K210046/01
20190215
Definitive

Hosted Alarm Solution

for the Kiwa process certificate for the infra structure and processes for hosted alarm handling

Trust
Quality
Progress

Preface

This international evaluation guideline / certification scheme has been accepted by the Kiwa Board of Experts Security, in which all relevant parties in the field of the alarm chain are represented. The Board of Experts also supervises the certification activities and where necessary requires the evaluation guideline / certification scheme to be revised. All references to Board of Experts in this evaluation guideline / certification scheme pertain to the above mentioned Board of Experts.

This international evaluation guideline / certification scheme will be used by Kiwa in conjunction with the Kiwa Regulations for Certification. The purpose of this certification scheme is to clarify the way in which a Declaration of Conformity regarding the performance, reliability, resilience and security requirements with respect to a hosted alarm handling (HAH) platform is structured. An HAH platform is intended for hosted alarm processing and handling, where the necessary equipment is not necessarily in one location.
The HAH platform therefore consists of locations, hardware, software and networks. All this is under the control of a monitoring centre or alarm reception centre that performs the same function. All the above components are tested against European standards.

Kiwa Nederland B.V.

Sir Winston Churchilllaan 273

Postbus 70 - 2280 AB RIJSWIJK

The Netherlands
Tel. +31 88 998 44 00
info@kiwa.nl
www.kiwa.nl

Kiwa FSS
Dwarsweg 10
5301 KT Zaltbommel
The Netherlands
Tel. +31 (0)88 998 5100
Info.ncp@kiwa.nl
www.kiwafss.nl

© 2019 Kiwa N.V.
All rights reserved. No part of this report may be reproduced, stored in a database or retrieval system, or published, in any form or in any way, electronically, mechanically, by print, photoprint, microfilm or any other means without prior written permission from the publisher.
The use of this evaluation guideline by third parties, for any purpose whatsoever, is only allowed after a written agreement is made with Kiwa to this end.

Validation
This evaluation guideline has been validated by the Director Certification and Inspection FSS of Kiwa on February 22th, 2019

5911.80330

Contents

1 Introduction

1.1 General

This evaluation guideline / certification scheme includes all relevant requirements which are employed by Kiwa when dealing with applications for the issue and maintenance of a certificate for the processes and infrastructure for the application of the hosted alarm solution.

The function and performance, reliability, resilience and security requirements with respect to a hosted alarm handling (HAH) platform is structured. An HAH platform is intended for hosted alarm processing and handling, where the necessary equipment is not necessarily in one location.
The HAH platform therefore consists of locations, hardware, software and networks. All this is under the control of a monitoring centre or alarm reception centre that performs the same function. All the above components are tested against European standards.

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

1.2 Field of application / scope

The processes and infrastructure are intended to be used for the handling of alarms in a hosted alarm solution.

An HAH platform is a solution for the processing of alarms, where the processing and/or handling equipment is not only (or not) in the alarm receiving centre, but in data centres or distributed over multiple alarm reception centre locations. With an HAH platform, the customer, being the alarm receiving centre, is supported with respect to the technical set-up and continuity of alarm reception, processing and handling. By placing the required infrastructure and equipment in data centres or EN50518-certified locations and spreading it over multiple locations (redundancy), there is a much higher degree of availability. The customer connects to the servers via a secure session, which enables alarm handling in the alarm management software via a client.

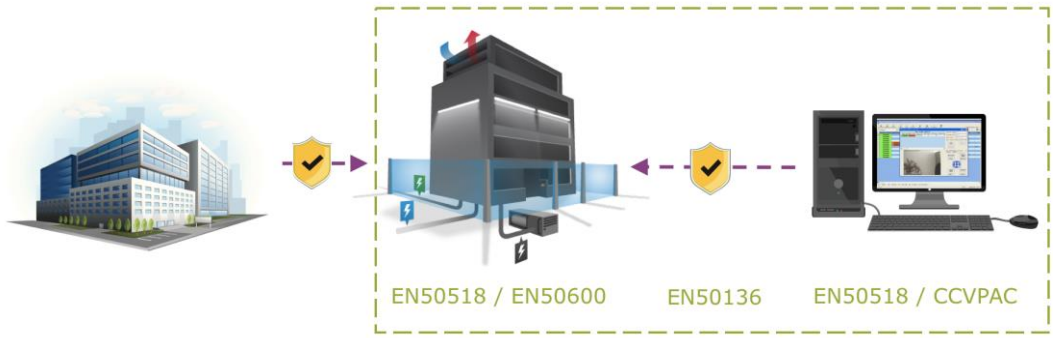

Figure 1. Hosted alarm handling scope

An HAH platform consists of locations, hardware, software and network(s). All of this is under the control of a MARC or ARC that performs the same function. There are always at least two locations so that continuity of service can be guaranteed. If one of the locations should drop off due to unforeseen circumstances, the service will not be interrupted, due to the availability of the other location(s). This concerns a total solution for infrastructure, equipment and alarm management system.

Figure 2. Example of data sources distributed over multiple locations

All the above components are tested against European standards. The delivery of an HAH platform requires:

A. A location or locations that meet the criteria set in EN50518 and/or EN50600;
B. An alarm receiver/processor (RCT=**B1** and iRCT=**B2**) that functionally meets the requirements set in EN50136-3 and is compatible with a defined alarm transmitter (Supervised Premises Transceiver (SPT));
C. A network between the customer and the RCT as part of EN50136-1;
D. A management system, as described in Requirements for the management system, which is focused on the performance of the HAH platform and produces periodic reports, which are sent directly to the end-user if necessary. In addition, the Plan-Do-Check-Act (PDCA) cycle is used, with which corrective and preventive measures are taken if the HAH platform does not meet the performance requirements;
E. Alarm management software required for the handling of alarms within an EN50518-approved alarm centre;
F. The monitoring or alarm receiving centre that collects the data and handles alarms according to requirements and thus meets the criteria set in EN50518.

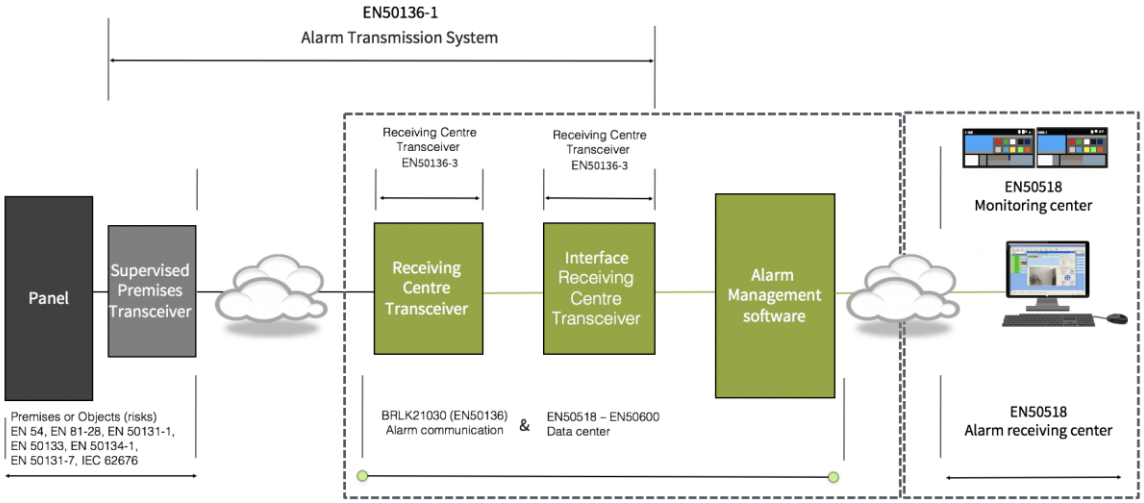

Figure 3. Components within Hosted Alarm Handling

1.3 Demarcations

For certification based on this scheme are the following domains recognized:

1) The supplier of the HAH platform;
2) An alarm receiving centre that uses an HAH platform and a data centre for operational continuity;
3) The operator of the data centre who (physically) provides a location in which the HAH platform can be placed.

1.4 Responsibilities

With regard to the scope and responsibilities, the following should be recognized:

1.The supplier of the HAH platform that supplies the equipment, the network and the service, which is responsible for the entire scope and with that the service (A - E);

2.The supplier, being the monitoring or alarm receiving centre, that collects the data and handles alarms according to requirements and thus meets the criteria set in EN50518 (F);

3.The supplier of the location of the hosted environment, which is responsible for the environment as well as continuity of service (A);

4.The supplier of an alarm receiver/processor RCT and/or interface alarm receiver/processor iRCT that functionally meets the requirements set in EN50136-3 and which is compatible with a defined alarm transmitter SPT approved in accordance with EN50136-2; (B1 and B2);

5.The supplier of the network, which is responsible for the components, security and availability and therefore performance of the (critical communication) network (C);

6.The supplier of alarm management software for the handling of alarms (E).

Overview of certification types and test ;criteria based on International / European standards				
	Certification type	**Demarcation**	**Component**	**Standard(s)**
1	Process	1	A, B, C, D and E	EN50136-1/A1, EN50136-3, EN50518 and EN50600 (partly*)
2	Process	2 (in combination with A)	F	EN50518
3	Process	3	A	EN50518 and EN50600 (partly*)
4	Product	-	B1 and B2	EN50136-3
5	Process	-	C	EN50136-1
6	Product & Process	-	E	EN50136-3 and EN50518

* EN50600-2-5 availability class 3 and security class 4

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 Kiwa process certificate.
The supplier of the process leading to the service (demarcations 1, 2 and 3) of the "Hosted Alarm Handling" will thus be certified.
A model of the certificate to be issued on the basis of this evaluation guideline / certification scheme has been included for information as Annex.

2 Terms and definitions

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

2.1 Definitions general

Board of Experts: the Board of Experts Security.

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.

Evaluation Guideline (BRL): certification scheme with the agreements made within the Board of Experts on the subject of certification.

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 evaluation guideline.

IQC scheme (IQCS): a description of the quality inspections carried out by the supplier as part of his quality system.

Initial investigation: tests in order to ascertain that all the requirements recorded in the evaluation guideline are met.

Private Label Certificate: A certificate that only pertains to products that are also included in the certificate of a supplier that has been certified by Kiwa, the only difference being that the products and product information of the private label holder bear a brand name that belongs to the private label holder.

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.

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.

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

2.2 Definitions specific

AMS: Alarm Management System; software for handling alarms as defined in EN50518.

ARC: Alarm Receiving Centre; a monitoring or alarm centre that collects data and handles alarms according to requirements and thus meets the criteria set in EN50518.

ATS: Alarm Transmission System. This is a transmission system for alarm communication in accordance with EN50136-1, whereby the transmission system is provided by a service organization that ensures the guaranteed monitoring of the functioning and performance of the transmission system. In addition, proactive management is conducted over this system to ensure that failing transmission is restored to specification and end-users are informed about this. These systems are intended for users who want to have a guarantee from end to end about the functioning of a transmission system.

HAH: Hosted alarm handling platform as described in this assessment guideline

CTS: This concerns a transmission system for critical communication, a Critical Communication Transmission System, where the transmission system is provided by a service organization that ensures secure monitoring of the functioning and performance of the transmission system. In addition, proactive management is conducted over this system to ensure that failing transmission is restored to specification and end-users are informed about this. These systems are intended for users who want to guarantee the functioning of a transmission system for a large part of the transmission. Where further reference is made in this scheme to ATS, but the scope is limited to critical transmission, CTS will have to be read. There is no end-to-end situation here.

MARC: Monitoring & Alarm Receiving Centre as agreed in EN50518.

RCT: Receiver Centre Transceiver; an alarm receiver required for receiving and processing incoming alarms.

3 Procedure for granting a product certificate

3.1 Initial investigation

The initial investigation to be performed are based on the (process) requirements as contained in this evaluation guideline / certification scheme, including the test methods, and comprises the following:

- testing to determine whether the processes comply with the performance and/or functional requirements;
- infra structural process assessment;
- assessment of the quality system and the IQC-scheme;
- assessment on the presence and functioning of the remaining procedures.

Initial assessment

The initial assessment to be done will take place based on the requirements included in this evaluation guideline including test methods and, depending on the nature of the system/process to be certified:

- the establishment of the demarcation (configuration) and the specifications (categories) of the Hosted Alarm Handling platform on the basis of the requirements in EN50136-1 and EN50518;
- the assessment of the product quality of relevant components on the basis of EN50136-3;
- the assessment of the location(s) based on EN50518 or EN50600;
- the assessment of the network architecture based on EN50136-1;
- the assessment of the security requirements of the HAH platform on the basis of EN50136-1;
- the assessment of the availability of the HAH platform on the basis of EN50136-1;
- the assessment of HAH functionality within the monitoring or alarm receiving centre that collects the data and handles alarms according to requirements and thus meets the criteria set in EN50518;
- the assessment of the corrective actions by the HAH supplier on failing communication;
- the assessment of the management system of the HAH supplier regarding the delivery of the service;
- testing the functioning of supporting procedures to be able to meet the above assessments.

Part of the audit is carried out in two phases, namely:

- Document audit: this determines on the basis of documentation and architectural drawings to what extent the HAH platform has the potential to meet the requirements.
- Implementation audit: this determines on the basis of inspection(s) on location(s) to what extent the system has met the documented requirements.

3.2 Granting the process certificate

After finishing the initial investigation, the results are presented to the Decision maker (see 8.2) 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 processes against the certification requirements as stated in the certification requirements.
The necessary samples inspections will be drawn by or on behalf of Kiwa.

3.4 Infra structural process assessment

When assessing the infra structural processes, it is investigated whether the supplier is capable of a continuously delivery process that meet the certification requirements.
The evaluation of the process takes place during the ongoing work at the supplier.
The assessment also includes at least:

- The quality of infra structure and the functions and output of the process;
- Internal controls on the process and storage of the data.

3.5 Contract assessment

If the supplier is not the supplier of the process to be certified, Kiwa will assess the agreement between the sub supplier and the end supplier.
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 supplier.

4 Requirements

4.1 General

This chapter contains the requirements that the processes have to fulfil.

The requirements included in this assessment guideline are used by the certification body for processing an application, maintaining certification of an "HAH platform" based on EN50136-1; alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for Alarm Transmission Systems, EN50518 Alarm receiving centres and EN50600 - Data centre facilities and infrastructure.

The origin of this scheme lies in the need of the market to organize hosted alarm processing and handling according to quality standards on the basis of agreed and measurable requirements.

The purpose of this scheme is to make the quality at the suppliers of this service verifiable, in order to provide customers and the market with insight into which services fall within the scope and which meets the set requirements.

In this scheme are International / European standards used as the basis for the assessment of the processes and/or products.

4.2 Regulatory requirements

4.2.1 For the Netherlands

This process aims to fulfil the requirements in the Rpbr; “Regeling particuliere beveiligingsorganisaties en recherchebureaus”.

4.3 Infra structure and process requirements

This chapter contains the requirements that the system must meet, as well as the determination methods to establish that the requirements are met. Below is an overview of the technical verification points to be applied.

Subject	Test criteria	Methodology
The location or locations where the alarm reception and processing equipment is located	The assessment of the location(s) will take place on the basis of EN50518-Chapter 5 or EN50600-2-5 availability class 3 and security class 4	• Verification of documentation • Inspection • Testing
The functional operation of the alarm receiver/processor (RCT and iRCT) must be the same as that set in EN50136-3 and compatible with a defined and accordingly approved alarm transmitter (SPT)	The assessment of the alarm receiver/processor (RCT and iRCT) will take place on the functional operation as set in EN50136-3 or by verification of existing product certificates issued by a (17025) accredited test institute. This also applies to the alarm transmitter (SPT)	• Verification of documentation • Testing
The network between the customer alarm centre (ARC) and the Alarm Receiver (RCT)	The assessment of the network will take place on the basis of EN50136-1, where the DP4 requirement (99.9% availability and at least 256-bit encrypted tunnel based on end-to-end encryption - device to device) is maintained.	• Verification of documentation • Inspection • Testing
Alarm management software for handling alarms within an EN50518 approved alarm centre	The assessment of the alarm management software (AMS) will take place by means of on-site verification and the functional operation for the RCT as set in EN50136-3 or existing product certificates issued by an (17025) accredited testing institute.	• Verification of documentation • Testing
The monitoring or alarm receiving centre that collects the data and handles alarms according to requirements and thus meets the criteria set in EN50518;	The assessment of the alarm receiving centre ((M)ARC) will take place by means of on-site verification and the existing EN50518 process certificates for the ARC issued by an (17065) accredited testing institute.	• Verification of documentation • Inspection
The management system focuses on the performance of the HAH platform, which produces periodic reports, which are sent directly to the end user if necessary	The assessment of the management system will take place on the basis of chapter Requirements for the management system. The requirements from this chapter are from EN50518 and ISO27001.	• Verification of documentation • Interviews

4.3.1 Specific requirements for HAH platform

This chapter contains the requirements that the system must meet, as well as the determination methods to establish that the requirements are met.

Below is an illustration of the structure of an HAH platform:

Figure 4. Example landscape Hosted Alarm Handling

Below is an overview of the technical verification points to be applied.

Subject	Test criteria	Methodology
Scope The software required for HAH runs on multiple servers/receivers with possibly physical data storage. The HAH platform consists of multiple modules (software components) (e.g. interface modules for connection to the RCTs, routers, firewalls, switches, etc.). IP addresses are owner of the IP addresses.	The assessment of the scope of the HAH platform takes place on the basis of network infrastructure drawings and access to issued IP addresses.	• Verification of documentation • Inspection • Testing
Structure of AMS If the AMS consists of an interface module for connecting RCT (IRCT in Figure C1), it is considered as part of the AMS that must meet the requirements of this standard. (*The use of different RCTs from different manufacturers connected to an AMS with an interface module (IRCT)).*	The assessment of the AMS of the HAH platform takes place on the basis of network infrastructure drawings and demonstration of the functioning of the AMS.	• Verification of documentation • Inspection of the AMS
Integration of AMS The AMS can be integrated in a single housing with RCT(s), a standalone device or system or distributed over multiple servers. In all cases, the functional effect must be the same as that stated in EN50136-3.	The assessment of the set-up of the AMS within the HAH platform takes place on the basis of network infrastructure and insight into the structure of the system.	• Verification of documentation • Inspection • Testing
Influence and preference Primary is the platform intended for alarm handling. When the AMS contains functions other than those required for receiving and presenting alarm information and messages, alarms should be presented as first priority above all other functions.	The assessment of the set-up of the AMS within the HAH platform takes place on the basis of network infrastructure and insight into the structure of the system. In addition, the prioritization of the various functions must be demonstrated by means of a functional test.	• Verification of documentation • Inspection • Testing

Subject	Test criteria	Methodology
Links If the connection module of an AMS is connected to another AMS or integrated in the same or distributed over multiple locations, the communication path(s) between two or more AMSs must have at least the same security level (256-bit encryption) and the same performance (DP4) as the most demanding alarm transmission system connected to one of the AMSs.	The links with the AMS within the HAH platform takes place on the basis of network infrastructure and insight into the structure of the system.	• Verification of documentation • Inspection • Testing
User interface The interface for the ARC operators must be part of the AMS. It is also possible to connect the AMS via connection module to a following AMS with user interface for the ARC operators. However, the communication path(s) between two or more AMSs must have at least the same security level and the same performance as the most demanding alarm transmission system connected to one of the AMSs.	The assessment of the user interface of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing
Access level(s) The AMS must be provided with means to limit access to its functions. The manufacturer must specify the means to restrict access and specify the functions that are accessible at each access level (e.g. physical keys or logical passwords).	The assessment of insight into the structure of the system and a demonstration of the different access levels.	• Inspection • Testing

Subject	Test criteria	Methodology
Access to AMS functions must be subdivided into at least four levels, as specified below: - access level 1: no authorization required; - access level 2: enabling the operation of the AMS (e.g. acceptance of messages); - access level 3: enabling access for configuring or modifying the configuration of the AMS (e.g. disabling warning indication or setting input priorities): - access level 4: granting access and changing the hardware or software of the AMS (e.g. changes made by the manufacturer).	The assessment of the access levels of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing
Access to the AMS Access to message acceptance and information presentation functions should be limited to access level 2. If the AMS contains configuration data, access to the data must be authorized by appropriate access levels. Tools must be provided for viewing and modifying the system configuration data. To view configuration data, access on level 2 is required. Modification of configuration data requires access on level 3. All modifications to the configuration must be documented (e.g. entering or changing passwords).	The assessment of the access levels of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection Testing

Subject	Test criteria	Methodology
Access to the database Modification of the database must be possible locally and/or remotely at access level 3. RCTs used for communication with SPTs may not be used for remote access to the database.	The assessment of the access to the database of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing
Shared databases If a shared database is used, access to the otherwise database must be prevented by authorizations and logical access rights.	The assessment of the access to the database of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing
Access to log data A means must be provided to access the log data. Access to the log data to back up the data for long-term storage must be limited to access level 3. The log data must be incorruptible at all times.	The assessment of the access to the log data of the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing
Monitoring the interconnection with the RCT / iRCT The AMS must monitor the interconnection with the RCTs. The means to monitor and the type of error that must be detected must be described in the manufacturer's documentation. As a minimum, the physical interruption of the interconnection must be recognized and detected. In the event that the interconnection fails, error information must be generated and presented within 10 s.	The assessment of the monitoring of the interconnection with the RCT(s) within the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing

Subject	Test criteria	Methodology
Detecting errors The AMS must monitor its actual function and the function of the hardware and software components (e.g. software watchdog). At least the following must be detected: - disruption or failure of parts of the management software; - receipt of data that cannot be correctly interpreted or processed by the AMS.	The assessment of the detection of errors within the HAH platform takes place on the basis of network infrastructure drawings and demonstration.	• Verification of documentation • Inspection • Testing

5 Marking

5.1 General

The processes shall be marked with following indelible marks and indications:

- name or logo of the supplier;
- data or code indicating of the version;
- type indication.

5.2 Certification mark

After concluding a Kiwa certification agreement, the certified products shall be indelible marked with the certification mark relating to this process.

6 Requirements in respect of the quality system

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

6.1 Manager of the quality system

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

6.2 Internal quality control / quality plan

The supplier shall have an internal quality control scheme (IQC scheme) which is applied by him.

The following must be demonstrably recorded in this IQC scheme:

- 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 IQC scheme as shown in the Annex.

6.3 Control of test and measuring equipment

The supplier 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.

6.4 Procedures and working instructions

The supplier 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.

6.5 Management system

The supplier has set up a management system for the scope of this certification scheme. Within the management system, the supplier has in particular documented and regularly updated policies and plans for:

6.5.1 Risk and operational continuity management

These aspects of resilience, operational continuity and disaster recovery are covered with a comprehensive risk analysis, for example according to ISO27005.

It will include plans for data centre(s) and/or ARC location and take into account measures to handle unexpected events and associated measures for prevention, early detection and handling at the management and technical level.

It includes in particular;

- Standard operational procedures;
- ICT security (information and communication technology) within the Data Centre and the ARC;
- Prioritization for the maintenance and/or restoration of activities and services, including contact details of contractors and service providers that can achieve re-entry and a description of the means by which the services will be continued or restored;
- Management of personnel level during unexpected events;
- Communication to all stakeholders during and after disruption or failure;
- Current risk analysis reports and plans are available at all times for management review and audit.

6.5.2 Services

Management of the service portfolio for creating, managing and deploying the services provided, including a list of services that currently apply to existing customers and that is available to new customers.

6.5.3 Customer management

Customer management ensures that the personal data provided by the customer, contract and transaction data are kept up to date and that the liability of third parties is clearly excluded. Taking into account the requirements set in the General Data Protection Regulation (GDPR).

6.5.4 Quality of service

The procedures for processing the individual services must contain prevention against poor quality of the handling. They include checking the execution quality (technical/human) of the handling according to the agreed action plan. The supplier has:

Listing and measurement methods for Key Performance Indicators (KPIs) that are essential for demonstrating that the services sold by the HAH supplier meet certain performance levels;

- Uptime of the platform is 99.9%
- Capture of a disruption within 4 hours
- Resolution time within 8 hours

Listing and measurement methods for operational KPIs that are essential for daily management and continuous improvement of performance;

Complaints handling for all stakeholders with a view to settling each individual complaint, and identifying systematic errors that also require adjustment of procedures, policies or guidelines.

6.5.5 Personnel

Management of professional competence and confidentiality of staff regarding access to the Data Centre and/or ARC buildings and processes. In addition, job descriptions, qualification profiles, training plans and career profiles must be available for all employees.

6.5.6 Partners

In the event of outsourcing or subcontracting, the requirements set out in this assessment guideline will remain fully in force on the supplier. By means of an SLA, it must be possible to demonstrate whether the parties have agreed to the requirements as set out in this scheme.

6.6 Information management

6.6.1 Information processing

Documented procedures describe how all data will be stored, organized, changed, managed and recovered. The procedure determines how data are connected to all alarm receiving devices of all messages for each alarm system and for maintaining records of operational events. Additional procedures describe how the data is maintained, protected, stored and deleted. Checks will be set up and maintained to prevent loss, destruction, falsifying, unauthorized access and unauthorized release of data by means of unintended or malicious interference. These checks take into account applicable laws and regulations, contractual obligations and operational requirements.
This also implies IT systems and IT security, including observation of the European General Data Protection Regulation (GDPR) or similar.

6.6.2 Backup of data

Documented procedures are set up indicating how all client and system data are handled with regard to availability and reliability. In addition, the client and system data must be backed up for at least three months. Customer information must also be stored within the HAH platform in accordance with the written term agreed with the customer, but for at least two years, as well as the log files regarding operator actions.

6.6.3 Confidentiality and classification of information

Clear and unambiguous procedures are established and documented for every person who has access to the data in order to guarantee confidentiality.

The procedure includes:
A clear policy for paper and removable storage media and a clear screen policy for information processing facilities;
Information classification and labelling in terms of legal requirements, value, critical status and sensitivity to unauthorized disclosure or modification will be appropriate and applied by all employees.

6.6.4 Installation, maintenance, protection, removal and re-use of resources

There will be documented procedures to describe who may approve and execute the installation, maintenance, disposal and/or reuse of resources. These will take into account the specific risks associated with the data and licensed software. The procedure also ensures that unmanaged equipment has appropriate protection.

7 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.

7.1 Test matrix

Description of requirements	Article no. scheme	Within the scope of:	
		Pre-certification	Inspection by Kiwa after granting of certificate a,b)
Scope			
Infra structure Demarcations Responsibilities	1.2 1.3 1.4	X	X
Requirements			
Infra structure & process	4	X	X
Other requirements			
Quality system	6	X	X
Certification mark			
Application	5	X	X

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

b) All 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 8.6 of this evaluation guideline.

7.2 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.

8 Agreements on the implementation of certification

8.1 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.

8.2 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.

8.2.1 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: • Electronical Engineering; • Security Engineering; • Safety Engineering.
Testing skills	**General:** • A laboratory training (general and scheme specific) including measuring techniques and performing tests under supervision ; • Conducting tests (per scheme).
Experience - specific	**CAS** • 1 complete applications (excluding the initial assessment of the site) under the direction of the **PM** • 1 complete application self-reliant (to be evaluated by **PM**) • 1 initial assessments of the site under the direction of the **PM** • 1 initial assessment of the site self-reliant (witnessed by **PM**) **SAS** • 2 inspection visits together with a qualified **SAS** • 1 inspection visits conducted self-reliant (witnessed by **PM**)
Specific knowledge	**CAS & SAS** • EN50136-1, 2 and 3 • EN50600-2-5 • EN50518 parts 1, 2 and 3 • ISO27001 • ISO22301
Skills in performing witnessing	**PM** Internal training witness testing

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

8.2.2 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**.

8.3 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.

8.4 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.

8.5 Layout of quality declaration

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

8.6 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.

The audit surveillance program on site shall cover at least:
The (surveillance) audit to be conducted takes place on the basis of the requirements included in this certification scheme, including test methods and, depending on the nature of the system to be certified, the following components:

- the establishment of the demarcation (configuration) and the specifications (categories) of the HAH platform on the basis of the requirements in EN50136-1 and EN50518;
- the determination that the location(s) still comply on the basis of EN50518 or EN50600;
- the determination that the product quality of relevant components is still satisfactory on the basis of EN50136-3;
- the determination that the network architecture still complies with EN50136-1
- the assessment of the security requirements of the HAH platform on the basis of EN50136-1;
- the assessment of the availability of the HAH platform on the basis of EN50136-1;
- the assessment of HAH functionality within the monitoring or alarm receiving centre that collects the data and handles alarms according to requirements and thus meets the criteria set in EN50518;
- the assessment of the corrective actions by the HAH supplier on failing communication;
- the assessment of the management system of the HAH supplier regarding the delivery of the service;

- testing the functioning of supporting procedures to be able to meet the above assessments.

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

8.7 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".

8.8 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.

8.9 Interpretation of requirements

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

8.10 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.
Compliance audits are carried out annually by a body accredited for EN 50518 and ISO27001 based on EN/ISO/IEC 17065 and 17021 in accordance with EA MLA (European Cooperation for Accreditation).

9 Titles of standards

9.1 Regulations

Rpbr Netherlands	Regeling particuliere beveiligingsorganisaties en recherchebureaus (1-10-2016)

9.2 Standards / normative documents

Number	Title	Version*
NEN-EN ISO/IEC 17020	Conformity assessment - General criteria for the operation of various types of bodies performing inspection	
NEN-EN ISO/IEC 17021	Conformity assessment - Requirements for bodies providing audit and certification of management systems	
NEN-EN ISO/IEC 17024	Conformity assessment - General requirements for bodies operating certification of persons	
NEN-EN ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories	
NEN-EN ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services	
EN 50136-1 also IEC 60839-5-1	Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems	2012 A1/2018 2013
EN 50136-2	Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)	2013
EN 50136-3	Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)	2013
EN 50518-1	Monitoring and alarm receiving centres - Part 1: Location and construction requirements	2013
EN 50518-2	Monitoring and alarm receiving centres - Part 2: Technical requirements	2013
EN 50518-3	Monitoring and alarm receiving centres - Part 3: Procedures and requirements for operation	2013
EN 50600-1	Information technology - Data centre facilities and infrastructure - Part 1: General	2012
ISO27001	Information Security Management System	2017

*) 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 "xxxxxxxxxxxxxxxxxxxxxxxxf" **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 Churchillaan 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 (example)

Inspection subjects	Inspection aspects	Inspection method	Inspection frequency	Inspection registration
Infrastructure: - Layout; - Functions - Performance - Security	According scheme	According scheme Design Testing configuration Commissioning Verification Handover Maintenance	Setup Ongoing	According scheme
Maintaining process: - Functions; - Performance; - Security.	According scheme	According scheme Verification Maintenance	Ongoing	According scheme
Management processes: - Quality; - Staff - Corrective actions - Corrective measurements	According scheme	According scheme Verification	Ongoing	According scheme
Measuring and testing equipment - measuring equipment - calibration if applicable				
Information management Confidential Integrity Availability	According scheme	According scheme Verification	Ongoing	According scheme