certification scheme is according to EN-ISO/IEC 17067 “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes” type 6.

2 Terms and definitions

2.1 Definitions general

In this evaluation guideline, the following terms and definitions apply:

2.1.1 Board of Experts:

the Board of Experts Security

2.1.2 Certification scheme:

the agreements made within the Board of Experts on the subject of certification.

2.1.3 Inspection tests:

tests carried out after the certificate has been granted in order to ascertain whether the certified products continue to meet the requirements recorded in the certification scheme.

2.1.4 IQC scheme (IQCS):

a description of the quality inspections carried out by the supplier as part of his quality system.

2.1.5 Initial assessment:

assessment in order to ascertain that all the requirements recorded in the certification scheme are met.

2.1.6 Process certificate:

a document in which Kiwa declares that a process may, on delivery, be deemed to comply with the process specification recorded in the process certificate.

2.1.7 Process requirements:

requirements made specific by means of measures or figures, focussing on (identifiable) characteristics of processes and containing a limiting value to be achieved, which can be calculated or measured in an unequivocal manner

2.1.8 Certification mark:

a protected trademark of which the authorization of the use is granted by Kiwa, to the supplier whose products can be considered to comply on delivery with the applicable requirements and possibly with quality information on the application of the product is added by a specially designed label which is based on the result , as stated in the report issued by Kiwa on the inspection of the prototype

2.1.9 Supplier:

the party that is responsible for ensuring that the products meet and continue to meet the requirements on which the certification is based.

2.2 Specific definitions

In this certification scheme, the following specific terms and definitions apply

2.2.1 Server Mobile Alarm System:

Server in a secure location which is the heart of the Mobile Alarm System. This server processes, controls and reports on the Mobile Alarm system.

2.2.2 Conditions:

For the function of a MAS are certain conditions needed. These conditions can be for example enabling a connection between the MD to the positioning function and the MAS itself.

2.2.3 Mobile Alarm System (MAS)

System to inform and alarm the (external) emergency organisation in a timely and secured way of the status of the good(s) or person(s) to be able to start the emergency process.

2.2.4 Mobile Device (MD)

Device with a positioning function to be used in a Mobile Alarm System. The mobile devices are split into track and trace devices for the protection of vehicles and goods and personal alarm devices for the protection of persons.

2.2.5 Track and trace device

Mobile device to be used in the protection of vehicles and goods.

2.2.6 Personal alarm device

Name for mobile devices which could be either a dedicated mobile device or a smart device used for protection of persons. The applicable scope determines which devices shall be used.

2.2.7 Dedicated mobile alarm device

Mobile device which is used in the scopes of protection of persons. These devices shall be used when a higher security and / or safety level is needed by the end user. These devices shall be used in scope 1

2.2.8 Smart mobile alarm device

Mobile device used in protection of persons as smart mobile device (smart phone) with a positioning function to be used in a Mobile Alarm System.

2.2.9 Global Positioning System (GPS)

GPS, or the Global Positioning System, is a global navigation satellite system that provides location, velocity and time synchronization. GPS is part of the Global Navigation Satellite Systems (GNSS).

Note: Where GPS is referenced, also other GNSS systems could be used.

2.2.10 Positioning Function (PF)

Function on the mobile device to determine its current location using GPS or beacons/access points .

2.2.11 Secure location:

location that is an ARC or another location that complies with a published data centre standard.

Note 1: Examples of published data centre standards or accepted best practices are: a data centre designed and maintained to EN 50600 series. Availability class 3, protection class 4 or ARC category I in accordance to EN 50518; or as best practice Uptime Institute Tier 3.

[SOURCE: 4.1.38 EN 50136-1/A1]

Note 2; ISO27001 certification with the right scope with accepted accreditation (EA MLA) is also possible based on additional Service Level Agreement with clear Key Performance Indicators (KPI) and trusted reporting based on these KPI's.

2.2.12 Hosted RCT:

RCT that consists of two parts, where one part is located in a secure location (RCT-H) and another part is installed in the MARC (RCT-A).

[SOURCE: 4.1.41 EN 50136-1/A1]

2.2.13 Alarm Receiving Centre (ARC):

continuously manned centre where information concerning the status of one or more AS is reported

Note 1: The MARC is not always certified for monitoring the status of one or more ATS. In that case it is an Alarm Receiving Centre (ARC).

[SOURCE: 4.1.39 EN 50136-1/A1]

2.2.14 Alarm Management System (AMS):

System at a MARC which stores, organizes, controls, manages and allows retrieval of client data and is interfaced to the alarm receiving equipment (RCT) for automatic annunciation of messages for each alarm system. For more information: annex C EN 50518:2019.

[SOURCE: 3.1.4 EN 50518:2019]

2.2.15 BYOD:

Bring your own device.

2.2.16 Monitoring Centre (MC);

centre in which the status of one or more ATSNs is monitored.

[SOURCE: 4.1.15 EN 50136-1/A1]

2.2.17 Alarm Transmission Equipment (ATE):

Collective term to describe SPT, MCT and RCT

[SOURCE: 4.1.4 EN 50136-1/A1]

2.2.18 Alarm Transmission System (ATS):

ATE and networks used to transfer information concerned with the state of one or more Alarm Systems at supervised premises to one or more AMSs of one or more MARCs.

Note 1 to entry: An ATS may consist of more than one ATP.

[SOURCE: 4.1.8 EN 50136-1/A1]

2.2.19 Alarm Transmission Service Network (ATSN):

Group of ATSs of the same category.

Note: An ATSN consists of one or more ATSs of the same category, functioning under supervision of the same management and monitoring centre.

[SOURCE: 4.1.6 EN 50136-1/A1]

2.2.20 Mobile Alarm System Provider

Entity which provides the Mobile Alarm System

3 Procedure for granting a product certificate

3.1 Initial investigation

The initial investigation to be performed is based on the (product, process and system) requirements as contained in this certification scheme, including the test methods, and comprises the following:

- type testing to determine whether the products comply with the product and/or functional requirements;
- first installation process assessment;
- maintenance process assessment;
- assessment of the quality system and the IQC-scheme;
  assessment on the presence and functioning of the remaining procedures.

3.2 Granting the product certificate

After finishing the initial investigation, the results are presented to the Decision maker deciding on granting the certificate. This person evaluates the results and decides whether the certificate can be granted or if additional data and/or tests are necessary.

3.3 Investigation into the process and/or performance requirements

Kiwa will investigate the to be certified products / systems against the certification requirements as stated in the certification requirements.
The necessary samples will be drawn by or on behalf of Kiwa.

3.4 Contract assessment

If the supplier is not the manufacturer of the products to be certified, Kiwa will assess the agreement between the supplier and the producer.
This written agreement, which is available for Kiwa, includes at least:
Accreditation bodies, scheme managers and Kiwa will be given the opportunity to observe the certification activities carried out by Kiwa or on behalf of Kiwa at the producer.

4 Requirements Mobile Alarm System (MAS)

4.1 General

This chapter contains the requirements which products have to fulfil.
The requirements for timely alarming, supervision of the communication and the availability of the system are arranged in the product and system requirements.

4.2 Product requirements

The devices arranging the supervised alarm transmission have to comply with the requirements in EN 50136-3; Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT);

- Server secure location <> Mobile device users emergency organisation.
- Server secure location <> Monitoring Centre (MC) and/or Alarm Receiving Centre (ARC)

These requirements are about the software of the devices and can be verified functional.

The mobile equipment shall comply with the Radio Equipment Directive (2014/53/EU).

4.3 System requirements

The supervised alarm transmission between the server in the secure location and the Monitoring Centre (MC) / Alarm Receiving Centre (ARC) has to comply with the requirements in EN50136-1/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).

The supervised alarm transmission between the server in the secure location and the mobile device users has to comply with the requirements in EN50136-1/A1 / IEC 60839-5-1; Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements.

The mobile devices shall be equipped with a multi network SIM with a minimum of two physical Telecom Provider Networks without data limit. A prepaid contract is not allowed. It is also allowed to use 2 different SIM cards from different providers that switch automatically.

SMS is only used as a backup when data communication 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 MAS per mobile device user must have the following specifics:

- Accuracy positioning on a surface level: this has to be specified by the supplier, it needs to have a minimum accuracy of 100 meter, determined using at least two methods of location positioning with no disturbance to the satellites:
- In case of inaccurate automatic positioning there needs to be a manual input for users.

4.3.1 Loggings of the system

According to EN50136-1 / 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.

4.4 Mobile devices supporting the MAS

The business continuity strategy of the MAS is such that dedicated and regular mobile devices can be used supporting the functioning of the MAS.
Dedicated devices are used when a higher security and / or safety (scope 1) level is needed by the end user.

By enforcing this strategy on a location, creates the possibility that all staff present on the designated location can use their regular mobile device (company using the MAS) obtaining a high percentage of users.

The settings on mobile devices shall be the following and are monitored by the MAS:

- The push notifications shall be turned on, and on priority when possible;
- The location services shall be turned on, and on high accuracy when possible.

The settings on mobile devices shall be the following:

- Any battery savers, task killers and virus scanners need to be turned off;
- VPN shall be turned off;
- Wi-Fi and Mobile data shall be turned on.

Remark; if these settings are not met by the users, this shall result in a low availability of users in a designated area. This shall be reported by the MAS.

4.5 Application mobile smart devices

This part contains the requirements that the application on the smart mobile device shall have to fulfil.

4.5.1 Use and access levels of the application

The application is attended to be used on general mobile smart devices.
The application shall connect direct to the MAS.
The application requires for this a logical access level 2 on the mobile smart device according to EN50131-1. The application shall enforce a new code after first installation.

The server of the MAS shall connect to a hosted web platform.
The hosted web platform requires for this a logical access level 3 according to EN50131-1.

4.5.2 Connections of the device

The application shall have a secure confidentiality connection between the MD and the MAS and met 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 server of the MAS shall have a secure connection to a hosted web platform according to IEC 60839-5-1 (EN50136-1/A1).

4.5.3 Acknowledgment un/setting

The setting made by means of the application shall be acknowledged by the MD of the MAS and the hosted web platform.
The setting made by means of the hosted web platform shall be acknowledged by the application of the smart mobile device.
By this is the live situation 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.

4.5.4 Uptime – availability – business continuity

The availability of the hosted web platform shall meet the requirements DP 4 according to IEC 60839-5-1 (EN50136-1).

The hosted web platform shall be hosted from a secure location complying with EN 50518 or EN 50600. See 2.2.8.

Hosting of the secure information shall be within the European Union.

4.5.5 Authenticity mobile smart devices

The definitions and processes of ISO/IEC 29115 shall be applied.
LoA3 shall be defined in the process of getting first access (onboarding) as an account to the application to the host and the MAS.
The application shall restrict a limited time within 2 factor authentication process.
The procedure getting access to the application on the mobile device shall be the same as to the MAS.
The procedure giving more users entrance to the application is the same as for the server
It is allowed to use biometrics according to latest standards according the standardisation group ISO/IEC JTC 1 SC 37 on Biometrics.

4.5.6 Session time mobile smart devices

A maximum session time shall be applied preventing un-authorized use for critical function(s) within the application such as the opening the application function for (settings) the server.
Protection against hostile access (brute force) to the application within the secure functions shall be in the testing stage of the application by penetration testing.

4.5.7 Instructions by the application towards the user

The application shall warn and instruct the user to use the application in a secure manner.

This part contains the requirements that the secure development process for the code shall have to fulfil.

4.6 Testing

The process shall be arranged according to parts of ISO27001.

Remark; An approved process according to scheme K21048 fulfils also this requirement.

4.6.1 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 threads / weakness of the security;
6. Deploying of the code in a hosted solution;
7. Review of the process for improvement of the next development.

4.6.2 Testing

The security testing of the code is based on minimal requirements in “The Ten Most Critical Web Application Security Risks” according to the latest OWASP rules, laid down at; www.owasp.org/

The code shall be tested according the latest applicable version of these rules.
The testing shall be performed in the end-to-end situation in a laboratory situation.

The testing shall be performed by an expert with a validated qualification by Kiwa.
The qualification shall be based on the:

- Level of general knowledge and experience of code testing (5 years);
- Level of specific knowledge and experience of the code (3 years);
- Level of general knowledge and experience of the product in its application in the specific market sector (1 year);
- Level of specific knowledge and experience of the latest OWASP rules based of the applicable specific “Vulnerability Subcategories” (2 years).

5 Functional requirements MAS - protection of vehicles and goods

In this chapter the additional functions are described that are not arranged in the product and system requirements. The protection of vehicles and goods is used for example in the logistic sector.

5.1 Installation of track and trace devices

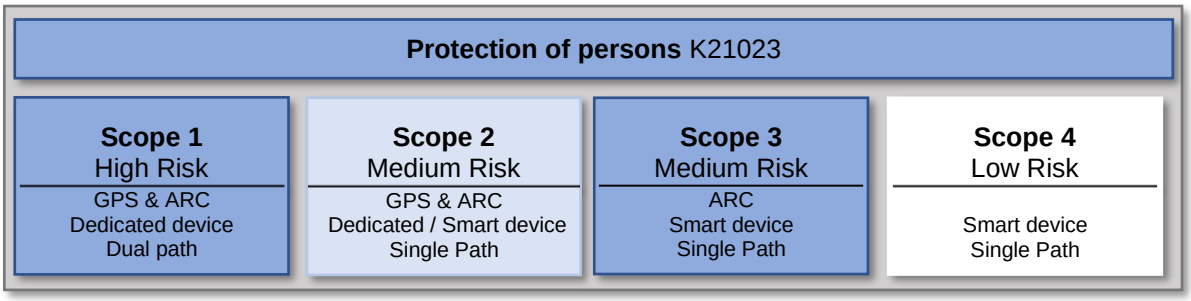
The installation is according to the specifications of the authority having jurisdiction in the scope and region where the MAS is in use.

5.2 Notification to the Alarm Receiving Centre (ARC)

Notification to the Alarm Receiving Centre is obliged. The action pattern is an agreement between the client and the ARC.

6 Functional requirements MAS - protection of persons

In this chapter the additional functions are described for personal alarm systems that are not arranged in the product and system requirements. This chapter contains of four scopes:



6.1 Security personal alarm systems with a high threat – scope 1 with GPS & ARC (High risks)

The requirements for these high risk personal alarm devices in scope 1 for the following specific applications are:
Persons who have high threat on aggression, violence or other incidents and where it is important that the location can be determined externally. Police or another authority determines who gets a device with this scope.

The dedicated device shall comply with:

- Touching the alarm activating function on the personal alarm device (press and hold for at least 1.5 seconds to activate the alarm;
- The device shall determine its current position at least every 90 seconds. The most up-to-date location is sent in the event of an alarm transmission;
- The device shall be equipped with a radio mobile data connection or better. A secondary alarm process should be arranged by SMS;
- The battery usage life of at least 8 hours during regular movement from a charged situation;
- The battery usage life of at least 2 hours in alarm status from a charged situation (with open / listen connection open);
- A compartment in which the battery and the SIM card are stored and shall be closed with mechanical protection to prevent sabotage;
- A vibrating signal (noticeable by hand) shall alert the user when the alarm has been sent, acknowledged and the operator of the ARC actually monitors the situation;
- A function in which a speaking/listening connection can be established by the ARC without the user's control;
  Note; this function shall be adjustable 1-way or 2-way connection.
- The speaking-listening connection may not be able to be interrupted by the user / attacker by any operation;
- The quality of the microphone should be such that the personal alarm device can be worn underneath one piece of clothing (tested in the pocket of a trousers) and can be easily heard during the listening in function if a normal noise level is used 45 dBA;
- A function where from 20% of the battery power the user of the personal alarm device receives a signal of the device of this status and sends a status signal to the MAS;

- A function that sends a stay alive (poll) of the personal alarm device by mobile data to the MAS at least every 90 seconds when the device is switched on;
- A secure pin code setting that cannot be changed by the user;
- A mobile data connection that can send the alarm message by, for example, a TCP / UDP protocol with an encryption of 128 bits to the MAS;
- An SMS function with which the alarm report can be sent as a backup to the ARC with the GPS location;
- No switch on the personal alarm device with the possibility to switch the device off;
- A "Whitelist" with only predetermined numbers that can connect with the device. This to prevent conscious or unconscious attempts of listening at the user;
- A device in scope 1 cannot be activated by a man down function.

6.1.1 Notification to the ARC in scope 1

The alarm handling by the alarm receiving centre (ARC) should be conform priority 1 according EN 50518. An extra requirement is:
Alarms within scope 1 shall be handled by 2 operators within 30 seconds. The first operator is listening to the client and the second operator is contacting the police.

6.2 Single workers / persons personal alarm systems – scope 2 with GPS & ARC (lone workers safety / single workers security)

The requirements for these medium risk personal alarm devices in scope 2 for the following specific applications are:
Single workers or employees who run the risk of aggression, violence or other incidents and where it is important that the location can be determined externally.

The dedicated devices / mobile device shall comply with:

- Touching the alarm activating function on the personal alarm device (press and hold for at least 1.5 seconds to continue the alarm or another activation mechanism with a low risk for false alarms);
- The device shall determine its current position at least every 120 seconds. The most up-to-date location is sent in the event of an alarm transmission;
- Battery or battery life of at least 8 hours during regular movement from a charged situation;
- Battery or battery life of at least 2 hours in alarm status from a charged situation (with dial-up connection open);
- Section in which the battery / accumulator and the SIM card are stored and must be closed with a mechanical protection to prevent sabotage;
- A tangible or audible signal notifies the user when the alarm has been sent and when the operator actually monitors the situation;
- A function where a speaking listening connection can be established by the alarm centre without the user's control; In case of danger of aggression, the 1-way connection is recommended, in the event of danger of accidents and health risks, the 2-way connection. This can be set customer and case dependent. The speaking-listening connection may not be able to be interrupted by the user / attacker by any operation;
- The quality of the microphone should be such that the personal alarm device can be worn underneath the clothing / jacket and can be easily heard during the listening in if a normal noise level is used;
- A function where from 20% of the battery or battery voltage the user of the personal alarm device receives a signal and sends a signal to the MAS;
- A function that sends a stay alive (poll) of the personal alarm device by mobile data to the MAS at least every 120 seconds when the device is switched on;
- A secure pin code setting that cannot be changed by the user;

- A mobile data function that can send the alarm message to the alarm platform;
- The personal alarm device must have the possibility that it cannot be switched off. This should be possible at the customer's request;
- Have a "Whitelist", so that only predetermined numbers can be called into the device. This is to prevent conscious or unconscious attempts at eavesdropping on the user.

6.2.1 Notification to the ARC in scope 2

The alarm handling by the alarm receiving centres (ARC) should be conform priority 1 according EN 50518.

6.3 Single workers personal alarm systems – scope 3 with ARC & without GPS

The requirements for the medium risk personal alarm devices is in scope 3 for internal use are for the following specific applications are:
Single workers or employees who run the risk of aggression, violence or other incidents working internally at a location or where it is not important that the location can be determined.

The mobile device must comply with:

- Touching the alarm activating function on the personal alarm device (press and hold for at least 1.5 seconds to continue the alarm or another activation mechanism with a low risk for false alarms);
- Battery or battery life of at least 8 hours from a charged situation;
- Battery or battery life of at least 2 hours in alarm status from a charged situation (with dial-up connection open);
- Section in which the battery / accumulator and the SIM card are stored and must be closed with a mechanical protection to prevent sabotage;
- A tangible or audible signal notifies the user when the alarm has been sent and when the device rings. When this last signal stops, the user knows that it is being monitored;
- A function where a speaking listening connection can be established by the alarm centre without the user's control; In case of danger of aggression, the 1-way connection is recommended, in the event of danger of accidents and health risks, the 2-way connection. This can be set customer and case dependent. The speaking-listening connection may not be able to be interrupted by the user / attacker by any operation;
- The quality of the microphone should be such that the personal alarm device can be worn underneath the clothing / jacket and can be easily heard during the listening in if a normal noise level is used;
- About a function where from 20% of the battery or battery voltage the user of the alarm device receives a signal and sends a signal to the alarm platform;
- A function that has been set from the moment of switch-on GPRS is connected to the alarm platform at least every 60 minutes (heart beat);
- A secure pin code setting that cannot be changed by the user;
- A mobile data function that can send the alarm message to the alarm platform;
- The personal alarm device must have the possibility that it cannot be switched off. This should be possible at the customer's request;
- The system must have the possibility to determine indoor positions using beacons or access points and to give this to the alarm receiving centre (ARC);
- Have a "Whitelist", so that only predetermined numbers can be called into the device. This is to prevent conscious or unconscious attempts at eavesdropping on the user.

6.3.1 Notification to the ARC in scope 3

The alarm handling by the alarm receiving centres (ARC) should be conform priority 1 according EN 50518.

6.4 Single workers personal alarm systems – scope 4 without ARC

The requirements for the low risk personal alarm devices in scope 4 for the following specific applications are: single workers or employees who run the risk of aggression, violence or other incidents that work internally at a location and where the alarms are sent to colleagues or third parties.

The mobile device must comply with:

- Touching the alarm activation function on the device (press and hold for at least 1.5 seconds to continue the alarm) or another activation mechanism with a low risk for false alarms).
- A tangible or audible signal notifies the user when the alarm has been sent.
- A function where from 20% of the battery or battery voltage the user of the alarm device receives a signal and sends a signal to the alarm platform.
- A function that has been set from the moment of switch-on GPRS is still connected to the alarm platform (stay-alive) at least every 60 minutes;
- A secure pin code setting that cannot be changed by the user;
- A mobile data function that can send the alarm message to the alarm platform.
- The alarm device must have the possibility that it cannot be switched off. This should be possible at the customer's request.
- The system must have the possibility to determine indoor positions using beacons or access points and to give this with the alarm message.
- Have a "Whitelist", so that only predetermined numbers can be called into the device. This is to prevent conscious or unconscious attempts at eavesdropping on the user.

7 Marking

7.1 General

The systems and products shall be marked with a declaration of conformity according this certification scheme and applicable standards. The declaration shall contain at least following information:

- name or logo of the supplier or manufacturer;
- data or code indicating the date of delivery or maintenance;
- type indication;
- certification marking according this scheme.

Indications and markings shall at least fulfil the requirements in the relevant product standard.

7.2 Certification mark

After concluding a Kiwa certification agreement, the certified products shall be indelible marked with the certification mark as is detailed in this scheme.

8 Requirements in respect of the quality system

This chapter contains the requirements which have to be met by the supplier's / service providers quality system.

8.1 Manager of the quality system

Within the supplier's / service provider organizational structure, an employee who will be in charge of managing the supplier's quality system must have been appointed.

8.2 Internal quality control / quality plan

The supplier / service provider shall have an internal quality control scheme / plan which is applied by him.

The following must be demonstrably recorded in this QC scheme / plan:

- which aspects are checked by the supplier;
- according to what methods such inspections are carried out;
- how often these inspections are carried out;
- in what way the inspection results are recorded and kept.

This IQC scheme should at least be an equivalent derivative of the model QC scheme / plan as shown in the Annex.

8.3 Control of test and measuring equipment

The supplier / service provider shall verify the availability of necessary test and measuring equipment for demonstrating product conformity with the requirements in this evaluation guideline.
When required the equipment shall be kept calibrated (e.g recalibration at interval).
The status of actual calibration of each equipment shall be demonstrated by traceability through an unique ID.
The supplier must keep records of the calibration results.
The supplier shall review the validity of measuring data when it is established at calibration that the equipment is not suitable anymore.

8.4 Procedures and working instructions

The supplier / service provider shall be able to submit the following:

- procedures for:
    - dealing with products showing deviations;
    - corrective actions to be taken if non-conformities are found;
    - dealing with complaints about products and/or services delivered;
- the working instructions and inspection forms used.

8.5 Instructions

The supplier / service provider shall design and deliver together with its MAS an installation, user and maintenance instruction. These instructions together with the software application shall arranges the access levels to the system according this scheme.

8.6 Training

The supplier / service provider shall design and deliver training to the staff that has the task for the setting of the configurations of the MAS.

The supplier / service provider shall adhere to training procedures for all relevant employees covering theoretical and practical skills to comply with the training requirements as laid down by legislation or by the ARC. There shall be a period of training, appropriate to ensure the minimum competency to carry out the specific duties, provided to all operators before they are allowed to handle alarms without supervision.
Further training shall be given on specific subjects such as new technical equipment or changes in operational procedures.

Employees training shall be documented and reviewed every year.

8.7 GDPR - General Data Protection Regulation

The user registration to the MAS and the position function of the system shall met the requirements off the General Data Protection Regulation (GDPR).
The requirements in this scheme attempt to fulfil these requirements in technical way.

A contract for parties exchanging personal data is needed

8.8 Monitoring and Alarm Receiving Centre

The applicable acting monitoring and alarm receiving centre shall fulfill the requirements of EN 50518.

Secure locations used to receive and sent information (data center) shall fulfill the requirements of EN 50518 or EN 50600.

8.9 Legal and operational set-up

The services shall only be offered, sold and executed by legal entities which are registered according to the law at their place of business. If the services are offered or sold or produced in different places, this requirement shall apply to each place of business used by the service provider.

The supplier / service provider shall have an liability insurance for its activities

8.10 Security screening and vetting

All employees in relevant employment shall be security screened and vetted. Other than visitors any person entering the Service Provider & ARC shall be screened. Visitors shall be accompanied by an Service Provider & ARC employee at all times while inside the Service Provider & ARC.
Screening shall be of a minimum of five years up to the commencement of relevant employment with the Service Provider & ARC, or back to the date of ceasing full-time education. A progress record shall be maintained to monitor and record the action taken and the information received during the screening and vetting process. The screening process shall be completed as soon as practicable but at least within 12 weeks unless an extension period is authorized by a director/principal of the Service Provider & ARC. In all instances, screening shall not exceed 16 weeks.
If the individual is employed prior to the completion of the screening or vetting process then the individual shall be notified that employment is subject to satisfactory screening and vetting and should be supervised at all times while working in the Service Provider & ARC.
A procedure shall describe how access rights are terminated.

8.11 Client Management

Client Management ensuring that profile data provided by the customer, contract and transaction information are kept current, and that third party liability is clearly excluded – in particular for installers and telecommunication providers.

8.12 Business Partner Management

Business Partner Management considering the various applicable business cases and contractual / operational relationships with the partners (for example; ARC's, equipment suppliers, telecommunication services providers).

9 Summary of tests and inspections

This chapter contains a summary of the following tests and inspections to be carried out in the event of certification:

- **initial investigation:** tests in order to ascertain that all the requirements recorded in the evaluation guideline are met;
- **inspection test:** tests carried out after the certificate has been granted in order to ascertain whether the certified products continue to meet the requirements recorded in the evaluation guideline;
- **inspection of the quality system of the supplier:** monitoring compliance of the IQC scheme and procedures.

9.1 Test matrix

Description of requirement	Article no. scheme	Tests within the scope of:	
		Pre-certification	Inspection by Kiwa after granting of certificate a,b)
Product requirements MAS			
Per applicable scope	4	x	x
Process requirements MAS – vehicles and goods			
If needed per applicable scope	5	x	x
Process requirements MAS - persons			
If needed per applicable scope	6	x	x
Quality system and Certification mark			
	7 & 8	x	x

a) In case the product or production process changes, it must be determined whether the performance requirements are still met.

b) All product characteristics that can be determined within the visiting time (maximum 1 day) are determined by the inspector or by the supplier in the presence of the inspector. In case this is not possible, an agreement will be made between the certification body and the supplier about how the inspection will take place. The frequency of inspection visits is defined in chapter 10.6 of this evaluation guideline.

9.2 Inspection of the quality system of the supplier

The quality system of the supplier will be checked by Kiwa on the basis of the IQC scheme.
The inspection contains at least those aspects mentioned in the Kiwa Regulations for Certification.

10 Agreements on the implementation of certification

10.1 General

Beside the requirements included in these evaluation guidelines, the general rules for certification as included in the Kiwa Regulations for Product Certification also apply. These rules are in particular:

- the general rules for conducting the pre-certification tests, in particular:
  - the way suppliers are to be informed about how an application is being handled;
  - how the test are conducted;
  - the decision to be taken as a result of the pre-certification tests.
- the general rules for conducting inspections and the aspects to be audited,
- the measures to be taken by Kiwa in case of Non-Conformities,
- the measures taken by Kiwa in case of improper use of Certificates, Certification Marks, Pictograms and Logos,
- terms for termination of the certificate,
- the possibility to lodge an appeal against decisions of measures taken by Kiwa.

10.2 Certification staff

The staff involved in the certification may be sub-divided into:

- Certification assessor (**CAS**): in charge of carrying out the pre-certification tests and assessing the inspectors' reports;
- Site assessor (**SAS**): in charge of carrying out external inspections at the supplier's works;
- Decision maker (**DM**): in charge of taking decisions in connection with the pre-certification tests carried out, continuing the certification in connection with the inspections carried out and taking decisions on the need to take corrective actions.

10.2.1 Qualification requirements

The qualification requirements consist of:

- qualification requirements for personnel of a certification body which satisfies the requirements EN ISO / IEC 17065, performing certification activities
- qualification requirements for personnel of a certification body performing certification activities set by the Board of Experts for the subject matter of this evaluation guideline

Education and experience of the concerning certification personnel shall be recorded demonstrably.

Basic requirements	**Evaluation criteria**
Knowledge of company processes Requirements for conducting professional audits on products, processes, services, installations, design and management systems.	*Relevant experience: in the field* **SAS, CAS** : 1 year **DM**: 5 years inclusive 1 year with respect to certification Relevant technical knowledge and experience on the level of: **SAS**: High school **CAS, DM** : Bachelor

Basic requirements	Evaluation criteria
Competence for execution of site assessments. Adequate communication skills (e.g. reports, presentation skills and interviewing technique).	**SAS**: Kiwa Audit training or similar and 4 site assessments including 1 autonomic under review.
Execution of initial examination	**CAS**: 3 initial audits under review.
Conducting review	**CAS**: conducting 3 reviews

Technical competences	Evaluation Criteria
Education	**General**: Education in one of the following technical areas: • Engineering.
Testing skills	**General:** • 1 week laboratory training (general and scheme specific) including measuring techniques and performing tests under supervision; • Conducting tests (per scheme).
Experience – specific	**CAS** • 3 complete applications (excluding the initial assessment of the production site) under the direction of the **PM** • 1 complete application self-reliant (to be evaluated by **PM**) • 3 initial assessments of the production site under the direction of the **PM** • 1 initial assessment of the production site self-reliant (witnessed by **PM**) **SAS** • 5 inspection visits together with a qualified **SAS** • 3 inspection visits conducted self-reliant (witnessed by **PM**)
Skills in performing witnessing	**PM** Internal training witness testing

Legend:
- Certification assessor (**CAS**)
- Decision maker (**DM**)
- Product manager (**PM**)
- Site assessor (**SAS**)

10.2.2 Qualification

The qualification of the Certification staff shall be demonstrated by means of assessing the education and experience to the above mentioned requirements. In case staff is to be qualified on the basis of deflecting criteria, written records shall be kept.

The authority to qualify staff rests with the:
- **PM**: qualification of **CAS** and **SAS**;
- management of the certification body: qualification of **DM**.

10.3 Report initial investigation

The certification body records the results of the initial investigation in a report.
This report shall comply with the following requirements:

- completeness: the report provides a verdict about all requirements included in the evaluation guideline;
- traceability: the findings on which the verdicts have been based shall be recorded and traceable;
- basis for decision: the **DM** shall be able to base his decision on the findings included in the report.

10.4 Decision for granting the certificate

The decision for granting the certificate shall be made by a qualified Decision maker which has not been involved in the pre-certification tests. The decision shall be recorded in a traceable manner.

10.5 Layout of quality declaration

The product certificate shall be in accordance with the model included in the Annex.

10.6 Nature and frequency of third party audits

The certification body shall carry out surveillance audits on site at the supplier at regular intervals to check whether the supplier complies with his obligations. The Board of Experts decides on the frequency of audits.

At the time this certification scheme entered into force, the frequency of audits amounts of 1 audit on site per year for suppliers.

The results of each audit shall be recorded by Kiwa in a traceable manner in a report.

10.7 Non conformities

When the certification requirements are not met, measures are taken by Kiwa in accordance with the sanctions policy as written in the Kiwa Regulation for Certification.
The Sanctions Policy is available through the “News and Publications” page on the Kiwa website "Kiwa Regulation for Certification".

10.8 Report to the Board of Experts

De certification body shall report annually about the performed certification activities.
In this report the following aspects are included:

- mutations in number of issued certificates (granted/withdrawn);
- number of executed audits in relation to the required minimum;
- results of the inspections;
- required measures for established Non-Conformities;
- received complaints about certified products.

10.9 Interpretation of requirements

The Board of Experts may record the interpretation of requirements of this evaluation guideline in one separate interpretation document.

10.10 Specific rules set by the Board of Experts

By the Board of Experts the following specific rules have been defined. These rules shall be followed by the certification body.

11 Titles of standards

11.1 Public law rules

Not applicable

11.2 Standards / normative documents

Number	Title	Version*
ISO/IEC 17020	Conformity assessment - General criteria for the operation of various types of bodies performing inspection	
ISO/IEC 17021	Conformity assessment - Requirements for bodies providing audit and certification of management systems	
ISO/IEC 17024	Conformity assessment - General requirements for bodies operating certification of persons	
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories	
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services	
IEC 60839-5-1	Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements	2014
EN 50136-1/A1	Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems	2012/ 2018
EN 50136-3	Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)	2013
EN50518	Monitoring & Alarm Receiving Centre	2019
EN50131-1	Alarm systems - Intrusion and hold-up systems - Part 1: System requirements	2006
ISO27001	Information technology - Security techniques - Information security management systems - Requirements	2017
K21030	Alarm Transmission Service Providers	2020

*) When no date of issue has been indicated, the latest version of the document is applicable.

I Model certificate (example)

CERTIFICATE

Product certificate
KXXXXXX/0X

kiwa

Issued

Replaces

Page 1 of 1

Name product

STATEMENT BY KIWA
With this product certificate, issued in accordance with the Kiwa Regulations for Certification, Kiwa declares that legitimate confidence exists that the products supplied by

Name customer

as specified in this product certificate and marked with the Kiwa®-mark in the manner as indicated in this product certificate may, on delivery, be relied upon to comply with Kiwa evaluation guideline BRL-xxxx "xxxxxxxxxxxxxxxxxxxxxxxxxf" **dated [dd-mm-yyyy]** inclusive amendment sheet dated dd-mm-yyyy.

Luc Leroy
Kiwa

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

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
P.O.Box 70
2280 AB RIJSWIJK
The Netherlands
Tel. +31 88 998 44 00
Fax +31 88 998 44 20
info@kiwa.nl
www.kiwa.nl

Company
Name customer
Address customer

Phone number
Fax number
www.
Email

Certification process consists of initial and regular assessment of:
- quality system
- product

140410

II Model IQC-scheme manufacturer (example)

Inspection subjects	Inspection aspects	Inspection method	Inspection frequency	Inspection registration
Base materials or materials supplied: - recipe sheets - incoming goods inspection base materials				
Production process, production equipment, plant: - procedures - working instructions - equipment - release of product				
Finished-products				
Measuring and testing equipment - measuring equipment - calibration				
Logistics - internal transport - storage - preservation - packaging - identification				