K21048

Version 3.0

03-12-2020

Secure Remote Access for Remote Services

Defining the behaviour, reliability, resilience and security of remotely accessible products and their enabling chain of entities.

Trust

Quality

Progress

Preface

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

This scheme has been drafted to fill in the gap in requirements existing for security at this moment for the use of applications on mobile devices that access systems remotely through utilization of the internet and digitalization. A basis for the setup in this certification scheme are the existing European standards used in the scope for intrusion and holdup systems and alarm transmission systems since they offer a solid framework for security requirements. The setup in these standards has a proven balanced setup on organisational and technical performance requirements. This creates an advantage making it possible to make use of an existing assessed infrastructure. The goal of this scheme is to use as much of the existing international standards and draft new requirements based on the existing structure. New relevant (inter)national requirements, and/or standards that are published shall be incorporated in this scheme. This scheme shall also be used in conjunction with the Kiwa Regulations for Certification.

Kiwa Nederland B.V.

Kiwa FSS

Dwarsweg 10

5301 KT Zaltbommel

The Netherlands

Tel. +31 88 998 51 00
Info.ncp@kiwa.nl
www.kiwafss.nl

Validation
This evaluation guideline has been validated by the Director FSS Certification and Inspection of Kiwa on 23-10-2019

Contents

1 Introduction

1.1 General

This international certification scheme comprises all the relevant requirements Kiwa applies when dealing with requests for the issue and maintenance of a certificate for products or systems where remote access of systems is utilized, also referred to as smart or IoT systems. Usually, the purpose for this is gaining access and/or executing actions within the physical system or product.

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”. Kiwa is accredited by the RvA in the certification of products according to ISO/IEC 17025 and 17065.

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

This scheme maintains several risk levels for categorizing the severity of the safety of the alarm systems. These risk levels are numbered from 1 until 4. For the risk levels 1, 2 and 3, as defined in chapter 1.5,
2 is applicable according to ISO/IEC 17067:2013.
For the high-risk level, risk level 4, scheme type 5 is applicable according to ISO/IEC 17067:2013.

This scheme shall be used in conjunction with the Kiwa Regulations for Certification and has a module structure based on certification scheme K21035; Electronic Security Certification, as described in: https://www.kiwa.com/nl/en/Products/electronic-security-certification-in-accordance-with-brl-k21035/

1.2 Field of application / scope

The field of application/ scope of this scheme is demarcated by:

- A definition of the behaviour, reliability, resilience and security of the transmission and communication between mobile applications and different types of systems (e.g. a Smart HVAC system, smart lighting system etc.) and receiving and monitoring equipment to ensure their suitability for use.
- A definition of where in the chain of entities the mobile application is used to remotely access the coupled physical system or product to gain access and/or execute actions within the physical system or product to ultimately operate the device remotely.

This scheme is meant to be applicable for the supplier/manufacturer of a system which is remotely accessible which in its turn is subjected to the requirements in this scheme. Ultimately, this system will be operated by an end user.

The aforementioned applications have many areas of use within the scope of remote access for remote services. For example, applications that transmit data together, with, or between different types systems, including alarm systems, HVAC systems, smart valves, smart consumer products, etc. To achieve a certificate for a product according to this scheme several requirements must be met. These requirements include certain thresholds to which the product must adhere to. To achieve these thresholds certain tests or assessments are necessary to be performed as the outflowing results are the deciding factor. The results of these assessments are collected in assessment reports from which the supporting documentation needs to be provided by the client of Kiwa.

This client is the manufacturer or responsible entity of the product that solicits for the certification according to the RARS scheme. An abstract overview of the infrastructure of the remotely accessible product according to this scheme can be seen below. This image is based upon the infrastructure that is found in alarm systems.

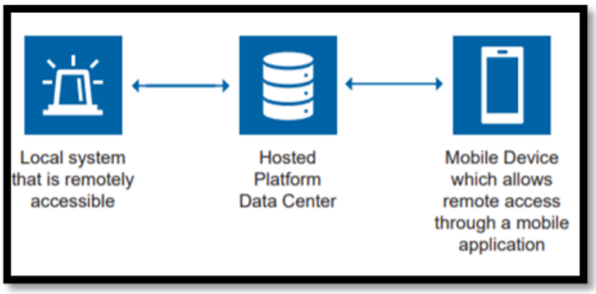

Local system that is remotely accessible
Hosted Platform Data Center
Mobile Device which allows remote access through a mobile application

Figure 1: General overview of alarm systems that utilize hosted platform data centers

Infrastructure

The infrastructure as made clear in the previous figure must adhere to the following standards and guidelines:

- Panels used for interacting with the system according to EN50131
- Connection to hosted Data centre according to EN50136 and EN50518
- Connection to monitoring centre (MC) according to EN50136-1 and EN50518
- The connection between Data centre and the mobile device according to EN50136
- The mobile application according to the mobile application security checklist provided by Kiwa. (Risk Level 1,2,3 use Level 1 of the Mobile Application Security Verification Standard (MASVS) requirements, Risk level 4 uses the MASVS Level 2 requirements and the MASVS reverse engineering requirements)
- The Hosted data centre according to relevant certification and compliance of the provider of the data centre services. If the hosted data centre doesn’t have the required certification(s), Kiwa will audit the cloud provider first.

1.3 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 scheme, the supplier shall prove that these reports have been drawn up by an institution that complies with the applicable accreditation standards, namely:

- EN-ISO/IEC 17020 for inspection bodies;
- EN-ISO/IEC 17021-1 for certification bodies certifying systems;
- EN-ISO/IEC 17024 for certification bodies certifying persons;
- EN-ISO/IEC 17025 for laboratories;
- 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) (Raad voor Accreditatie, 2019) 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.

1.4 Quality declaration by Kiwa

- Meeting all requirements as stated by this document, and the applicable accreditation standards will ultimately result in a certificate of conformity. This certificate confirms the compliance of the remotely accessible product and its enabling chain of entities to the requirements in the certification scheme K21048 “Secure Remote Access for Remote Services”.
- The models of the certificates for this scheme are included in this document is included with this document as the first and second annexes.
- The right to use the Kiwa marking by the certified supplier organisations based on these certification activities, is detailed in chapter 8 of this scheme.

1.5 Risk levels

For the risk levels (which are based on the risk levels in 50131-1) for remote access the following two risk levels are defined:

- Risk level 1,2,3 is applicable for normal risks.
- Risk level 4 is applicable for higher risks.
- The risk level has to be agreed on by the remote access service supplier, client and authorities.

Examples of high risk can be for example:

- *A grade 4 risk level according to EN50131-1.*
- *Situations where life safety is of great importance.*
- *Losses that are expected to be more than 2 million Euros.*

Additional remarks:

- Doing a risk assessment itself is out of scope for this document.
- Risk management for information security is defined in ISO 27005.
- Risk assessments should be done at least yearly.

2 Terms and Definitions

2.1 Definitions

In this scheme, the following terms and definitions apply:

- **Board of Experts**: The Board of Experts Security. This board consists of members that all fulfil different but necessary roles to ultimately make the appropriate decision regarding a product.

- **Application**: Remote Access Terminal (RAT): The software and/or hardware used to gain remote access to functions of one or more systems. See EN50136-10 for further information.

  Note: If a panel is mentioned it is assumed it performs the same functionality as explained for an application.

- **Certification mark**: a protected trademark of which the authorization of the use is granted by Kiwa, to the supplier whose products / process / services can be considered to comply on delivery with the applicable requirements.

- **Certification Scheme**: the agreements made within the Board of Experts on the subject of certification within this international TIC -scheme.

- **Conditions**: for the function of a remote access application certain conditions are needed. These conditions can be for example organisation requirements for the use in conjunction with an intruder and holdup alarm system.

- **Hosted web platform:** Platform as a Service (PaaS) or Application Platform as a Service (aPaaS) or platform-based service is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

- **Inspection tests**: tests carried out after the certificate has been granted in order to ascertain whether the certified products / processes and services continue to meet the requirements recorded in this scheme in conjunction with the factory production controls.

- **IQC scheme (IQCS):** a description of the quality controls carried out by the supplier as part of his quality system also named internal quality plan per scope.

- **Initial investigation**: tests in order to ascertain that all the requirements recorded in this scheme guideline are met.

- **Manufacturer:** party that manufactures a product or a system or who has a product or a system designed or manufactured, and markets that product or system under his name or trademark or uses the product for his own purposes**.**

- **Marking:** a marking affixed by the supplier on its products, processes or services based on the requirements in this scheme.

- **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.

- **Product:** A system that is remotely accessible of which the remote access is enabled by a chain of entities.

- **Product certificate**: a document in which Kiwa declares that a product may, on delivery, be deemed to comply with the product specification recorded in the product certificate.

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

- **Remote Access Service Provider (RASP): a** person or an entity that is responsible for design, operation and the security of the remote access infrastructure. See EN50136-10 for further information. The perimeters within which the RASP operates are restricted by the scope in section 2.1.

- *Note 1 to entry: The RASP may take responsibility for the RASP provision and security monitoring of the remote access infrastructure as the design authority, through contracts with customers, ARCs, transmission network operators, etc.*

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

3 Procedure for Granting a Product Certificate

3.1 General

This chapter elaborates on the different phases of the process for granting a certificate of conformity according to this scheme.

3.2 Initial investigation

The initial investigation to be performed are 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 performance / functional requirements;
- production process assessment (if applicable according to threat level);
- assessment of the quality system and the IQC-scheme;
- assessment on the presence and functioning of the remaining procedures regarding the product.

3.3 Granting the 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 specifying the product's compliance can be granted or if additional data and/or tests are necessary. The issued certificate expires after three years. There will be at least one yearly re-assessment to conclude the conformity of the product according to the K21048. This is explained in more detail in chapter 6.2.

3.4 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 when necessary and applicable.

3.5 Process assessment

When assessing the process, it is investigated whether the manufacturer is capable of continuously producing products that meet the certification requirements. The evaluation of the production process takes place during the ongoing work at the manufacturer. This is according to the level definition based on scheme type 2 or 5 as mentioned in section 1.1.

3.6 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 manufacturer.
- This written agreement, which must be available for Kiwa, includes at least a statement that the supplier has total control over the product and has an agreement with the manufacturer that lets the supplier behave as it if were the owner of the product. With this the supplier takes full responsibility for the product.
- Accreditation bodies and scheme managers will be given the opportunity to observe the certification activities carried out by Kiwa. Furthermore, Kiwa, accreditation bodies and scheme managers will also be given the opportunity to observe the certification activities on behalf of Kiwa at the location of the manufacturer or user of the product.

4 Requirements for the Product

4.1 General

This chapter contains the requirements that the product shall have to fulfil to achieve the certificate of approval by Kiwa. These requirements are valid for security level 1,2 and 3. For level 4 there is an additional on-site audit scheme which will be performed by Kiwa. Annex IV gives the deliverables and explanation per requirement. It can be consulted for getting an understanding of what documents are expected by Kiwa for a proper assessment of the product.

The requirements listed in this chapter and in Annex III are specific mobile security requirements that are intended to connect to a broad range of products that utilize remote access. The specific requirements for level 4 are also mentioned in this annex. However, some products have industry specific requirements that need to be met in order to ensure secure remote access. These specific requirements per type of industry/ product can also be found in the annexes of this document. Annex V for example elaborates on additional requirements for remotely accessible alarm systems.

4.2 Regulatory requirements

Not applicable.

4.3 Use and access levels of the application

- The application shall connect through the Data Centre (DC) to the panel or mobile application of the remotely accessible system, if a panel is part of the architecture (e.g. Intrusion & Holdup Alarm System I&HAS, smart lightning system etc.). This infrastructure has been chosen to implement a secure connection by the hosted platform to the security system.
- The application requires a logical access level 2 on the (mobile) smart device according to EN50131-1.
- The mobile application shall enforce setting-up a new password code after first installation by the user.
- The panel of the system, if there is one, (e.g. I&HAS, Fire- and Social Alarm Systems) shall connect to a secure hosted web platform through the internet.
- The application requirement for access by the panel, if there is one, is a logical access level 3 according to EN50131-1.

4.4 Connections of the application

- The application shall have a secure confidential connection to the panel, if there is one, of the system (e.g. I&HAS, Fire and Social Alarm Systems) and meet the key management requirement of TLS1.2 or higher if it is known that the security level is insufficient, or other accepted best industry practices for encryption when a mobile network connection is used.
- Cryptographic 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 standard ISO/IEC 18033 shall also be applied for non-repudiation.
- The cryptographic algorithms shall meet the updated list of SSL labs or better. See https://www.ssllabs.com/
- The minimal checking frequency is every half year or during periodic penetration testing to ensure the cryptographic algorithms meet the list of SSL labs. This shall be conducted by the manufacturer and/or supplier.

4.5 Acknowledgment (un)setting

- The setting made by means of the application shall be acknowledged by the panel of the system, if there is one, (e.g. I&HAS, Fire- and Social Alarm Systems) and the hosted web platform.
- The setting made by means of the hosted web platform shall be validated and then acknowledged by the panel, if there is one, of the remotely accessible product and the application of the smart mobile device.
- By these acknowledgements the status of the overall system is reflected.
- This process shall have a failsafe mechanism built in; 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.

4.6 Authenticity

- The definitions and processes of ISO/IEC 29115 shall be applied.
- The LoA3 scheme from ISO/IEC 29115 shall be defined in the process of getting first access (onboarding) as an account to the application, to the host and the panel of the remotely accessible product.
- The process by the supplier shall obtain minimal 2 factor authentication (2FA). The application shall restrict a limited time within 2 factor authentication process.
- The requirements for access level according to EN50131-1 for the application on the mobile device shall be the same as to the panel of the remotely accessible product.
- The requirements giving more users access to the application are the same as for the panel of remotely accessible product.
- For applications that require different level of access, Role Based Access Control should be applied.
- It is allowed to use biometrics according to latest standards according the standardisation group ISO/IEC JTC 1 SC 37 on Biometrics.

4.7 Accountability

- The hosted web platform and the application shall apply logging.
- The minimal time of storing the logging for the hosted web platform and the application is 6 months or more if defined based on the grade according to EN50131-1.
- The data in transmission and stored needs proper encryption according to the standards EN50136-1 and EN50518.

4.8 Time restrictions

- 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 (dis)arming) the panel.
- Process 1: if a user has access at level 2; a maximum time has to be applied before the application closes.
- Process 2: If the application is opened at level 1 and a code for access at level 2 or higher was filled in, the maximum time before the application will close will be applied.
- Protection against hostile access (brute force) to the application within the secure functions shall be at least in the testing stage of the application by means of penetration testing the application.

4.9 Instructions by the application towards the user

The application shall warn and instruct the user if the usage of the application is outside the grading requirements of EN50131-1. Privacy and security issues resulting from usage of the application outside the safe perimeters of the physical location of the remotely accessible product are not the responsibility of the manufacturer/ supplier but the responsibility of the end user.

5 Testing the Product

5.1 General

- This chapter contains the standards with the requirements for testing activities performed by Kiwa to determine the performances that the systems must fulfil.
- These tests are necessary if there is no integer and reliable information available according to relevant standards by accredited approval bodies such as test laboratories fulfilling the requirements ISO17025 “General requirements for the competence of testing and calibration laboratories”.
- If this is the case, Kiwa shall then execute third party witnessing of the tests according to ISO17065 “Conformity assessment - Requirements for bodies certifying products, processes and services”.

5.2 Functional testing

The functional testing of the product as is elaborated on in chapter 5.3 of these schemes shall be performed at the laboratories of Kiwa or at the site of the manufacturer under supervision of an expert of Kiwa. The testing shall be performed in the end-to-end situation in a laboratory situation.

5.3 Functional Security Assessment

- The security testing of the code is based on minimal requirements in “The Ten Most Critical Web Application Security Risks” and “Mobile Application” according to the latest OWASP rules, explained at https://www.owasp.org/. The specific tests are also described in annex III.
- The code of the application shall be tested according the latest applicable version of these rules and for the infrastructure layer. The testing shall be performed in the end-to-end situation in a production situation. This means all the components like the Supervised Premises Transceiver (SPT) & the Receiving Centre Transceiver (RCT) and Mobile Device will be undergoing tests.
- The report shall define the used tools for testing and the version of the tools.

The following points give an indication for the knowledge of the tester:

- Affinity and experience with code development and experience in the programming language used for the specific (web) application;
- Fluency in the operation of IDEs;
- Affinity and experience with mobile/web application development;
- Level of general knowledge and experience of code development and/or testing (approximately 4 years);
- Level of specific knowledge and experience of the code (approximately 2 years) *if possible*;
- Level of specific knowledge and experience of the latest OWASP rules based of the applicable specific “Vulnerability Subcategories” (approximately 2 years) ;
- Experience in Secure coding practices;
- Knowledge;
- Affinity and experience with code development and experience in the programming language used for the specific (web) application;
- Fluency in the operation of IDEs;
- Affinity and experience with mobile /web application development;
- Level of general knowledge and experience of code development and/or testing (approximately 4 years);

- Level of specific knowledge and experience of the code (approximately 2 years) *if possible*;
- Level of specific knowledge and experience of the latest OWASP rules based of the applicable specific “Vulnerability Subcategories” (approximately 2 years);
- Experience in Secure coding practices.

6 Requirements for the Secure Code Development Process

6.1 General

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

6.2 Process requirements for development

- The process shall fulfil the requirements of “A.14.2 Security in development and support processes” of ISO 27001 or the IEC 62443-4-1.
- The manufacturer shall have an certificate which was issued by a Notified Body according to the above mentioned standards for this activity or this process and it shall be assessed by an expert of Kiwa.
- Based on this process, the (re) developed code shall be tested. Updates shall be tested with a minimal frequency of 1 per year based on chapter 5.3 of this scheme or more frequent if need be, based on the risk assessment by the manufacturer.

  In this process the minimal stages are:
  - Development
  - Testing
  - Acceptation
  - Production

- All of the stages will be separated with only the required levels of access.

7 Requirements for Assessments

7.1 General

This chapter contains the requirements for assessments by Kiwa of the manufacturers and/or suppliers to determine the quality of the products have to fulfil.

7.2 Assessment by the manufacturer and/ or supplier and Kiwa

- The quality system of the suppling manufacturer will be assessed by Kiwa on the basis of the IQC scheme / Quality plan.
- The assessment contains at least those aspects mentioned in the Kiwa Regulations for Certification and the requirements of the applicable standards.
- The quality system of the manufacturer and/or supplier shall be audited internally at least once a year.
- The quality system of the manufacturer and/or supplier shall be assessed by Kiwa at least once a year.
- The manufactured products shall be inspected internally by the supplier.
- Kiwa shall make a high level structure checklists based on this scheme. These checklists are based on the matching OWASP guideline for checklists that will be applied to the application during testing. Furthermore, the type of assessment will be considered.

With section 1.5 of this scheme as reference the following assessments/ audits will be performed:

- For risk levels 1, 2, or 3 an off-site audit will be performed.
- For risk level 4 an additional market surveillance will be performed.

7.3 Surveillance activities

As stated in the previous section risk levels 4 requires an additional market surveillance. This is done at least once a year. The amount of times this happens depends on the outcomes of the analysis as stated in chapter 9.4. If there were to be a major update a market surveillance will be performed. During the market surveillance the following points are important:

- The main goal of the market surveillance is to confirm that the product available on the market complies to the requirements for the K21048 by Kiwa compared to the device assessed by Kiwa;
- The make sure a product available to customers is tested and to see if it fulfils the requirements as written in chapter 4, 5, and Annex 4. Annex 3 is applicable when a mobile app is also available;
- It is not necessary that all the requirements are rechecked by Kiwa for the market surveillance. The requirements are chosen by the assessor of Kiwa based on the checklists mentioned in clause 1.2;
- If the product passes the market surveillance no additional actions are needed to be taken. Otherwise Kiwa will communicate what additional actions are required to correct any detected deviations.

8 Marking

8.1 General

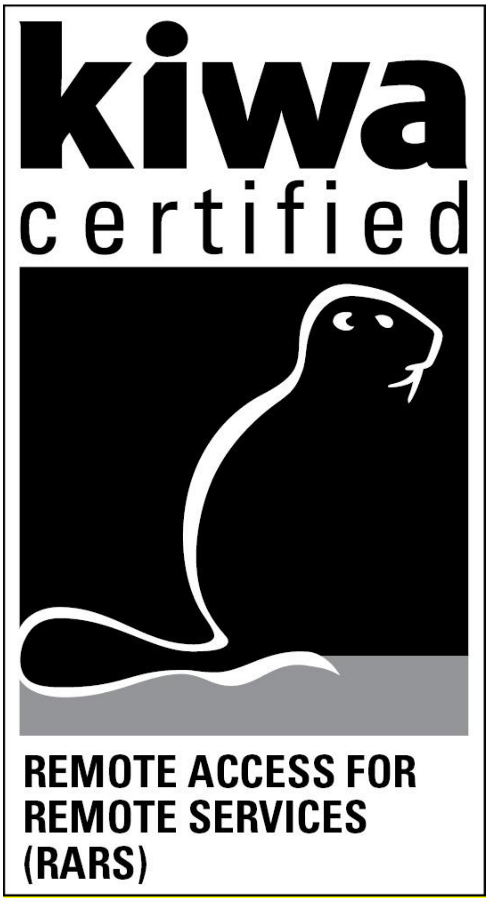
The systems and products shall be marked with a declaration of conformity according the certification part of this scheme and applicable standards. The declaration shall contain at least following information:

- 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. To keep making use of the mark a product has to adhere to requirements of the rules of certification by Kiwa. This can be found here.

8.2 Certification mark

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



9 Requirements with Respect to the Quality System

9.1 General

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

9.2 Manager of the quality system

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

9.3 Internal quality control / quality plan

The supplier shall have an internal quality control scheme (IQC scheme) which is applied by him. The following must have been demonstrably recorded in this IQC scheme:

- what aspects are checked by the producer;
- 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.

9.4 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.
- Whenever updates to either the OWASP or the product itself takes place the manufacturer needs to perform a risk analysis of the possible impact of these changes. Based on the outcome the re-assessment will be initiated.

10 Summary of Tests and Inspections

10.1 General

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 scheme 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 scheme;
- **inspections and audits of the quality system of the supplier:** monitoring compliance of the IQC scheme and procedures.

10.2 Test, inspection and audit matrix

Description of requirement	Article no. scheme	Tests within the scope of:	
		Pre-certification	Inspection by Kiwa after granting of certificate [a,b)]
Process requirements			
Per applicable scope a)	4	x	x
Testing performance of the systems			
If needed per applicable scope	5	x	x
Factory production control components			
If needed per applicable scope b)	6	x	x
Quality system and Certification mark			
	8 & 9	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 manufacturer and/or supplier in the presence of the inspector. In case this is not possible, an agreement will be made between the certification body and the manufacturer and/or supplier about how the inspection will take place. The frequency of inspection visits is defined in chapter 7.2 of this scheme.

10.3 Supplier Inspection of the quality system

The quality system of the suppling manufacturer will be checked by Kiwa on the basis of the IQC scheme / Quality plan.

The inspection contains at least those aspects mentioned in the Kiwa Regulations for Certification and the requirements of the applicable standards.

10.3.1 Auditing the quality system of the supplier

The quality system of the supplier shall be audited internally by the suppliers at least once a year.

The quality system of the supplier shall be assessed external by Kiwa at least once a year.

10.3.2 Inspecting the output of the process of the supplier

The process shall be inspected internally by the supplier according to the IQC scheme / Quality plan.

11 Agreements on the Implementation of Certification

11.1 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 tests 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.

11.2 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.

11.2.1 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
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 lab / inspection 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** • 1 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**)

11.2.2 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**.

11.3 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 made verifiable.;
- basis for decision: the **DM** shall be able to base his decision on the findings included in the report.

11.4 Decision for granting the certificate

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

11.5 Layout of quality declaration

The product certificate shall be in accordance with the model included in the Annex 1.

11.6 Nature 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 program on site shall cover at least:

- the product requirements;
- the production process;
- the suppliers IQC scheme and the results obtained from inspections carried out by the supplier;
- the correct way of marking certified products;
- compliance with required procedures;
- handling complaints about products delivered.

For suppliers with a private label certificate the frequency of audits amounts to one audit per two years. These audits are conducted at the site of the private label certificate holder. The audits are conducted at the site of private label holder and focussed on the aspects inserted in the IQC scheme and the results of the control performed by the private label holder. The IQC scheme of the private label holder shall refer to at least:

- the correct way of marking certified products;
- compliance with required procedures for receiving and final inspection;
- the storage of products and goods;
- handling complaints.

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

11.7 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, and the manufacturer will be informed.
The Sanctions Policy is available through the “News and Publications” page on the Kiwa website "Kiwa Regulation for Certification".

11.8 Report to the Board of Experts

The 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.

11.9 Interpretation of requirements

The Board of Experts may record the interpretation of requirements of this certification scheme in one separate interpretation document in annex III of this scheme.

11.10 Specific rules set by the Board of Experts

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

12 Titles of Standards

12.1 Public law rules

Not applicable

12.2 Standards / normative documents

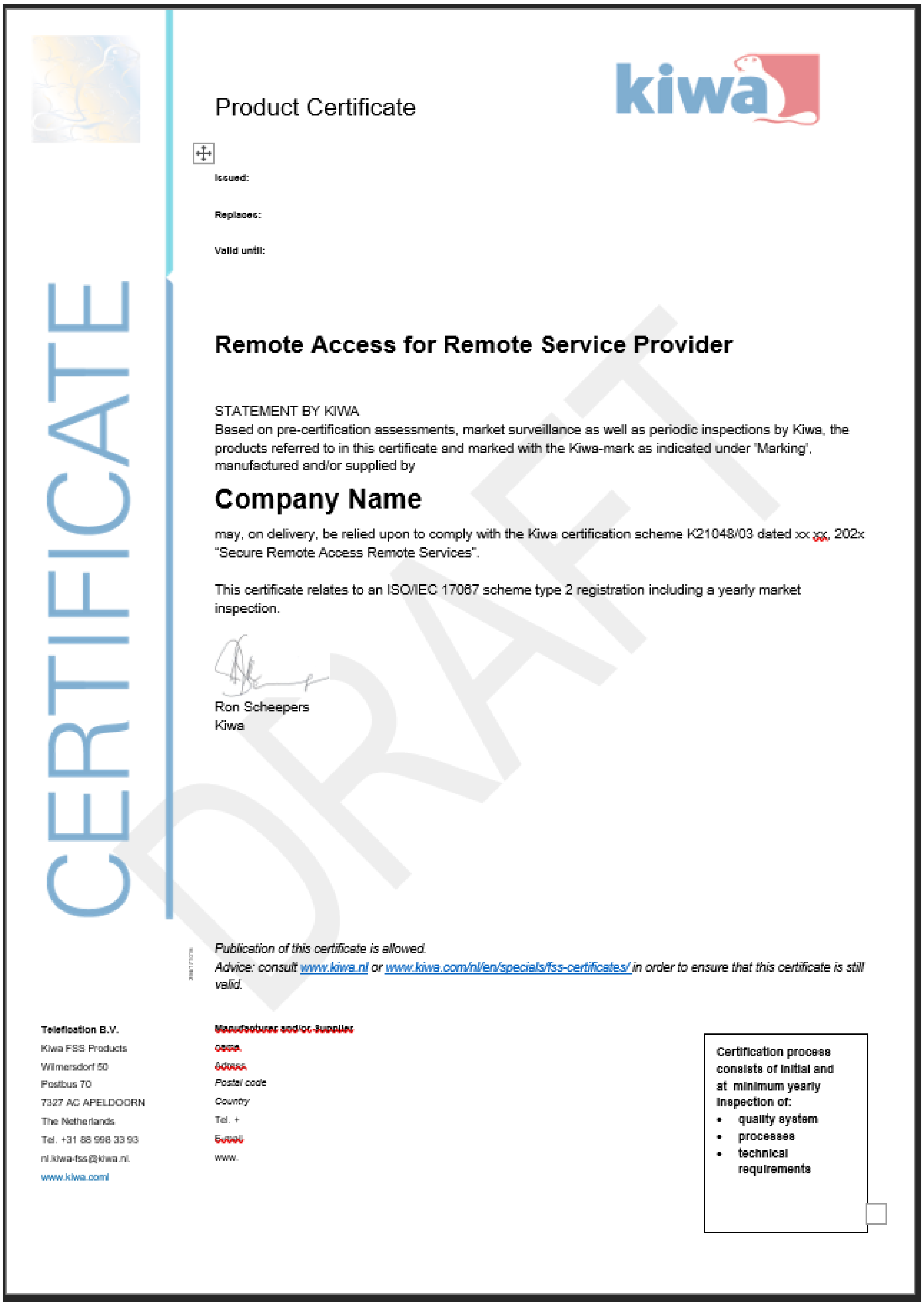
Number	Title	Version*
EN ISO/IEC 17020	Conformity assessment - General criteria for the operation of various types of bodies performing inspection	
EN ISO/IEC 17021	Conformity assessment - Requirements for bodies providing audit and certification of management systems	
EN ISO/IEC 17024	Conformity assessment - General requirements for bodies operating certification of persons	
EN ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories	
EN ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services	
EN ISO/IEC 17067	Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes	
EN 50131-1	Alarm systems - Intrusion and hold-up systems - System requirements	
IEC 60839-5-1	Alarm and electronic security systems - Alarm transmission systems - General requirements	
EN 50136-1	Alarm systems. Alarm transmission systems and equipment. General requirements for alarm transmission systems	
EN 50518	Monitoring & Alarm Receiving Centres	
ISO 27001	Information technology - Security techniques - Information security management systems – Requirements	
EN 50600	Information technology - Data centre facilities and infrastructures - General concepts	
ISO/IEC 11770-1/2/3	Information technology -- Security techniques -- Key management	
ISO/IEC 18033-1	Information technology -- Security techniques -- Encryption algorithms -- General	
IEC 29115	Information Technology – Security techniques – Entity authentication assurance framework	
IEC 62443-4-1	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.	
ISO/IEC JTC 1 SC 37	Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies;	

methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.

Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protections techniques, biometric security testing, evaluations and evaluations methodologies.

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

I Annex - Model certificate 1(example)



CERTIFICATE

Product Certificate

Issued:

Replaces:

Valid until:

Remote Access for Remote Service Provider

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

Company Name

may, on delivery, be relied upon to comply with the Kiwa certification scheme K21048/03 dated xx xx, 202x "Secure Remote Access Remote Services".

This certificate relates to an ISO/IEC 17067 scheme type 2 registration including a yearly market inspection.

Ron Scheepers
Kiwa

DRAFT

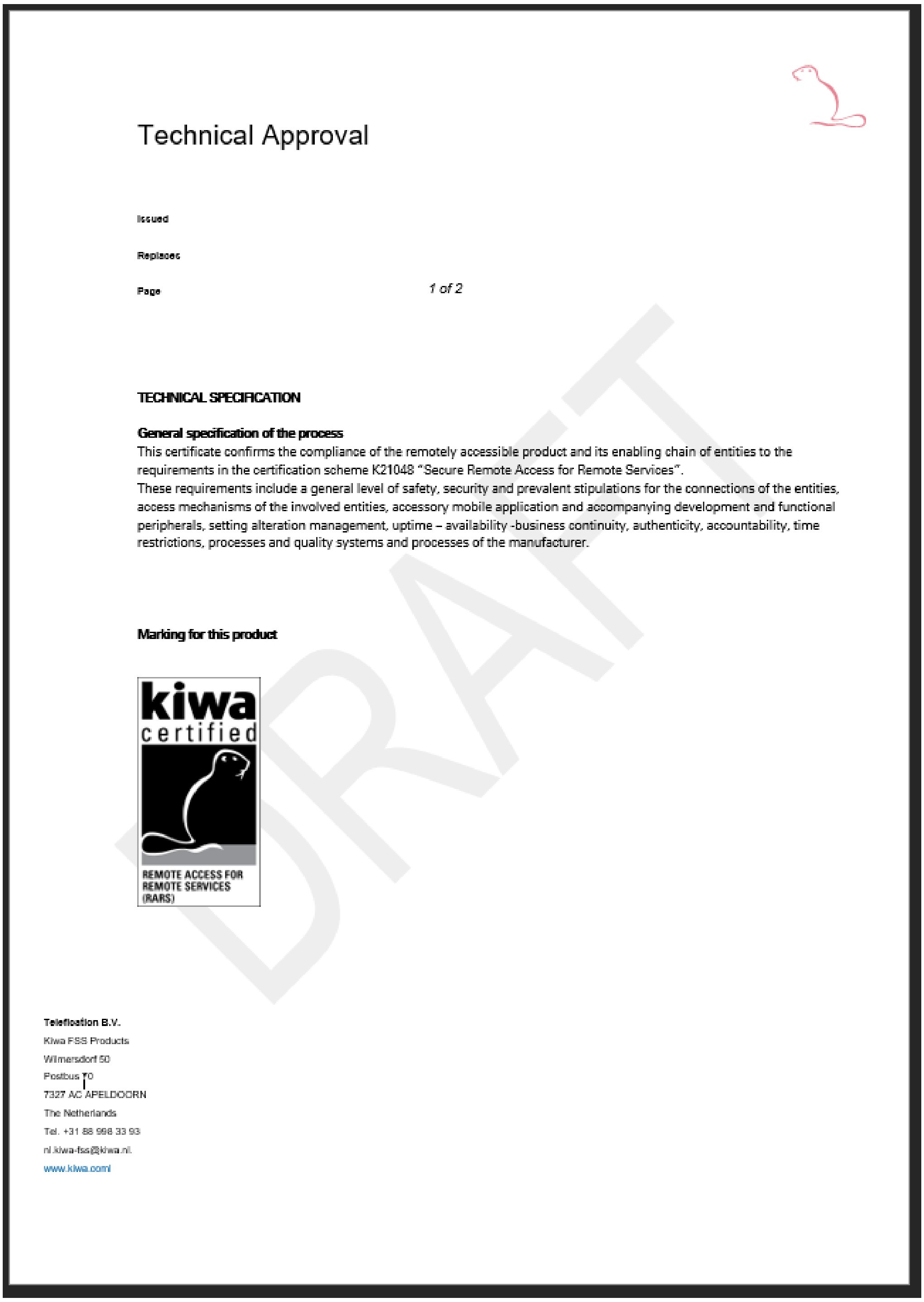
Publication of this certificate is allowed.
Advice: consult www.kiwa.nl or www.kiwa.com/nl/en/specials/fss-certificates/ in order to ensure that this certificate is still valid.

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl.
www.kiwa.com/

Manufacturer and/or Supplier
name
Adress
Postal code
Country
Tel. +
E-mail
www.

Certification process consists of initial and at minimum yearly inspection of:

- **quality system**
- **processes**
- **technical requirements**



Technical Approval

Issued

Replaces

Page 1 of 2

TECHNICAL SPECIFICATION

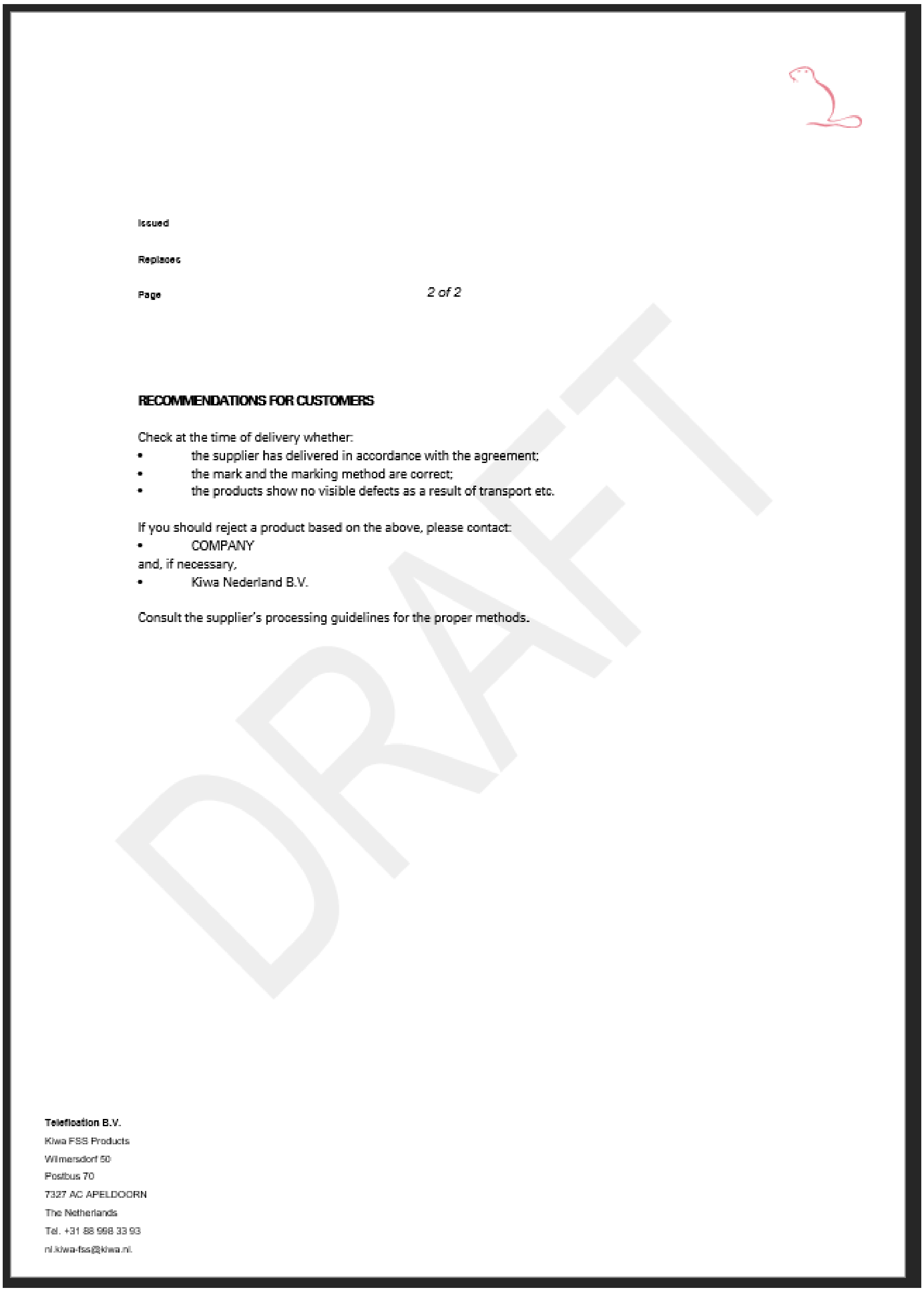
General specification of the process

This certificate confirms the compliance of the remotely accessible product and its enabling chain of entities to the requirements in the certification scheme K21048 "Secure Remote Access for Remote Services".
These requirements include a general level of safety, security and prevalent stipulations for the connections of the entities, access mechanisms of the involved entities, accessory mobile application and accompanying development and functional peripherals, setting alteration management, uptime – availability -business continuity, authenticity, accountability, time restrictions, processes and quality systems and processes of the manufacturer.

Marking for this product

kiwa
certified
REMOTE ACCESS FOR
REMOTE SERVICES
(RARS)

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl.
www.kiwa.coml



Issued

Replaces

Page 2 of 2

RECOMMENDATIONS FOR CUSTOMERS

Check at the time of delivery whether:

- the supplier has delivered in accordance with the agreement;
- the mark and the marking method are correct;
- the products show no visible defects as a result of transport etc.

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

- COMPANY

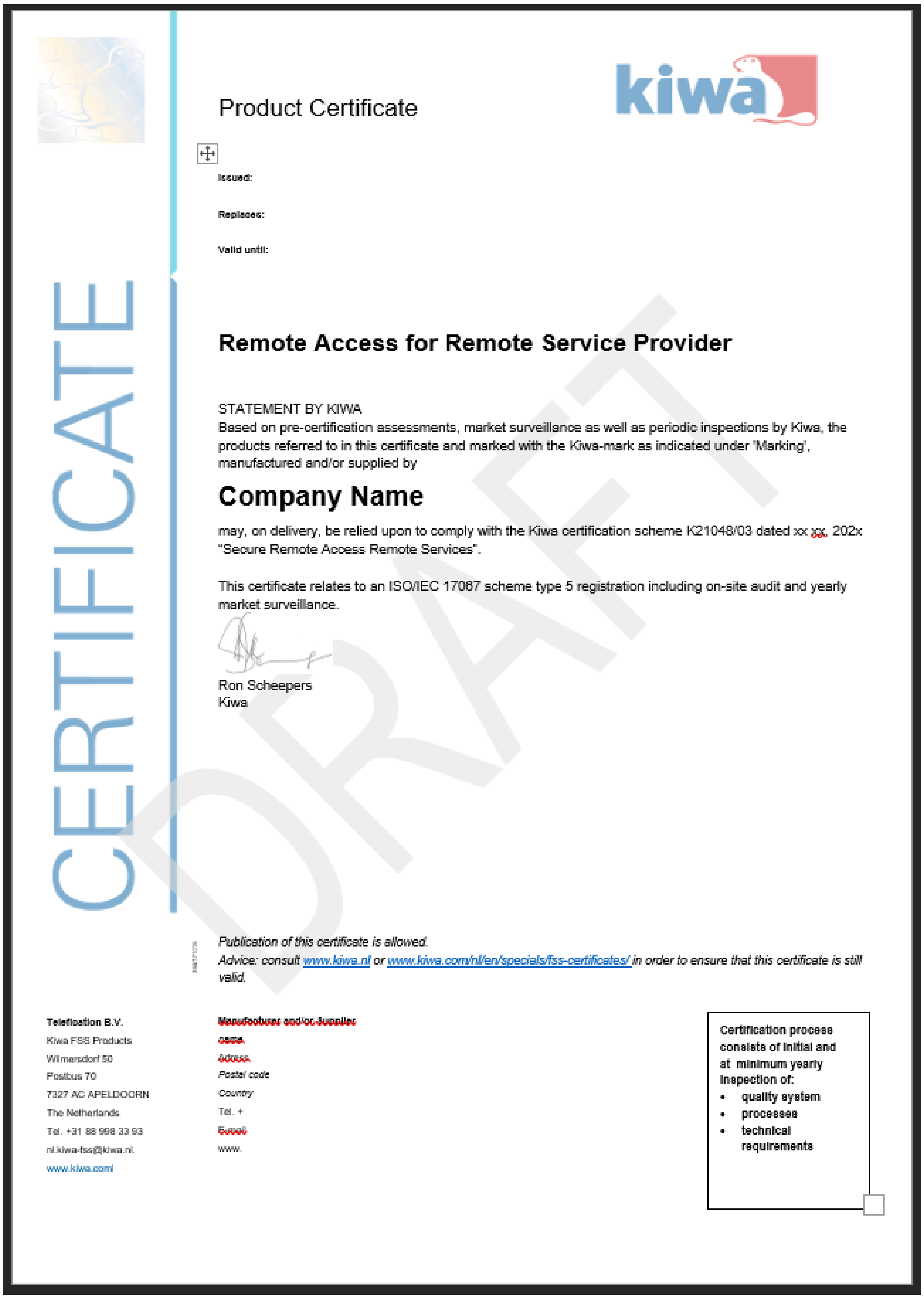
and, if necessary,

- Kiwa Nederland B.V.

Consult the supplier's processing guidelines for the proper methods.

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl

II Annex - Model certificate 2(example)



CERTIFICATE

Product Certificate

kiwa

Issued:

Replaces:

Valid until:

Remote Access for Remote Service Provider

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

Company Name

may, on delivery, be relied upon to comply with the Kiwa certification scheme K21048/03 dated xx xx, 202x "Secure Remote Access Remote Services".

This certificate relates to an ISO/IEC 17067 scheme type 5 registration including on-site audit and yearly market surveillance.

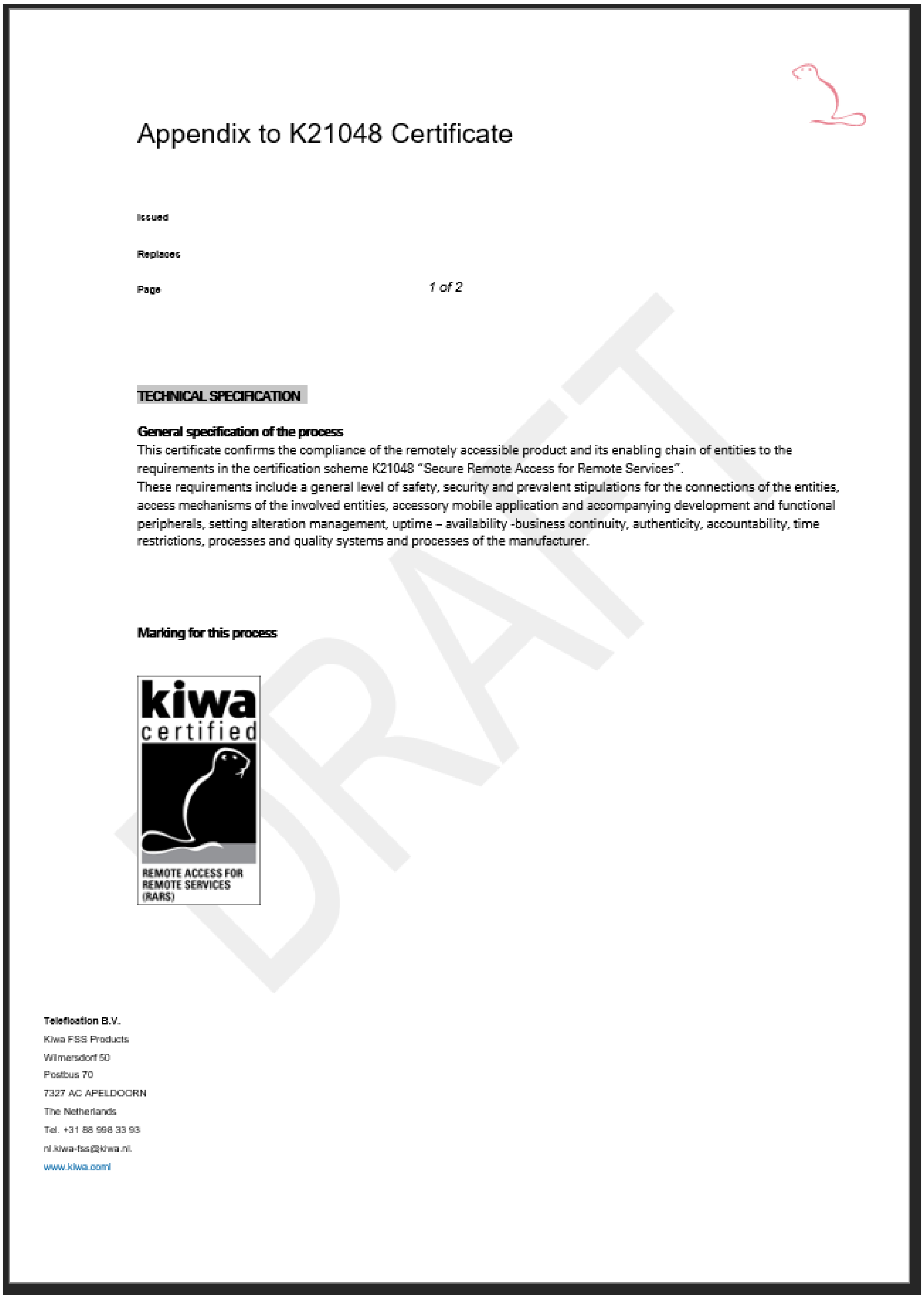
Ron Scheepers
Kiwa

Publication of this certificate is allowed.
Advice: consult www.kiwa.nl or www.kiwa.com/nl/en/specials/fss-certificates/ in order to ensure that this certificate is still valid.

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl
www.kiwa.com/

Manufacturer and/or Supplier
name
Adress
Postal code
Country
Tel. +
E-mail
www.

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



Appendix to K21048 Certificate

Issued

Replaces

Page 1 of 2

TECHNICAL SPECIFICATION

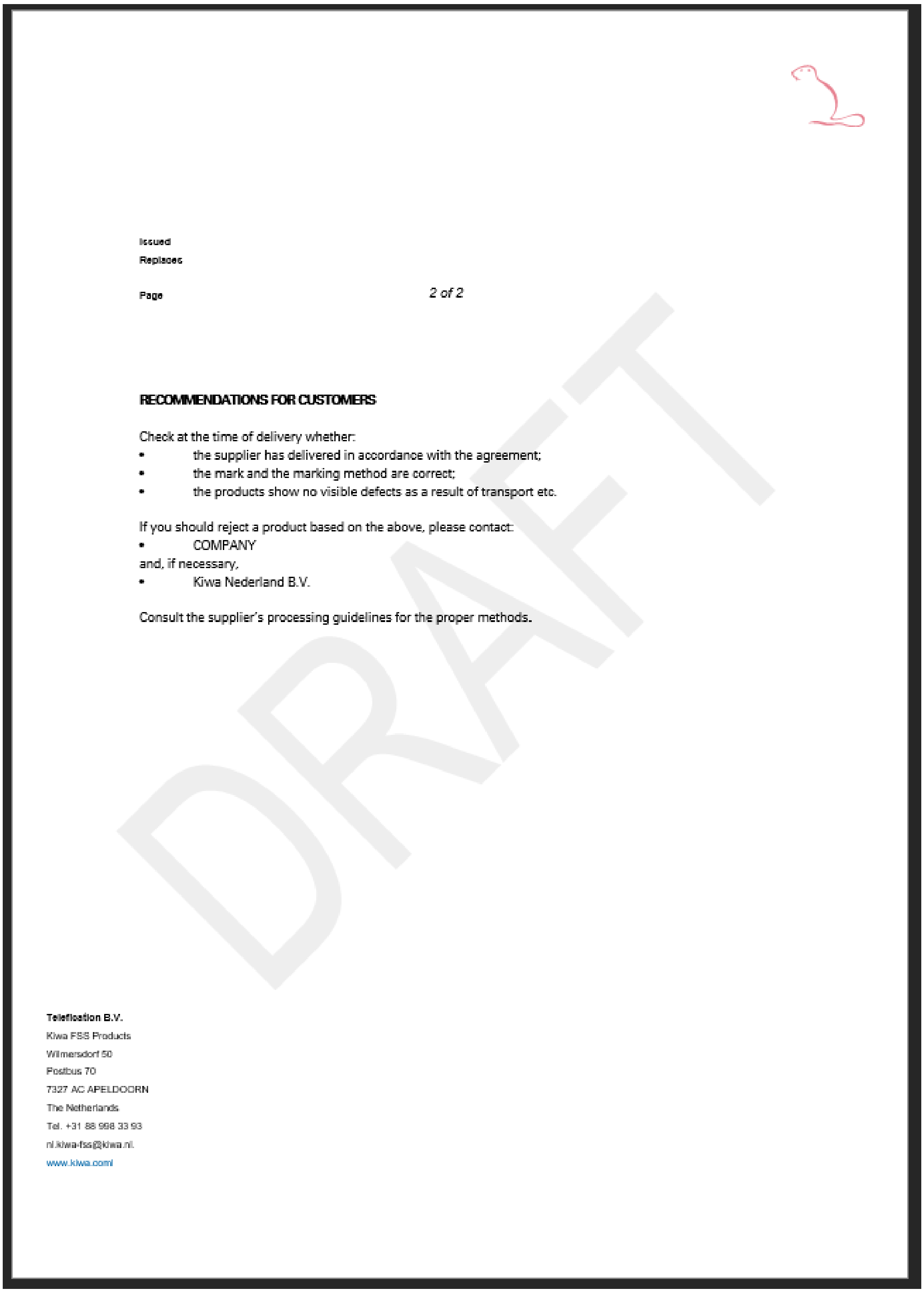
General specification of the process
This certificate confirms the compliance of the remotely accessible product and its enabling chain of entities to the requirements in the certification scheme K21048 "Secure Remote Access for Remote Services".
These requirements include a general level of safety, security and prevalent stipulations for the connections of the entities, access mechanisms of the involved entities, accessory mobile application and accompanying development and functional peripherals, setting alteration management, uptime – availability -business continuity, authenticity, accountability, time restrictions, processes and quality systems and processes of the manufacturer.

Marking for this process

kiwa certified

REMOTE ACCESS FOR REMOTE SERVICES (RARS)

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl.
www.kiwa.coml



Issued
Replaces

Page 2 of 2

RECOMMENDATIONS FOR CUSTOMERS

Check at the time of delivery whether:
- the supplier has delivered in accordance with the agreement;
- the mark and the marking method are correct;
- the products show no visible defects as a result of transport etc.

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

and, if necessary,
- Kiwa Nederland B.V.

Consult the supplier's processing guidelines for the proper methods.

Telefication B.V.
Kiwa FSS Products
Wilmersdorf 50
Postbus 70
7327 AC APELDOORN
The Netherlands
Tel. +31 88 998 33 93
nl.kiwa-fss@kiwa.nl.
www.kiwa.coml

III Annex – Vulnerability assessment and security assessment of applications

Abbreviations:
MSTG – Mobile security Testing Guide
DPIA – Data Protection Impact Assessment
PII – Personally Identifiable Information
IPC – Inter-Process Communication
API – Application Programming Interface
SDK – Software Development Kit
(Session) ID - Identification
HTTPS – Hyper-Text Transfer Protocol Secure
JWT – Json Web Token.
HMAC - Hash-based message authentication code
OWASP – Open Web application Security Project
JTI – Json Token ID
2FA – Two-Factor Authentication
IP – Internet Protocol
TLS – Transport Layer Security
IANA – Internet Assigned Numbers Authority
CA – Certificate Authority
SMS – Short Messaging System
URL – Uniform Resource Locator
UI – User Interface
HTML – HyperText Markup Language
NDK – Native Development Kit
PIE – Position-Independent code
CPP – C Plus Plus file
.H – Header file
.C – C file

I.1 The Mobile Application

- The mobile application is intended to be used on general (mobile) smart devices.
- The mobile application shall have a secure connection to the hosted web platform (according to IEC 60839-5-1 (EN50136-1).
- The app will at least comply with all Level 1 requirements from the newest OWASP Mobile Application Security Verification Standard (MASVS->L1) for risk level1-3. For risk level 4, the reverse engineering requirements and Level 2 requirements are also mandatory (e.g. applicable to a risk level /security grade 4 alarm system)*

*Compliance to these requirements can also be shown based on an accredited mobile app penetration testing report, or depending on the risk level, a complying OWASP app report for the MASVS that has at least the Level 1 (or all) requirements covered.

When a requirement is marked green in the table below, they are only necessary for a risk level 4 assessment. All the other requirements are valid for grades 1,2,3 (scheme type 5).

Annex III.1	The mobile application (android)	
MSTG-ARCH-1: All app components are identified and known to be needed.	An architectural overview of the app with identification of all app components and their use. (also see MSTG-ARCH-3)	Documentation/ architectural diagrams.
MSTG-ARCH-2: Security controls are never enforced only on the client side, but on the respective remote endpoints.	Proof that security controls are never enforced only on the client side but on the respective endpoint.	
MSTG-ARCH-3: A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	A high-level architecture for the mobile app and all connected remote services, with the addressing of security in that architecture.	
MSTG-ARCH-4: Data considered sensitive in the context of the mobile app is clearly identified.	A data identification process, with the identification of sensitive data that the app processes or will be processed externally.	
MSTG-ARCH-5: All app components are defined in terms of the business functions and/or security functions they provide.	A rationale of all the app components with the definitions of business functionality and or the security functions that they provide.	
MSTG-ARCH-6: A threat model for the mobile app and the associated remote services has	The threat model where the app and associated services has been produced and that it identifies potential threats and countermeasures.	The threat model

been produced that identifies potential threats and countermeasures.		
MSTG-ARCH-7 All security controls have a centralized implementation.	Proof of the centralized implementation of the security controls.	
MSTG-ARCH-8: There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.	Proof of the policy for cryptographic key management, and how the lifecycle of the cryptographic keys is enforced.	
MSTG-ARCH-9: A mechanism for enforcing updates of the mobile app exists.	Proof that the app updates can be enforced.	
MSTG-ARCH-10: Security is addressed within all parts of the software development lifecycle.	A description of the software development in place at the manufacturer.	
MSTG-ARCH-11: A responsible disclosure policy is in place and effectively applied.	Proof of the responsible disclosure set into place by the manufacturer and the responsible party. Either through: - /.well-known/security.txt file - A link on the home page of the website	
MSTG-ARCH-12: The app should comply with privacy	Relevant documentation for the compliance with privacy laws and regulations.	Compliance documentation, and

<table>
<tr><td>laws and regulations.</td><td></td><td>possibly a DPIA for the app that processes PII</td></tr>
<tr><td>MSTG-STORAGE-1: System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.</td><td>Documentation that system credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.</td><td></td></tr>
<tr><td>MSTG-STORAGE-2: No sensitive data should be stored outside of the app container or system credential storage facilities.</td><td>Proof that no sensitive data is stored outside of the app container or system credential storage facilities.</td><td></td></tr>
<tr><td>MSTG-STORAGE-3: No sensitive data is written to application logs.</td><td>Screenshots of: checks of the apps' source code for logging mechanisms by searching for the following keywords:
• Functions and classes, such as:
○ android.util.Log
○ Log.d | Log.e | Log.i | Log.v | Log.w | Log.wtf
○ Logger
• Keywords and system output:
○ System.out.print | System.err.print
○ logfile
○ logging
○ logs</td><td></td></tr>
<tr><td>MSTG-STORAGE-4: No sensitive data is shared with third parties unless</td><td>A screenshot of the permissions for the third-party libraries. **implement source code api calls and third-party library functions or sdk in proof**</td><td></td></tr>
</table>

it is a necessary part of the architecture.		
MSTG-STORAGE-5: The keyboard cache is disabled on text inputs that process sensitive data.	Proof that code for all input fields that take sensitive information have the xml attribute keyboardcache set to textNoSuggestions.	
MSTG-STORAGE-6: No sensitive data is exposed via IPC mechanisms.	Android manifest: - if android:exported is set to true, provide kiwa with the read/write permissions that are set - proof that data is protected by the android:permission tag - Proof that the android:protectionLevel attribute has the value signature Source code checks on: - Android.content.Contentprovider - Android.database.cursor - Android.database.sqlite - .query - .update - .delete	
MSTG-STORAGE-7: No sensitive data, such as passwords or pins, is exposed through the user interface.	Proof of the following attribute in the definition of EditText: android:inputType="textPassword"	
MSTG-STORAGE-8: No sensitive data is included in backups generated by the mobile operating system.	Proof of the android manifest: android:allowbackup="false" Proof of dynamic analysis by running adb backup -apk -nosystem <package-name>	

MSTG-STORAGE-9: The app removes sensitive data from views when moved to the background.	Proof of whether the FLAG_SECURE option has been set. It should state something similar to the following code snippet:
	
	getWindow().setFlags(WindowManager.LayoutParams.FLAG_SECURE,
	
	WindowManager.LayoutParams.FLAG_SECURE);
	
	setContentView(R.layout.activity_main);	

	AND navigate to any screen that contains sensitive information and click the home button to send the app to the background, then press the app switcher button to see the snapshot. As shown below, if FLAG_SECURE is set (right image), the snapshot will be empty; if the flag has not been set (left image), activity information will be shown:	
MSTG-STORAGE-10: The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.	Proof that the app does not hold sensitive data in memory longer than necessary and that the memory is cleared explicitly after use.	

MSTG-STORAGE-11:
The app enforces a minimum device-access-security policy, such as requiring the user to set a device passcode.
	Proof that the app can check the device for the following:
	• PIN- or password-protected device locking
	• Recent Android OS version
	• USB Debugging activation
	• Device encryption
	• Device rooting (see also "Testing Root Detection")
	And:
	Reassure that the lock screen is set:
	`KeyguardManager mKeyguardManager = (KeyguardManager) getSystemService(Context.KEYGUARD_SERVICE);`
	`if (!mKeyguardManager.isKeyguardSecure()) {`
	`// Show a message that the user hasn't set up a lock screen.`
	`}`	

MSTG-STORAGE-12: The app educates the user about the types of personally identifiable	Proof of: - Informing users on their private information that is being processed - Informing the user on the best security practices	

information processed, as well as security best practices the user should follow in using the app.	- Other information you have to share (OSS information), third party libraries, and their licenses	
MSTG-STORAGE-13: No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote endpoint when needed and only be kept in memory.	Proof that data is retrieved from a remote endpoint when needed and only be kept in memory.	
MSTG-STORAGE-14: If sensitive data is still required to be stored locally, it should be encrypted using a key derived from hardware backed storage which requires authentication.	Proof that if sensitive data is still required to be stored locally, that it is encrypted using a key derived from hardware hacked storage which requires authentication.	
MSTG-STORAGE-15: The app's local storage should be wiped after an excessive number of failed authentication attempts.	Proof that the app's local storage sis wiped after an excessive number of failed authentication attempts.	
MSTG-CRYPTO-1: The app does	Proof that the app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	

not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.		
MSTG-CRYPTO-2: The app uses proven implementations of cryptographic primitives.	Proof that the app uses proven implementations of cryptographic primitives. • identify all instances where cryptography is used • identify purpose why cryptography is used (to protect data in use, in transit or at rest) • identify type of cryptography • verify if cryptography is used according to its purpose	
MSTG-CRYPTO-3: The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	Documentation that describes the cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	
MSTG-CRYPTO-4: The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.	Proof that the app does not use cryptographic protocols or algorithms that are widely considered depreciated for security purposes.	
MSTG-CRYPTO-5: The app doesn't re-use the same cryptographic key for	Proof the app doesn't re-use the same cryptographic key for multiple purposes.	

multiple purposes.		
MSTG-CRYPTO-6: All random values are generated using a sufficiently secure random number generator.	Proof of: • all instances where random values are used, and all instances of random number generators are of SecureRandom • random number generators are considered as being cryptographically secure • how random number generators are used • verification of random values generated by application	
MSTG-AUTH-1: If the app provides users access to a remote service, some form of authentication, such as username/pasword authentication, is performed at the remote endpoint.	Proof of: • authentication factors the app uses. • all endpoints that provide critical functionality. • the additional factors are strictly enforced on all server-side endpoints.	
MSTG-AUTH-2: If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.	Proof that: • Session IDs are randomly generated on the server side. • The IDs can't be guessed easily (by using proper length and entropy). • Session IDs are always exchanged over secure connections (e.g. HTTPS). • The mobile app doesn't save session IDs in permanent storage. • The server verifies the session whenever a user tries to access privileged application elements, (a session ID must be valid and must correspond to the proper authorization level). • The session is terminated on the server side and session information deleted within the mobile app after it times out or the user logs out.	

MSTG-AUTH-3: If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.	Proof that (if using JWT): • the HMAC is checked for all incoming requests containing a token; • The location of the private signing key or HMAC secret key is secret. The key should remain on the server and should never be shared with the client. It should be available for the issuer and verifier only. • no sensitive data, such as personal identifiable information, is embedded in the JWT. If, for some reason, the architecture requires transmission of such information in the token, make sure that payload encryption is being applied. See the sample Java implementation on the OWASP JWT Cheat Sheet. • replay attacks are addressed with the jti (JWT ID) claim, which gives the JWT a unique identifier. • tokens are stored securely on the mobile phone, with, for example, KeyChain (iOS) or KeyStore (Android).	
MSTG-AUTH-4: The remote endpoint terminates the existing session when the user logs out.	Proof that the session is terminated on the server side and session information deleted within the mobile app after it times out or the user logs out.	
MSTG-AUTH-5: A password policy exists and is enforced at the remote endpoint.	Proof of the existence of a password policy and the verification of the implemented password complexity requirements	
MSTG-AUTH-6: The remote endpoint implements a mechanism to protect against the submission of credentials an excessive	Proof that after a few unsuccessful login attempts, targeted accounts are locked (temporarily or permanently), and additional login attempts should be rejected.	

number of times.		
MSTG-AUTH-7: Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.	Show proof of the following steps: 1. Log in to the application. 2. Access a resource that requires authentication, typically a request for private information belonging to your account. 3. Try to access the data after an increasing number of 5-minute delays has passed (5, 10, 15, ...). 4. Once the resource is no longer available, you will know the session timeout.	
MSTG-AUTH-8: Biometric authentication, if any, is not event-bound (i.e. using an API that simply returns "true" or "false"). Instead, it is based on unlocking the keychain/keystore.	Proof that the biometric authentication is based on unlocking the keychain/keystore	
MSTG-AUTH-9: A second factor of authentication exists at the remote endpoint and the 2FA requirement is consistently enforced.	Proof of: - The existence of 2fa and the 2fa requirement being consistently enforced	
MSTG-AUTH-10: Sensitive transactions require step-up authentication.	Proof of - The identification of sensitive transactions; and - The implementation of the step-up authentication	

MSTG-AUTH-11: The app informs the user of all sensitive activities with their account. Users are able to view a list of devices, view contextual information (IP address, location, etc.), and to block specific devices.	Proof of: - The informing of the user of all sensitive activities within their account. - A user is able to see from his account: A list of devices, contextual information and to block specific devices	
MSTG-AUTH-12: Authorization models should be defined and enforced at the remote endpoint.	Proof of the authorization factors are strictly enforced on all server-side endpoints.	
MSTG-NETWORK-1: Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	Proof that the app only uses recommended cipher suites described at: • IANA recommended cipher suites can be found in TLS Cipher Suites. or • OWASP recommended cipher suites can be found in the TLS Cipher String Cheat Sheet.	
MSTG-NETWORK-2: The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	See mstg-network-1	

MSTG-NETWORK-3: The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	Proof that the app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	
MSTG-NETWORK-4: The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.	Proof that Either - The app uses its own certificate store; or - Pins the endpoint certificate or public key and subsequently does not establish connections with endpoints that offer a different certificate or key even if signed by a trusted CA.	
MSTG-NETWORK-5: The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.	Proof that the app doesn’t rely on a single insecure communication channel (email or SMS) for critical operations such as enrollments and account recovery.	

MSTG-NETWORK-6: The app only depends on up-to-date connectivity and security libraries.	Proof that the app depends on up-to-date connectivity and security libraries	
MSTG-PLATFORM-1: The app only requests the minimum set of permissions necessary.	Please reference this for descriptions of the listed permissions that are considered dangerous and proof why the app needs it. Also include proof for all custom permissions that the app uses..	
MSTG-PLATFORM-2: All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.	Proof that the following custom URL scheme inputs are validated and/or sanitized. They can expose functionality to: • other apps (via IPC mechanisms, such as Intents, Binders, Android Shared Memory (ASHMEM), or BroadcastReceivers), • the user (via the user interface). The following portions of the source code should be checked if any app functionality has been exposed: • Custom URL schemes. Check the test case "Testing Custom URL Schemes" as well for further test scenarios. • IPC Mechanisms (Intents, Binders, Android Shared Memory, or BroadcastReceivers). Check the test case "Testing Whether Sensitive Data Is Exposed via IPC Mechanisms" as well for further test scenarios. • User interface	
MSTG-PLATFORM-3: The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.	An overview of custom url schemes from the androidmanifest, and proof that it is used securely.	

MSTG-PLATFORM-4: The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.	Identification of elements such as - <intent-filter> - <service> - <provider> - <receiver> Then browse the source code for vulnerable elements	
MSTG-PLATFORM-5: JavaScript is disabled in WebViews unless explicitly required.	If there's a webview class used: Look for the method setJavaScriptEnabled to check for JavaScript activation. If javascript is enabled, proof that: □ The communication to the endpoints consistently relies on HTTPS (or other protocols that allow encryption) to protect HTML and JavaScript from tampering during transmission. □ JavaScript and HTML are loaded locally, from within the app data directory or from trusted web servers only. □ The user cannot define which sources to load by means of loading different resources based on a user provided input	
MSTG-PLATFORM-6: WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.	- setAllowContentAccess - setAllowFileAccess: - setAllowFileAccessFromFileURLs: - setAllowUniversalAccessFromFileURLs: If one or more of the above methods is/are activated, provide proof whether the method(s) is/are really necessary for the app to work properly.	
MSTG-PLATFORM-7: If native methods of the app are exposed to a WebView,	Proof whether the method addJavascriptInterface is used, how it is used, and whether an attacker can inject malicious JavaScript.	

verify that the WebView only renders JavaScript contained within the app package.		
MSTG-PLATFORM-8: Object deserialization, if any, is implemented using safe serialization APIs.	Proof that object deserialization is implemented using save serialization APIs	
MSTG-PLATFORM-9: The app protects itself against screen overlay attacks. (Android only)	Proof that the app protects itself against screen overlay attacks.	
MSTG-PLATFORM-10: A WebView's cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed.	Proof that the cache, storage and loaded resources are cleared before the webview is destroyed.	
MSTG-PLATFORM-11: Verify that the app prevents usage of custom third-party keyboards whenever sensitive data is entered.	Proof that the app prevents usage of custom third-party keyboards whenever sensitive data is entered.	

MSTG-CODE-1: The app is signed and provisioned with a valid certificate, of which the private key is properly protected.	Test results from jarsigner for android showing that the app is properly signed.	
MSTG-CODE-2: The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).	Proof from the android manifest that android:debuggable=”false” or an export of drozer: dz> run app.package.attacksurface <packagename of the app>	Documentation / screenshots
MSTG-CODE-3: Debugging symbols have been removed from native binaries.	An nm export of all the static binaries used in the app. (e.g. export $NM = $ANDROID_NDK_DIR/toolchains/arm-linux.../prebuilt/darwin-x86_64/bin/arm-linux-androideabi-nm && $NM -a libfoo.so)	
MSTG-CODE-4: Debugging code and manufacturer assistance code (e.g. test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.	Proof with StrictMode that no debugging code and verbose error logging are available or enabled. Information	
MSTG-CODE-5: All third party components used by the mobile app, such as	Show proof that vulnerabilities can be detected in third-party libraries.	

libraries and frameworks, are identified, and checked for known vulnerabilities.		
MSTG-CODE-6: The app catches and handles possible exceptions.	Proof of a review the source code to understand the application and identification how it handles different types of errors (IPC communications, remote services invocation, etc.). the following proof checks should be applied.: • Make sure that the application uses a well-designed and unified scheme to handle exceptions. • Plan for standard RuntimeExceptions (e.g.NullPointerException, IndexOutOfBoundsException, ActivityNotFoundException, CancellationException, SQLException) by creating proper null checks, bound checks, and the like. An overview of the available subclasses of RuntimeException can be found in the Android manufacturer documentation. A child of RuntimeException should be thrown intentionally, and the intent should be handled by the calling method. • Make sure that for every non-runtime Throwable there's a proper catch handler, which ends up handling the actual exception properly. • When an exception is thrown, make sure that the application has centralized handlers for exceptions that cause similar behavior. This can be a static class. For exceptions specific to the method, provide specific catch blocks. • Make sure that the application doesn't expose sensitive information while handling exceptions in its UI or log-statements. Ensure that exceptions are still verbose enough to explain the issue to the user. • Make sure that all confidential information handled by high-risk applications is always wiped during execution of the finally blocks.	
MSTG-CODE-7: Error handling logic in security controls	Proof: • that the application uses a well-designed and unified scheme to handle exceptions. • that standard RuntimeExceptions (e.g.NullPointerException,	

denies access by default.	IndexOutOfBoundsException, ActivityNotFoundException, CancellationException, SQLException) work correctly by creating proper null checks, bound checks, and the like.. • that for every non-runtime Throwable there's a proper catch handler, which ends up handling the actual exception properly. • When an exception is thrown, that the application has centralized handlers for exceptions that cause similar behavior. This can be a static class. For exceptions specific to the method, provide specific catch blocks. • that the application doesn't expose sensitive information while handling exceptions in its UI or log-statements. Ensure that exceptions are still verbose enough to explain the issue to the user. • That all confidential information handled by high-risk applications is always wiped during execution of the finally blocks.	
MSTG-CODE-8: In unmanaged code, memory is allocated, freed and used securely.	If there are native code parts: check for the given issues in the general memory corruption section. Native code can easily be spotted given JNI-wrappers, .CPP/.H/.C files, NDK or other native frameworks. □ Is there Java code or Kotlin code? Look for Serialization/deserialization issues. Note that there can be Memory leaks in Java/Kotlin code as well. These can happen for various items, such as: BroadcastReceivers which are not unregistered, static references to Activity or View classes, Singleton classes that have references to Context, Inner Class references, Anonymous Class references, AsyncTask references, Handler references, Threading done wrong, TimerTask references.	
MSTG-CODE-9: Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference	Proof of the build.gradle file to see whether obfuscation settings have been applied.	

counting, are activated.		
MSTG-RESILIENCE-1: The app detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.	Proof of root detection either through: - SafetyNet - Programmatic detection (file existence checks, executing su and other commands, checking running processes, checking installed app packages, writable partitions and system directories, custom android builds)	
MSTG-RESILIENCE-2: The app prevents debugging and/or detects, and responds to, a debugger being attached. All available debugging protocols must be covered.	Java level with JWDP or the native layer via a ptrace-based debugger.	
MSTG-RESILIENCE-3: The app detects, and responds to, tampering with executable files and critical data within its own sandbox.	There are two topics related to file integrity: 1. *Code integrity checks:* Android's APK code signature check. Determined reverse engineers can easily bypass this check by re-packaging and re-signing an app. To make this bypassing process more involved, a protection scheme can be augmented with CRC checks on the app byte-code, native libraries, and important data files. These checks can be implemented on both the Java and the native layer. The idea is to have additional controls in place so that the app only runs correctly in its unmodified state, even if the code signature is valid. 2. *The file storage integrity checks:* The integrity of files that the application stores on the SD card or public storage and the integrity of key-value pairs that are stored in `SharedPreferences` should be protected. The RP should provide proof on the above chapters.	
MSTG-RESILIENCE-4: The app detects, and	Proof of checks on associated application packages, files, processes, or other tool-specific modifications and artifacts.	

responds to, the presence of widely used reverse engineering tools and frameworks on the device.	e.g. An obvious way to detect Frida and similar frameworks is to check the environment for related artifacts, such as package files, binaries, libraries, processes, and temporary files	
MSTG-RESILIENCE-5: The app detects, and responds to, being run in an emulator.	Proof of: - Emulator Detection (e.g. the build.prop) - Checks on the telephony manager (all android emulators have fixed values) Install and run the app in the emulator. The app should detect that it is being executed in an emulator and terminate or refuse to execute the functionality that's meant to be protected. Work on bypassing the defenses and answer the following questions: - How difficult is identifying the emulator detection code via static and dynamic analysis? - Can the detection mechanisms be bypassed trivially (e.g., by hooking a single API function)? - Did you need to write custom code to disable the anti-emulation feature(s)? How much time did you need? - What is your assessment of the difficulty of bypassing the mechanisms?	
MSTG-RESILIENCE-6: The app detects, and responds to, tampering the code and data in its own memory space.	Proof of: - comparing the contents of memory or a checksum over the contents to good values, - searching memory for the signatures of unwanted modifications.	
MSTG-RESILIENCE-7: The app implements multiple mechanisms in each defense category (RESILIENCE-1 to RESILIENCE-6). Note that resiliency scales with	Proof that the app implements multiple defense mechanisms in each defense category.	

the amount, diversity of the originality of the mechanisms used.		
MSTG-RESILIENCE-8: The detection mechanisms trigger responses of different types, including delayed and stealthy responses.	Proof of detection mechanisms that trigger responses including delayed and stealthy presponses.	
MSTG-RESILIENCE-9: Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.	Proof of: • meaningful identifiers, such as class names, method names, and variable names, have been discarded, • string resources and strings in binaries are encrypted, • code and data related to the protected functionality is encrypted, packed, or otherwise concealed.	
MSTG-RESILIENCE-10: The app implements a 'device binding' functionality using a device fingerprint derived from multiple properties unique to the device.	Proof of: • Augmenting the credentials used for authentication with device identifiers. This make sense if the application needs to re-authenticate itself and/or the user frequently. • Encrypting the data stored in the device with the key material which is strongly bound to the device can strengthen the device binding. The Android Keystore offers non-exportable private keys which we can use for this. When a malicious actor would then extract the data from a device, he would not have access to the key to decrypt the encrypted data. • Use token-based device authentication (Instance ID) to make sure that the same instance of the app is used.	
MSTG-RESILIENCE-11: All executable files and libraries belonging to the app are either encrypted on	Proof of - All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.	

the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.		
MSTG-RESILIENCE-12: If the goal of obfuscation is to protect sensitive computations, an obfuscation scheme is used that is both appropriate for the particular task and robust against manual and automated de-obfuscation methods, considering currently published research. The effectiveness of the obfuscation scheme must be verified through manual testing. Note that hardware-based isolation features are preferred over obfuscation whenever possible.	Proof of: - an obfuscation scheme is used that is both appropriate for the particular task and robust against manual and automated de-obfuscation methods, considering currently published research. - The effectiveness of the obfuscation scheme being verified through manual testing. Note that hardware-based isolation features are preferred over obfuscation whenever possible.	

MSTG-RESILIENCE-13: As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.	Proof of application level payload encryption to further impede eavesdropping.	

IV Annex – Table with RARS requirements and deliverables for general IoT applications.

Requirement	Description of what should be in the documents	Type of documents required for validation
4.3	Use and Access levels of the application	
Application should only be used for general mobile devices	Required are: - .apk or .ipa format check for either Android or iOS . (installation file depending on the designated platform) - A link to the correct app on the google play store / app store - Class Diagram of the source code - The used compiler(s) / interpreter(s) plus their version numbers. - A UML diagram and flow diagram of the app showing the different Views/Intents and their interdependence. *Note:* *In following requirements when a list of entities is requested the same names should be used as stated in the tree structure*	Documentation Code
Application connects to the panel of the alarm system through the data center	Documentation of: - The API(s) involved in the connection - The type of the API - URL's (redirects and full URL's) - A webpage with all the API documentation is also possible .. *Note: the above-mentioned points should be mentioned for every API*	Documentation Possible Webpage
Access through the mobile application should be according to access-level 2 according to 50131-1	Documentation of: - List of actions and their effects that a **user** can perform through the application. - Involved entities for every action (that are part of the whole chain) in every for every interaction. - Involved components of the source code for the actions of the user - Preferably UML or equivalent Diagram illustrating all involved processes, actions, technology and software. *Note: These requirements limit the actions a user can perform. The user should not have administrator level privileges.*	Documentation
Application shall enforce setting a new password	Documentation of: - Description of the process of how this requirement is enforced.	Documentation

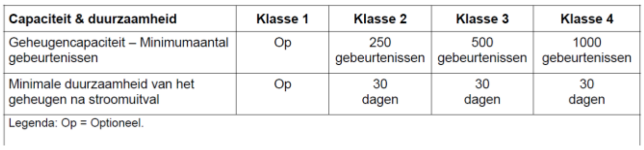
after first installation	- Password mechanism used must be such that this step cannot be skipped. - Description of the mechanism that keeps this process fail-safe. - UML diagrams of all involved processes, entities, parts, technology and software of aforementioned processes in this requirement.	
The panel of the alarm system shall connect to a secure hosted data web platform	Documentation of: - Description of the process of how the panel is connected to the data platform + UML diagrams - description of the hosted web platform used - Name of the hosting provider and or infrastructure provider for the web platform and the hosted platform. - IP address(es) of the hosted platform - DNS names that are used - Owner/ Responsible Party for the hosted web platform - Services used by the system - Purpose of the system	Documentation
Access through the panel should be according to access-level 3 according to 50131-1	Documentation of: - List of actions and their effects that an **administrator** can perform through the application. - Involved entities for every action (that are part of the whole chain) in every for every interaction. - Involved components of the source code for the actions of the administrator. - UML diagram of the process. *Note: Here we consider list of actions and their effects that a user can perform in a role of an administrator or employee of the alarm service provider. This includes all the configurations and settings that can be changed but does not affect the architecture of the alarm system.*	Documentation
4.4	Connections of the application	
The connection of the mobile application to the alarm panel should be secure and confidential. Key management according to TLS 1.2 or higher. Safe cypher suites according to TLS guidelines from NCSC (April 2019)	Documentation of: - List of components involved in the connection between the mobile application and the panel. - Description of how each of these components are connected to each other. - Purpose of each of the connection. - Encryption technique(s) and hashing technique(s) used - Cryptographic algorithms used - UML diagrams of all involved processes, entities, parts, technology and software of aforementioned processes in this requirement. *Note:* *SHA-1 shouldn't be used as it is deemed unsafe.*	Documentation
Key management should be arranged	Documentation of: - Type(s) of key management system used - UML of overall process	Documentation

according to **ISO/IEC11770-1/2/3**	- All relevant entities that make use of keys - Involved parties and processes for every type of key exchange - Used algorithms - Bitsizes per type of key	
Integrity of the connection should be according to **ISO/IEC 18033** (cryptographic algorithms)	Documentation of: - The document or resource is used to keep the cryptography algorithms up to date. *Note:* *Requirements for algorithms and cryptography for keeping up to date to the latest techniques (next point also has a requirement for keeping the techniques up to date)*	Documentation
Aforementioned cryptographic algorithms should be up to date with www.ssllabs.com (should be checked every half a year and during penetration testing on the infrastructure of the client)	Documentation of: - Which version number of the documents on the website is used to keep the cryptography algorithms up to date.	Documentation
The connection of the panel to the hosted web platform should meet the requirements according to IEC **60839-5-1 (EN50136-1)**	Documentation of: - The transmission network between the panel and the hosted web platform. - This should include availability of the network - The processes that ensures the robustness of the network in the form of an UML diagram or equivalent form of information. - Response times for incoming and outgoing actions from the perspective of both the panel and the data center - List of entities that share the transmission link that is used for connecting the panel and the data center. - Description of DDoS mitigation technique(s) in place. - Description of failure handling. *Note:* *The exact requirements for the various numbers that need to be met are well elaborated in the mentioned standard.*	Documentation
The connection of the mobile application to the hosted web platform should	Documentation of: - The transmission network between the panel and the hosted web platform. - This should include availability of the network - The robustness of the network.	Documentation

meet the requirements according to IEC **60839-5-1 (EN50136-1)**	- Description of the mechanism that ensures the robustness. - Response times for incoming and outgoing actions from the perspective of both the panel and the data center - List of entities that share the transmission link that is used for connecting the panel and the data center. - Description of DDoS Prevention technique - Description of failure handling. *Note:* *The exact requirements for the various numbers that need to be met are well elaborated in the mentioned standard.*	
4.5	Acknowledgement un/setting	
When a setting is made through the mobile application to the alarm system the panel and the hosted web platform should acknowledge that this change was made.	Documentation of: - Mechanism used for verification of actions by the panel. - Mechanism used for verification of actions by the hosted web platform. - List of involved entities. - UML diagrams of relevant processes.	Documentation
If there were to be made a setting that comes in through the hosted web platform, the panel will verify this setting and then acknowledge it.	Documentation of: - Mechanism used for verification by the hosted web platform. - List of involved entities. - UML diagrams of relevant processes.	Documentation
The overall process should have a failsafe mechanism that guarantees that if there were to be a connection failure the process of setting change is stopped, and the last and most recently saved settings shall be reinstated.	Documentation of: - Description of failsafe mechanisms for verifications at both the panel and the hosted web platform. - List of involved entities. - UML diagrams of relevant processes.	Documentation
4.6	Authenticity	
Definitions and Processes shall be applied based on **ISO/IEC 29115**		

<table>
<tr><td>Minimal of 2factor authentication is required for the application. And while authenticating there is a time limit to do so.</td><td>Documentation of:
- Description of the implementation of 2 factor authorization for the hosted provider and the web platform (if two separate instances).
- Failsafe mechanism
- Time limit of 2 minutes before the code expires
- UML diagrams of relevant processes.</td><td>Documentation</td></tr>
<tr><td>Access levels through the mobile app shall be the same as for the panel of the alarm system</td><td>Documentation of:
- UML diagram of mechanism that ensures this
- Involved entities</td><td>Documentation</td></tr>
<tr><td>Giving more users access through the mobile application is organized in a same way as done for the panel of an alarm system.</td><td>Documentation of:
- Mechanism that ensures this
- Involved entities</td><td>Documentation</td></tr>
<tr><td>For mobile applications that require different levels of access, Role based Access Control should be applied.</td><td>Documentation of:
- UML Diagram Mechanism that ensures this
- Involved entities

<i>Note:</i>
<i>Role-based access control (RBAC) is a policy-neutral access-control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.</i></td><td>Documentation</td></tr>
<tr><td>4.7</td><td colspan="2">Accountability</td></tr>
<tr><td>Logging of all activities is mandatory, and the minimum storage time of logs is 6 months or more defined according to the grading available in EN50131-1</td><td>Supporting documentation on:
- Description of mechanism for logs
- What is being logged
- Where it is stored
- For how long it will be logged
- How the mechanism is ensured
- How the logs are protected
- Whom has access to the logs
- Entities involved in the process of logging

<i>Note:</i>
<i>Minimum space that is required is stated in the number of actions that should at minimum be stored(table 21)</i>

<table>
<tr><th>Capaciteit &amp; duurzaamheid</th><th>Klasse 1</th><th>Klasse 2</th><th>Klasse 3</th><th>Klasse 4</th></tr>
<tr><td>Geheugencapaciteit – Minimumaantal gebeurtenissen</td><td>Op</td><td>250 gebeurtenissen</td><td>500 gebeurtenissen</td><td>1000 gebeurtenissen</td></tr>
<tr><td>Minimale duurzaamheid van het geheugen na stroomuitval</td><td>Op</td><td>30 dagen</td><td>30 dagen</td><td>30 dagen</td></tr>
<tr><td colspan="5">Legenda: Op = Optioneel.</td></tr>
</table></td><td>Documentation</td></tr>
<tr><td>Data in transmission and storage needs proper encryption</td><td>Documentation of:
- Description of techniques used to protect the whole alarm system and/or components of the</td><td>Documentation</td></tr>
</table>

that needs to be arranged according to EN50136-1 and EN50518	alarm system against malicious attacks and inadvertent influences. - Involved entities for each of the techniques - Failsafe mechanisms used - Relevant UML processes	
4.8	Time Restrictions	
There should be a maximum session time for critical functions	Documentation of: - List of critical functions - Time limit for each function - Involved entities	Documentation
Access levels and time limits	- Depending on the access level different time limits are specified until there has to be a re-login. - A table with every access level mapped to the corresponding time limit is required.	Documentation
Hostile access (brute forcing) to the application shall be impossible and shall be verified through means of penetration testing	Documentation of: - Proof that penetration testing was performed - Penetration test Report - How Brute Forcing Prevention is assured by means of proof of the Penetration Test - Aspects and/ or parts of the alarm system that were penetration tested	
4.9	Instructions by the application Towards the user	
The mobile application shall warn and instruct users if the application is used outside the grading requirements and boundaries as stated in EN50131-1. Privacy and security issues that arise due to usage of the mobile application outside of the safe perimeters of the physical location of the alarm system are not the responsibility of the service provider but are for the responsibility of the end user.	Documentation of: - Scope according to the requirement as stated for the alarm system should be defined well. - List of warning(s) that can be issued to the users. - Mechanism involved for warning the users. - Involved entities.	Documentation
5.2	Functional Testing	

Functional testing shall be performed in the laboratories of Kiwa or at a site of the manufacturer/ service provider under supervision of an expert of Kiwa. This will be done in an end to end situation.	Table 2 gives a general overview of the required documentation for fulfilling proper assessment for this requirement.	Agreements between Kiwa and Manufacturer
5.3	Functional Security Assessment	
Security testing of the code is based on the OWASP Ten most critical web application security risks and Mobile application. According to the latest owasp rules.	- Policy documents if ISO27001 certified. - Development life cycle documents stating which design and documentation process has been followed - Functional design documents - Technical design documents (the technical elaboration for the realization of functional wishes)	Documentation
The test report shall define a list of used tools used during development and their version numbers.	Self-explanatory	
The expert(s) that will carry out the tests shall meet the requirements as specified in the RARS scheme 5.3.	Profile of the tester documented should include: - CV - Relevant Work Experience	Documentation
6.2	Process Requirements for Development	
Process that needs to be followed for development shall fulfill 14.2 of 27001 or secure development processes according to IEC62443-4-1	Proof in form of documentation or relevant certificate of ISO27001	Certificate
The manufacturer needs an accredited ISO 9001 certificate according to the standard and it shall be assessed	Proof of certificate and relevant documents	Certificate

by an expert of Kiwa.		
Re-developed code shall be tested at a minimum of 1 time per year according to 5.3. If the need may be this can be more often but that has to be decided on basis of the risk assessment by the manufacturer.	- The manufacturer needs to contact and notify Kiwa when there is an update to the application with the changelog. - Any update should be reported to Kiwa. - Depending on the severity of the update re-assessment will be initialized.	Agreements between Kiwa and Manufacturer
7.2	Assessment by the manufacturer and Kiwa	
The quality system of the supplier will be assessed by Kiwa on the basis of IQC scheme/Quality plan	Proof of corresponding certificates and relevant documents	Document Certificate
Assessment shall be done once a year	In accordance with Kiwa and Manufacturer	Agreements between Kiwa and Manufacturer
The mobile application shall be inspected internally by the supplier through the IQS scheme/ quality plan	- Documentation of how this is performed. - And or relevant certificates and or documentation.	Document Certificate
Market samples of the mobile application shall be assessed once a year by Kiwa according to the Kiwa Quality plan		Mobile Application from app stores
A high-level structure checklist shall be made and used by Kiwa based on the OWASP guidelines		Documentation
9.2	Manager of the quality system of the product	
Manager of the quality system has to meet certain requirements and	Relevant certificate that manufacturer has this in proper order	Certificate

has certain responsibilities		
9.3	Internal quality control/ quality plan	
Requirements for supplier’s IQS plan (quality plan)	Relevant certificate that manufacturer has this in proper order	Certificate
9.4	Procedures and working instructions	
Requirements for suppliers’ responsibilities	Relevant certificate that manufacturer has this in proper order	Certificate

V Version Control

Version	Changes	Date	Initials of Author
1.0	Initial set up of the scheme	22/11/2019	SS
2.0	Addition of Annex 1 until 4 Editorial Changes	24/08/2020	SS
3.0	Editorial Changes	03/12/2020	SS