Decree

No …/2024 (… …) of the President of the Supervisory Authority for Regulatory Affairs (SZTFH)

on the national cyber security certification scheme for IoT devices

On the basis of the authorisation granted in Section 28(3)*(c)* of Act XXIII of 2023 on cyber security certification and cyber security supervision, and acting within the scope of my duties as defined in Section 13*(n)* and *(q)* of Act XXXII of 2021 on the Supervisory Authority for Regulatory Affairs, I hereby order the following:

Section 1

(1) For the purposes of this regulation, an IoT device shall mean an ICT product according to Act XXIII of 2023 on cyber security certification and cyber security supervision (hereinafter: Cyber Certification Act), which interacts with the environment through signal transformation. The form of interaction can be
(a) detection by which the IoT device collects data about the environment, or
(b) an intervention that triggers changes in the environment.

(2) Interaction with the environment referred to in paragraph 1 may take place through:
(a) an application programming interface (hereinafter referred to as: API) which enables other computing devices to communicate with an IoT device through the application provided by the IoT device,
(b) a user interface which enables direct communication between the IoT device and the user, or
(c) a network connection which ensures communication for the IoT device with an electronic communications network for the purpose of communicating data to or from an IoT device or ensures access to the network user interface.

(3) For the purposes of the application of paragraph (2)*(c)*, the interface capability to enable a network connection includes both the hardware and the software environment that operates and serves it.

Section 2

(1) This Decree, with the exception of paragraphs 2 and 3, applies to the IoT devices' conformity self-assessment and conformity assessment (hereinafter collectively referred to as: assessment).

(2) The regulation does not cover the assessment of IoT tools for which a national cyber security certification scheme has been established in a separate regulation by the President of the Supervisory Authority for Regulatory Affairs (SZTFH).

(3) The national cyber security certification scheme for IoT devices (hereinafter: certification scheme) is intended to ensure that decisions made by citizens, business organisations and

public bodies when procuring IoT products are supported and that the assets are comparable on the basis of the assurance levels defined in the certification scheme.

Section 3

(1) The certification scheme contains requirements for the assurance levels of ‘basic’, ‘significant’ and ‘high’ within the meaning of Section 8(1) of the Cyber Certification Act.

(2) On the basis of the certification scheme, conformity self-assessment may be carried out at ‘basic’ assurance level.

(3) Conformity assessments by conformity assessment bodies may be carried out, at most, at the assurance level registered by the Supervisory Authority for Regulatory Affairs as the national cyber security certification authority designated in Section 4(1)(a) of the Cyber Certification Act (hereinafter: certifying authority), upon the request of the manufacturer pursuant to the Cyber Certification Act (hereinafter referred to as: manufacturer).

Section 4

(1) A manufacturer may start a national conformity self-assessment procedure or a conformity assessment body may start the conformity assessment activities if the documents referred to in Annex 1 and produced by the manufacturer are available. A sample of the documents referred to in Annex 1 shall be published on the website of the certifying authority.

(2) The national conformity statement or the national cyber security certificate (together: national certificate) may only be issued for the given assurance level if the IoT device subject to assessment meets the requirements set out in Annex 2 for that assurance level.

(3) Compliance pursuant to paragraph 2 can be demonstrated by presenting the assessment report which must be issued based on an examination carried out according to the assessment methodology set out in Annex 4 (hereinafter referred to as: assessment report), or by carrying out a vulnerability test for the requirements set out in Annex 3.

(4) Certificates issued on the basis of an international, European or national standard shall not be accepted for demonstrating compliance in accordance with paragraph 2, in lieu of the required information according to paragraph 3.

(5) A manufacturer may issue a conformity statement in accordance with Annex 5 and a conformity assessment body may issue a national cyber security certificate in accordance with Annex 6 if the assessment report collectively brings positive results with a ‘pass’.

(6) The manufacturer or conformity assessment body shall submit the national certificate, the documents referred to in Annex 1 and the assessment report for registration to the certifying authority, by means of an electronic form established for that purpose by the certifying authority.

(7) The administrative time limit for registration pursuant to paragraph 6 shall be 45 days.

Section 5

(1) The validity period of the national certificate (hereinafter referred to as: period of validity) is maximum 365 days from the date of issue.

(2) The manufacturer shall affix the label, referred to in Annex 7, as a conformity marking to an IoT device which has a national certificate produced until the end of the validity period, and the label shall have the content indicated in the certifying authority’s decision.

(3) During the period of validity, the manufacturer shall continuously and consecutively conduct safety impact assessments for each change affecting an IoT device, stating:
(a) the date of change,
(b) the reason for the change,
(c) whether the change affects the IoT devices manufactured prior to the change,
(d) a detailed description of the elements of the change,
(e) what risks are affected by the change, and
(f) whether the change addresses a vulnerability or introduces a new security control.

(4) For the purposes of paragraph 3, any change that affects the security status of the IoT device, including the emergence of new threats and vulnerabilities, shall be considered as a change.

(5) The manufacturer shall update the implementation document mentioned in Annex 1 continuously and consecutively during the period of validity.

Section 6

(1) The manufacturer may, with the exception of paragraph 5, submit a request to maintain the validity of the national declaration of conformity in the certifying authority’s register (hereinafter referred to as: a request for maintenance), which shall be submitted to the certifying authority by means of an electronic form created by the certifying authority for this purpose, not earlier than 60 days before the expiry of the validity period, but no later than 30 days before the expiry thereof.

(2) The request for maintenance shall be accompanied by the safety impact assessment referred to in Section 5(3), the implementation document (referred to in Annex 1) in its updated version pursuant to Section 5(3), and the new requested validity period shall be indicated in the application, which shall not exceed 365 days.

(3) During the maintenance procedure, the certifying authority’s administrative deadline is 30 days.

(4) The certifying authority may set a validity period different from the period of validity indicated in the maintenance application, but this should be at least 120 days calculated from the end of the initial validity period, if it cannot be established that, with the changes made to the IoT device under examination, the said IoT device continuously complies with the requirements of the certification system and ensures the achievement of the safety objectives starting from the date of issue of the national declaration of conformity. If the new validity period indicated in the application for maintenance is less than 120 days, the certifying authority shall establish the new period of validity in accordance with the application.

(5) In the case referred to in paragraph 4, the manufacturer may not submit another (further) maintenance application for the declaration of conformity that has been issued for the given IoT device.

(6) In the case referred to in paragraph 4, or where the validity period of the declaration of conformity issued for the IoT device has expired, the manufacturer may submit, to the certifying authority, a request to renew the national declaration of conformity for the IoT device by means of an electronic form created for that purpose by the certifying authority.

(7) The application referred to in paragraph 6 shall be accompanied by the new declaration of conformity which has been issued according to Section 4(5) on the basis of the examination referred to in Section 4(1)–(4), the documents referred to in Annex 1 and the assessment report.

(8) The administrative deadline for the renewal procedure referred to in paragraph 6 shall be 45 days.

(9) Paragraphs 1 to 4 shall apply to the maintenance of the validity of a new declaration of conformity, which has been registered by the certifying authority on the basis of a request pursuant to paragraph 6.

Section 7

(1) In order to extend the validity period of the certificate for a given IoT device which has been registered on the basis of a national cyber security certificate issued by a conformity assessment body, the manufacturer shall, within 60 days prior to the expiry of the validity period, make the following available to the conformity assessment body: the safety impact assessment referred to in Section 5(3) and the implementation document (referred to in Annex 1) in its updated version in accordance with Section 5(5).

(2) On the basis of the examination of the documents referred to in paragraph 1, provided that – even with the changes made to the IoT device under examination – the IoT device continuously complies with the requirements of the certification scheme and ensures the achievement of the security objectives starting from the issue of the national cyber security certificate, it shall revalidate the expiring certificate no later than 8 days prior to the expiry of the validity period, with the new period of validity not exceeding 365 days from the end of the initial period of validity.

(3) If, on the basis of the documents referred to in paragraph 1, it cannot be established that the examined IoT device continuously complies with the requirements of the certification scheme from the date of issue of the national cyber security certificate and that it ensures the achievement of the security objectives, the conformity assessment body may revalidate the expiring certificate on condition that the new validity period does not exceed 90 calendar days from the end of the initial period of validity.

(4) In the case referred to in paragraph 3, the validity period of the national cyber security certificate issued for a given IoT device may not be extended after the expiry of the new validity period referred to in paragraph 3. Instead, its renewal may be initiated.

(5) The manufacturer may initiate the renewal of the national cyber security certificate of the IoT device with the conformity assessment body in the case referred to in paragraph 3 or when the period of validity of the national cyber security certificate has expired.

(6) In the context of renewal, the conformity assessment body will, by means of an electronic form created for this purpose by the certifying authority, submit the following for registration: the new national cyber security certificate which has been issued according to Section 4(5) on the basis of the examination referred to in Section 4(1)–(4), as well as the documents referred to in Annex 1 and the assessment report.

Section 8

The validity period of the national certificate will not be affected if, during the period of validity, a new national cyber security certification scheme is established for the IoT device pursuant to Section 2(2), but after this the validity period of the national certificate for the IoT device may not be extended, an application for maintenance may not be submitted and the national certificate may not be renewed.

Section 9

This Decree shall enter into force on the third day following its publication.

Section 10

The requirement for the prior notification of this draft decree, as stipulated in Articles 5-7 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, has been met.

Annex 1 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)

Documentation requirements

1. IoT device identification document

1.1. The document with information to identify the IoT device subject to conformity self-assessment or conformity assessment (hereinafter: VE), which contains as detailed information as possible about the subject of the examination, in particular in terms of version numbers and configuration options.

1.2. Minimum content of the identification document:

a) Name of product under examination
b) Brand designation
c) Commercial name.
d) Model ID
e) Hardware configuration (including release number and serial number)
f) Running environment or operating system
g) Firmware version in factory state
h) Manufacturer details:
(ha) name
(hb) short name
(hc) registered address
(hd) phone number
(he) e-mail address
(hf) contact person details: name, nationality, phone number, e-mail address
i) Planned annual number of produced items in terms of VE
j) An indication of the commercial markets in which the device under examination is expected to be sold in the following 1 year:
(ia) only Hungary
(ib) EU Member States (if not in the EU as a whole, list of Member States), or
(ic) other
k) An indication of the assurance level to which the test will be conducted: basic/significant/high

2. Implementation document

2.1. The implementation document (hereinafter referred to as: MD) contains detailed information relevant to the assessment of the requirements set out in Annex 2 which are used in the implementation of the IoT instrument identified in accordance with point 1.

2.2. Minimum content of the MD

2.2.1. MD 1-UserInfo: User information

The MD lists the documentation, publications and information provided to users. This includes both the manufacturer's website and the corresponding URL, user manual or built-in help. The list contains information on the operation of the following independent functions and mechanisms:

	A	**B**
1.	Documentation of change mechanisms	Documentation of the mechanisms for modifying authentication values for the user, including all the information needed to access the documentation.
2.	Sensor documentation	Documentation, for the user, of information related to external sensing capabilities, including all necessary information to access the documentation.
3.	Documentation of the secure setting	The user documentation methodology for the safe configuration of VE, including all the information that is necessary to access the documentation.
4.	Documentation of set-up verification	A description of how the method for verifying the safe configuration of VE is documented for the user, including all the information needed to access the documentation.
5.	Documentation of personal data	The manner in which the information relating to the processing of personal data is documented for the user, including all the information necessary to access the documentation.
6.	Documentation of telemetry data	The way information relating to the collection of telemetry data is documented for the user, including all the information necessary to access the documentation.
7.	Documentation of deletion	A description, for the user, how personal data is deleted, including all the information necessary to access the documentation.
8.	Model name	An indication of the VE model and a brief description of how the VE model designation can be recognised by the user. Specify here if the version number of VE and its software components can be retrieved by means of a network query and how it is done. If open source software is used, the kernel and application versions of the open source operating system and their long-term support (LTS) time should be indicated here.

9.	Support period	The period during which the product or service is maintained by the manufacturer, e.g. in the form of updates, including kernel and application versions of the open source operating systems.
10.	Publication of the support period	The way the support period is published and documented for the user, including all the information about access to the publication.
11.	Disclosure of vulnerability	The way vulnerabilities are disclosed, including all the information about access to disclosure.
12.	Publication of non-upgradable components	A description of the reasons for the absence of software updates, including all the information needed to access the publication.

2.3.2. MD 2-SecDev: Safe development processes

The MD lists all the safe development processes that the manufacturer has carried out or has implemented for VE. The MD contains the following entries

	A	**B**
1.	ID	Unique identifier for each process, starting with SecDev-1.
2.	Description	A brief description of the safe development process. If an existing standard is used, a reference to the corresponding standard shall be provided. A description should be included about the applied programming techniques to demonstrate that they are suitable to mitigate tampering, fault and leakage attacks.

2.3.3. MD 3-VulnTypes: Relevant vulnerabilities

The MD lists every type of vulnerability that is relevant to VE. The MD shall contain the following entries:

	A	**B**
1.	ID	Unique identifier for each vulnerability, starting with VulnTypes-1.
2.	Description	A brief description of the vulnerability relevant to VE.
3.	Action	Where vulnerability is detected, a description of the way action is taken in relation to this type of vulnerability, including all organisations involved in the action and their responsibilities.
4.	Time-frame	A dedicated time-frame in which specific steps of action are scheduled in the event of vulnerability. Example: 5 days for the first response and 90 days until the correction is published.

2.3.4. MD 4-Conf: Statements, declarations

The MD lists the declarations for the various processes. The MD contains the following independent entries, for which clear YES or NO answers should be indicated.

	A	**B**
1.	Confirmation of vulnerability actions	Confirmation that the necessary infrastructure is available for each "Action" described in MD 3-VulnTypes and that operators have been informed in order to reach the target "Timeframe".
2.	Confirmation of vulnerability surveillance	Confirmation that the necessary infrastructure is in place to monitor, identify and correct each vulnerability described in MD 5-VulnMon and that the operators have been informed.
3.	Confirmation of update procedures	Confirmation that the necessary infrastructure is available for each update process described in MD 6-UpdProc and that operators have been informed to achieve the targeted "Timeframe".
4.	Confirmation of secure management	Confirmation that the secure management processes described in MD 15-SecMgmt have been established.
5.	Confirmation of safe development	Confirmation that the safe development processes described in MD 2-SecDev have been established.

2.3.5. MD 5-VulnMon: Vulnerability monitoring

The MD lists all procedures for verifying, identifying and correcting vulnerabilities, with the following entries.

	A	**B**
1.	ID	Unique identifier for each procedure, starting with VulnMon-1.
2.	Description	A description of how to track, identify, and correct security gaps in products and services.

2.3.6. MD 6-UpdProc: Updating procedures

The MD lists the manufacturer's procedures for issuing security updates, with the following data:

	A	**B**
1.	ID	Unique identifier for each procedure, starting with UpdProc-1.
2.	Description	A brief description of the procedure for issuing security updates, including all organisations and responsibilities.
3.	Time-frame	The planned time frame for the completion of the procedure.

2.3.7. MD 7-Intf: Interfaces

The MD lists all network, physical and logical interfaces of VE, with the following parameters:

	A	**B**

1.	ID	Unique identifier for each interface, starting with Intf-1.
2.	Description	Description of the interface, including its purpose. In the case of physical interfaces, it is also necessary to describe whether the interface is always necessary, or it is only necessary in certain cases as specified in the description (e.g. intermittent use) or if it is never necessary.
3.	Type	Indication whether the interface is of network, physical (including wireless interfaces), logical or multiple type.
4.	Status	Indication that the interface is enabled or disabled in the initialised state. In the case of authorised interfaces, an explanation is required.
5.	Change of status	A list of interface states, indicating how and with what role can the status changes be triggered by the user, citing the role pursuant to MD 9-Role.
6.	Structure of the relationship	Description of how the interface builds the connection, what validation and authentication mechanisms it uses, with reference to the MD-10-Auth authentication mechanism.
7.	Published information	If the interface is a network interface: a description of the information disclosed in the initialised state without authentication and the reasons for its disclosure, as well as an indication of whether the disclosure is relevant for information security purposes.
8.	Debugging interface	If the interface is a physical interface: whether the interface can be used as a debugging interface.
9.	Protection	If the interface is a physical interface: description of the protection methods necessary to limit the exposure of the interface. In the case of debugging interfaces, it is a requirement to describe the software mechanism used to disable the interface.

2.3.8. MD 8-DevID: Device identifiers

All VE identifiers used to identify the device shall be included in the MD.

	A	**B**
1.	ID	A unique identifier for each device identifier, starting with DevID-1.
2.	Identifier type	Information on the form of the identifier (label, physical or logical identifier) and its uniqueness.
3.	Accessibility of the identifier	With what role and how can the ID be identified by the user in each state of the device (factory packaged, factory default and set-up). If available through the identification interface, reference shall be made to the MD 7-Intf interface.
4.	Identifier source	“Pre-installed” or “Can be added by user”.
5.	Identifier generating mechanism	A brief description of the algorithm which is used to generate the identifier, describing the actions to ensure, in a risk-proportionate

		manner, that the identifiers reduce the risk of automatic attacks that build on obvious regularities, common strings, publicly available information or insufficient complexity.
6.	Performance of operations	A description of the operations that can be carried out in the knowledge of the identifier and the manner in which they are carried out, with reference to the MD 7-Intf interfaces involved in the operation.
7.	Security objectives	A description of the security objectives achieved and the threats that the mechanism should address.
8.	Brute Force Protection	If the identifier can be accessed directly from a network interface, a description of the method designed to prevent the attacker from obtaining the identification data through a brute force attack via the network interfaces.
9.	Timing Attack Protection	If the identifier is available directly from a network interface, a description of the method designed to prevent the attacker from gaining unauthorised authorisation by exploiting timings.

2.3.9. MD 9-Role: Roles

The MD shall include the roles handled by VE in factory state, including actors not subject to identification and even machine-to-machine connections.

	A	**B**
1.	ID	Unique identifier for each role, starting with Role-1.
2.	Description	A brief description of the role.
3.	Purpose	The general purpose of the users in the role.
4.	Operations	A list of actions that can be performed by the users in the role.

2.3.10. MD 10-AuthMech: Authentication mechanisms.

All VE authentication mechanisms shall be included in the MD. The MD shall contain the following entries:

	A	**B**
1.	ID	Unique identifier for each authentication mechanism, starting with AuthMech-1.
2.	Description	A brief description of the authentication mechanism and the associated authorisation process. Specify whether the mechanism is used for user authentication or machine-to-machine authentication, and whether it can be accessed directly from a network interface. In the case of a third-party implementation, it should be explained how the design of the supply chain prevents the leakage of VE-specific credentials.
3.	Authentication	Type of attribute used for authentication. For passwords, it is also

	factor	necessary to indicate whether the password is set and used by the user in the initialised state.
4.	Password-generating mechanism	If the authentication factor is a password that is not set by the user, a description of the mechanism to generate the password, noting that no detailed description is required. The description shall specify whether the password is unique per device and whether it is pre-installed, it shall describe the actions which ensure that passwords are unique for each device in any state other than factory default and that they reduce the risk of automatic attacks that build on obvious regularities, common strings, publicly available information or inappropriate complexity when such passwords are used as pre-installed and unique passwords per device.
5.	Security guarantees	A description of the security objectives achieved and the threats that the mechanism should address.
6.	Cryptographic details	A description of the cryptographic methods (protocols, operations, primitives, modes and key sizes) used to provide the authentication mechanism and to facilitate the described "security guarantees", taking into account key management.
7.	Brute Force Protection	If the authentication mechanism is available directly from a network interface, a description of the method designed to prevent the attacker from obtaining the authentication details through a brute force attack via the network interfaces.
8.	Timing Attack Protection	If the authentication mechanism is available directly from a network interface, a description of the method designed to prevent the attacker from gaining unauthorised authorisation by exploiting timings.
9.	Customisation	Setting options associated with the authentication mechanism.
10.	Application	The roles of interfaces and users using the authentication mechanism, with reference to MD 7-Intf interfaces and MD 9-Role roles.
11.	Handling.	Description of the process of changing the authentication identifier.

2.3.11. MD 11-Account: Account management

The MD shall include solutions related to the management of user accounts.

	A	B
1.	ID	Unique identifier for each action and solution, starting with Account-1.
2.	Operation	Operation name.
3.	Description	A detailed description of the mechanism of the operation carried out.
4.	Configuration	A description of what data can be configured in the account management operation for users with what type of MD 9-Role roles.

2.3.12. MD 12-SoftComp: Software components

The MD lists all the software components of VE. The applied level of detail for dividing the examined software into software components is intended to identify which components can be updated and which cannot in the case of a vulnerability test. The MD contains the following entries.

	A	**B**
1.	ID	Unique identifier for each software component, starting with SoftComp-1.
2.	Description	A brief description of the software component. Please indicate separately if the update of the software component contains sensitive data.
3.	Update mechanism	Reference to the MD 13-UpdMech update mechanisms that are used to update the software component. A blank list of update mechanisms indicates the failure of software component updates, and the lack of such updates needs to be justified.
4.	Cryptographic use	Indicates whether the software component uses cryptographic algorithms or primitives (yes/no) and, if so, whether the manufacturer has taken into account the side effects of updating these algorithms and primitives (yes/no).

2.3.13. MD 13-UpdMech: Update mechanisms

The MD lists all VE update mechanisms, for which the following entries are included.

	A	**B**
1.	ID	Unique identifier for each update mechanism, starting with UpdMech-1.
2.	Description	A brief description of the update mechanism, including its main features. In addition, it is necessary to specify whether the delivery of the update is network-based.
3.	Security guarantees	A description of the security objectives achieved and the threats to be addressed by the mechanism. In addition, for the sake of authenticity and integrity, it is necessary to indicate whether the security guarantee is provided by the VE itself.
4.	Cryptographic details	A description of the cryptographic methods (protocols, operations, primitives, modes and key sizes) used to ensure the safety of the key management update mechanism and to facilitate the described “Security Guarantees”. Method of installing public keys for verification.
5.	Initiation and interaction	A brief description of how the update is initiated and a brief description of the user interaction needed to initiate and apply the update, indicating whether it is an automatic update mechanism.
6.	Configuration	A brief description of how the user can configure the automation and notification of software updates, and what options (e.g. authorisation, blocking, postponement) the user may choose from. The default configuration should also be specified here.

7.	Update check	A brief description of the query mechanism and timing for the availability of security updates and whether the availability of the security update is verified by VE itself.
8.	User notification	A brief description of how the user is informed of the available update and the disruptions caused by the update mechanism, e.g. the limited availability of certain features, indicating the information contained in the notification and whether the notification is implemented by VE itself.
9.	Version management	A brief description of how VE checks and validates the update version before installation.

2.2.14. MD 14-SecParam: Safety parameters

The MD lists all sensitive (public and critical) safety parameters that are permanently stored on VE during normal use, with the following parameters:

	A	**B**
1.	ID	Unique identifier for each parameter, starting with SecParam-1.
2.	Description	A brief description of the safety parameter, including its purpose, indicating that the safety parameter is a hard encoded unique device identifier used in the device for security purposes and is hard encoded in the source code of the device’s software.
3.	Place of storage	Location and method of storing the safety parameter.
4.	Type	Record whether the safety parameter is public or critical.
5.	Security guarantees	A description of the basic security objectives achieved and the threats against which the safety parameter is protected during long-term storage.
6.	Protection system	A description of the actions taken to achieve the security guarantees, including the authorisations and roles through which access to the parameter is possible, as well as the rights associated with each role.
7.	Allocation mechanism	If the “Type” indicates that the parameter is critical: a description of the mechanism through which the parameter is given a value.
8.	Communication mechanisms	A reference to the communication mechanisms used in MD 16-ComMech to communicate the parameters and an indication whether the communication takes place via remotely accessible interfaces.
9.	Creation mechanism	If the ‘Type’ indicates that the parameter is critical or it is used to verify the integrity and authenticity of software updates or to protect communication with related services: a description of the mechanism which is used to create values for the parameter and, in addition, an indication that the parameter is used to verify the integrity and authenticity of software updates or to protect communication with related services.

2.2.15. MD 15-SecMgmt: Safe management processes

The MD lists each safe management process for critical safety parameters that the manufacturer has implemented during the VE life cycle:

	A	**B**
1.	ID	Unique identifier for each process, starting with SecMgmt-1.
2.	Description	A brief description of the safe management process for the entire life cycle of critical safety parameters, with reference to the corresponding standard when an existing standard is used. The life cycle of critical safety parameters typically takes into account generation, provision, storage, updates, extraction, archiving, destruction, expiration processes and parameter vulnerability. During generation, the method of producing the random numbers used and the measurement of its entropy shall also be described. If there is a file integrity check, it should also be described how it is implemented.

2.2.16. MD 16-ComMech: Communication mechanisms

The MD lists all VE communication mechanisms, with the following detailed information:

	A	**B**
1.	ID	Unique identifier for each mechanism, starting with ComMech-1.
2.	Description	A brief description of the communication mechanism, including its purpose and a description of the protocol used. For standardised protocols, reference with a version number is sufficient. In addition, it should be indicated whether the mechanism is remotely available.
3.	Security guarantees	A description of the security objectives achieved and the threats to be addressed by the mechanism.
4.	Cryptographic details	A description of the cryptographic methods which are used to provide the communication mechanism (protocols, operations, primitives, modes and key sizes), taking into account key management, in order to achieve the objectives of the described “Security guarantees”.
5.	Resilience measures	A description of the actions to ensure that the relationship is established in an orderly manner, including the expected, operational and stable state leading to the achievement of a stable relationship.

2.2.17. MD 17-NetSecImpl: Network and security implementations

The MD lists all the implementations of the VE’s network and security functions.

	A	**B**
1.	ID	Unique identifier for each item, starting with NetSecImpl-1.
2.	Description	A brief description of the implementation of the network or security function, including its purpose and scope.

3.	Review/evaluation method	A description of the methodology used to review or evaluate implementation, including basic principles (e.g. audit, peer review, automatic code analysis) and a description of the scope of implementation covered by the methodology.
4.	Report	The result of the review or evaluation, or a reference to the certificate or assessment report demonstrating that the implementation has been assessed as successful.

2.2.18. MD 18-SoftServ: Software services

The MD lists all the VE software services, as follows:

	A	B
1.	ID	Unique identifier for each service, starting with SoftServ-1.
2.	Description	A brief description of the service, including its purpose, indicating whether the service is available and through which MD 7-Intf network interface and whether this is also the case in the initialised state.
3.	Status	An indication that the service is enabled or disabled in the initialised state.
4.	Explanation	If the service is authorised, an explanation why the service is necessary for the proper use or operation of VE.
5.	Configuration	If the service is available via a network interface: information on whether the service allows for a security-relevant change of the configuration and, if so, a brief description of the possible configuration. In the case of a third-party software component, a statement that the service is disabled by default.
6.	Authentication mechanism	If the service is available via a network interface: reference in MD 10-AuthMech to authentication mechanisms that are used for authentication before using the service.
7.	Third-party SW	An indication whether the software component originates from a third party. If so, a description of the separation procedure.

2.2.19. MD 19-CodeMin: Code minimisation

The MD lists the methods used to minimise the codes:

	A	B
1.	ID	Unique identifier for each method, starting with CodeMin-1.
2.	Description	A brief description of the method used to minimise the code to the required functionality.

2.2.20. MD 20-PrivlCtrl: Entitlement control

The MD lists all entitlement control mechanisms, as follows:

	A	B
1.	ID	Unique identifier for each mechanism, starting with PrivlCtrl-1.
2.	Description	A brief description of the mechanism to verify the rights and authorisations for the roles and the software on VE.
3.	Matrix	The authorisation matrix managed by the respective entitlement control mechanism.
4.	Authentication	Reference to the authentication mechanism required by the respective entitlement control mechanism.

2.2.21. MD 21-AccCtrl: Access protection

The MD lists the memory access protection mechanisms at the hardware level, as follows.

	A	B
1.	ID	Unique identifier for each mechanism, starting with AccCtrl-1.
2.	Description	A brief description of the hardware-level access control mechanism, including how VE's operating system supports it.

2.2.22. MD 22-SecBoot: Secure system boot mechanisms

The MD lists all VE's secure boot mechanisms, as follows:

	A	B
1.	ID	Unique identifier for each mechanism, starting with SecBoot-1.
2.	Description	A brief description of the mechanism used for VE's secure boot process (including safety assumptions) and identification of the protected part of the software. Special attention should be given to all control options, API calls that affect the operation of the mechanism. If VE uses a backup of the protected software, its use is also included in the description.
3.	Security guarantees	A description of the implemented security objectives of the mechanism. The mechanisms implement the authenticity and integrity of the kernels of the operating systems.
4.	Detection mechanisms	A description of the mechanism for detecting the unauthorised modification of the VE software.
5.	User notification	A brief description of how the user is informed of any unauthorised modification of the software, as supplementary information indicating what information is contained in the notification.
6.	Notification functions	A brief description of the network functions required for user notification.

2.2.23. MD 23-Store: Storage and restoration

The MD lists the way in which the data processed by VE is stored and how the data can be restored, as follows:

	A	B
1.	ID	Unique identifier for each storage method, starting with Store-1.
2.	Storage product	The method and place how and where the data, processed by VE, are stored.
3.	Redundancy	In the event of a failure in the storage mechanism, its replacement mechanism.
4.	The method of data restoration	The way historical data are restored in the event of a failure of primary storage or VE.
5.	Encryption	The encryption algorithm used on the storage product, indicating whether encryption is enabled in the factory default state, and how and with what role can the encrypted storage be configured by the user.

2.2.24. MD 24-DataSec: Data protection

The MD lists all the data processed by VE, with the exception of telemetry data, as follows:

	A	B
1.	ID	Unique identifier for each data, starting with DataSec-1.
2.	Description	A brief description of the category of data which is processed by VE. Personal data is information about any identified or identifiable natural person.
3.	Processing activities	A description of the processing of data, describing all the parties concerned and the purposes for which the data are processed.
4.	Communication mechanisms:	Reference to the MD 16-ComMech communication mechanisms which is used to communicate the data and an indication whether the communication partner is an associated service (yes/no). A blank list of communication mechanisms indicates that the data is not transmitted.
5.	Sensitivity	An indication of whether the data is sensitive data. Sensitive data is any data the disclosure of which is likely to cause harm to the data subject. What qualifies as sensitive data may vary by product and usage, but examples include payment information, content of communication data and time-stamped location data.
6.	Obtaining consent	If personal data are processed on the basis of the data subject’s consent: a description of how consent is obtained.
7.	Withdrawal of consent	Where personal data are processed on the basis of the data subject’s consent: a description of how the data subject can withdraw his or her consent to the processing of the personal data.
8.	Cryptographic	The cryptographic algorithm which is used to protect personal data, with

	protection	reference to MD 12-SoftComp.
9.	Storage product	Storage product(s) for storing data, according to MD 23-Store.

2.2.25. MD 25-ExtSens: External sensors

The MD lists all VE's external sensing capabilities, as follows:

	A	B
1.	ID	Unique identifier for each sensor, starting with ExtSens-1.
2.	Description	A brief description of the sensing ability.

2.2.26. MD 26-ResMech: Resilience mechanisms

The MD lists all resilience mechanisms for VE's network disconnection or power failure, as follows:

	A	B
1.	ID	Unique identifier for each mechanism, starting with ResMech-1.
2.	Description	A description of the resilience mechanism that contributes to VE's resilience to grid and power outages.
3.	Type	The resilience mechanism is used to handle disruption in the network connection or a power outage, or to manage both.
4.	Security guarantees	A description of the security objectives achieved and the threats that the mechanism should address.

2.2.27. MD 27-TelData: Telemetry data

The MD lists all telemetry data collected by VE, as follows:

	A	B
1.	ID	Unique identifier for each data, starting with TelData-1.
2.	Description	A brief description of the telemetry data collected by VE and provided to the manufacturer.
3.	Purpose	A brief description of the purposes for which the data is collected.
4.	Safety test	If the data is used for safety testing, a description of how and by whom (device or related service) are telemetry data examined for security disorders.
5.	Data connections	Reference in MD 24-DataSec to data processed in telemetry data.

2.2.28. MD 28-DelFunc: Deletion functions

The MD lists all the deletion functions for user data, as follows:

	A	**B**
1.	ID	Unique identifier for each deletion function, starting with DelFunc-1.
2.	Description	A brief description of the function which is used to delete the user’s data. If the “Target type” indicates that it is addressed to a related service, the related service covered by the function shall also be indicated.
3.	Target type	Indication whether the function applies to user data on the device or personal data processed in related services, or both.
4.	Initiation and interaction	A brief description of the user interaction which is needed to start and apply the deletion function.
5.	Confirmation	A brief description of how the user receives an indication that the data concerned has been deleted, after the deletion function has been applied.

2.2.29. MD 29-UserDec: User decisions

The MD lists all the decisions that need to be taken during installation and maintenance, as follows:

	A	**B**
1.	ID	Unique ID for each decision, starting with UserDec-1.
2.	Description	A description of the decisions to be taken by the user within the framework of the installation and maintenance processes, including the user’s role in the installation or maintenance process.
3.	Options	A description of security-relevant options that the user may choose from and an indication of the default value.
4.	Decision	A brief description of how the decision is made, specifying whether the decision can also be made by the end-user.

2.2.30. MD 30-UserIntf: User interfaces

The MD lists all VE user interfaces that allow user input, as follows:

	A	**B**
1.	ID	Unique identifier for each interface, starting with UserIntf-1.
2.	Description	A description of the purpose, function and input fields of the user interface allowing the user to enter data, also explaining how the user can access the interface.
3.	Configuration interface	An indication whether the interface can be used for VE configuration.

4.	Communication mechanism	If the interface can be used for VE configuration, then a reference to communication mechanisms in MD 16-ComMech, which is used to protect the interface.

2.2.31. MD 31-ExtAPI: External APIs

The MD lists all VE APIs that allow data input from external sources, as follows:

	A	**B**
1.	ID	Unique identifier for each API, starting with ExtAPI-1.
2.	Description	A description of the VE API allowing input from external sources. External APIs are typically used for machine-to-machine communication.

2.2.32. MD 32-InpVal: Data entry validation

The MD lists all VE data entry validation methods, as follows:

	A	**B**
1.	ID	Unique identifier for each method, starting with InpVal-1.
2.	Description	A description of the method which is used to validate the data entered through user interfaces or transmitted through APIs or between networks in services and devices, including the management of unexpected data. It is also necessary to specify which of the data entry sources are targeted by the method. In order to validate data entry, it is possible to verify whether the data is of the permissible type (format and structure), the permissible value, the number or the order allowed.

2.2.33. MD 33-Notif: Notifications

The MD shall include all modes of user notifications, as follows:

	A	**B**
1.	ID	Unique identifier for each notification method, starting with Notif-1.
2.	Mode of notification	A description of which MD 7-Intf interface the notification appears on and to which users.
3.	Management of notifications	Actions to be performed by the user in connection with the notification.
4.	Contents	The content of notifications if they can be configured, a description of the MD 9-Role role with which the user can configure the data content and at what depth.

2.2.34. MD 34-AuditLog: Log data

The MD lists all VE logging methods, as follows:

	A	**B**
1.	ID	Unique ID for each log element, starting with AuditLog-1.
2.	Description	The scope of the logging activity, the content of the logs.
3.	Security guarantees	A description of the basic security objectives achieved and the threats against which log data are protected during long-term storage.
4.	Protection system	A description of the actions taken to achieve the security guarantees, describing the authorisations and roles through which access to the parameter is possible, including the rights associated with each role.

3. Document underpinning the assessment

3.1. The manufacturer shall issue an assessment document, which substantiates compliance with the requirements set out in Annex 2 with respect to the assurance level for the VE subject to testing (hereinafter referred to as: EMD).

3.2. The document shall include a list of the requirements set out in Annex 2 for the target assurance level, as well as the following information:

a) manufacturer’s classification: manufacturer’s statement of compliance with that requirement. It may have the following values:

   (aa) “Not applicable”: this may be used if the requirement is not applicable in relation to VE, and the physical design, the intended functions and the area of use of VE do not allow the requirement to be met.

   (ab) “Applicable and fulfilled”: this may be used if the requirement for VE is applicable and VE fulfils the requirement.

b) method of fulfilment: In case of the marking ‘applicable and fulfilled’, a description of which components included in the MD are concerned in relation to the requirement and how they fulfil the requirement individually or together.

c) explanation: In the case of the marking ‘not applicable’, the statement of reasons in the light of all the circumstances.

<u>*Annex 2 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)*</u>

Set of requirements

1. As regards the safety requirements, the requirements that must be met by the device defined in the IoT device identification document in point 1 of Annex 1, per assurance level, are specified in columns C to E.

2. The requirements have been developed subject to the following European and national standards:
   (a) ETSI EN 303 645 V2.1.1,
   (b) NIST Special Publication 800-213A and
   (c) NIST Special Publication 800-53 Revision 5.

3. In any column
   (a) the lines marked with '-' indicate the names of the control families;
   (b) 'X' indicates that compliance with the safety requirement in that row is mandatory at the assurance level specified in columns C to E;
   '0' indicates that compliance with the safety requirement in that row is not mandatory at the assurance level specified in columns C to E.

	A	B	C	D	E
1.	**Identifier**	**Description**	**basic**	**significant**	**high**
2.		DEVICE IDENTIFICATION	-	-	-
3.		Device identification	-	-	-
4.	DEVID-1	The model marking of the IoT device is clearly recognisable, either on the label on the device or through a physical interface.	X	X	X
5.	DEVID-2	The IoT device has a unique logical identifier that can be retrieved through an interface or can be found on the device.	X	X	X
6.	DEVID-3	It is possible to define the unique identifier and model marking of an IoT device that can be remotely controlled.	X	X	X
7.	DEVID-4	The IoT tool provides for the possibility to add a unique physical identifier that can be accessed by authorised entities.	0	X	X

8.		Performance of operations			
9.	DEVOP-1	The IoT tool is able to perform operations that may occur with the identification or use of the device.	X	X	X
10.	DEVOP-2	The IoT tool is able to distinguish between identified and unidentified users.	X	X	X
11.	DEVOP-3	Non-authorised users cannot become aware of the unique logical IoT device identifier.	0	X	X
12.	DEVOP-4	Knowing the IoT device identifier, the current software version can be verified.	0	X	X
13.	DEVOP-5	For the purpose of identifying and managing network devices, the device identifier may be used to detect the IoT device.	0	0	X
14.		Support for device identification	-	-	-
15.	IDSUPP-1	The IoT tool is able to advertise itself to other assets as a pre-identified entity.	0	X	X
16.	IDSUPP-2	Verification of the authenticity of other IoT devices is ensured.	0	X	X
17.	IDSUPP-3	In the case of network and remote network connections, the IoT device performs cryptographic bidirectional identification before building the identified connection.	0	0	X
18.	IDSUPP-4	The IoT tool supports certificate-based identification and authentication.	0	0	X
19.		DEVICE CONFIGURATION	-	-	-
20.	DEVCONF-1	The setting of the logical access rights, the configuration of the IoT device – in accordance with the ‘External connections, interface control’ requirements – is only possible through privileged users.	X	X	X
21.	DEVCONF-2	Only authorised users can configure the IoT device identification policy and the access restrictions lists in accordance with the ‘External connections, interface control’ requirements.	X	X	X
22.	DEVCONF-3	Only authorised users can configure the logical and physical interfaces of the IoT device in accordance with the ‘External connections, interface control’ requirements.	X	X	X
23.	DEVCONF-4	Authorised users can configure the software settings of the IoT device.	X	X	X
24.	DEVCONF-5	Authorised users can restore the IoT device to its factory status.	X	X	X
25.	DEVCONF-6	Authorised users can restore the IoT device to a previous secure state other than the factory state.	0	0	X
26.	DEVCONF-7	The previous configuration status is ensured during, or after servicing, repairing the IoT device.	0	X	X
27.		DATA PROTECTION	-	-	-
28.		Cryptographic support	-	-	-
29.	CRYPT-1	The IoT tool provides a cryptographic algorithm of sufficient strength and efficiency to protect the data.	X	X	X

30.	CRYPT-2	The IoT tool is capable of validating individual certificates.	0	X	X
31.	CRYPT-3	Digital signature verification is ensured.	0	X	X
32.	CRYPT-4	The IoT tool can run Hash algorithms.	X	X	X
33.	CRYPT-5	They can be updated to the recommended versions of cryptographic algorithms and primitives.	0	X	X
34.	CRYPT-6	The source code of the device does not contain any hard-coded critical safety parameters.	0	X	X
35.	CRYPT-7	The critical safety parameters, which are used to verify the integrity and authenticity of software updates and to protect communications in device software with related services, are unique for each device and are produced with a mechanism that reduces the risk of automated attacks.	X	X	X
36.		Support for cryptographic keys	-	-	-
37.	CRYKEY-1	The IoT device manages cryptographic keys securely.	X	X	X
38.	CRYKEY-2	The IoT tool is capable of generating key pairs.	X	X	X
39.	CRYKEY-3	The IoT device stores the cryptographic keys securely.	X	X	X
40.	CRYKEY-4	The IoT device makes changes to the cryptographic keys securely.	X	X	X
41.	CRYKEY-5	The IoT tool checks the cryptographic keys generated by external systems.	0	X	X
42.		Safe storage	-	-	-
43.	SECSTR-1	The IoT device does not store and transmit passwords, excluding the storage of the hash value generated from the password with the irreversible cryptographic splitting function.	X	X	X
44.	SECSTR-2	Safe storage may be permitted through the IoT device or its interface.	X	X	X
45.	SECSTR-3	In factory state, secure, safe and encrypted storage of the data is allowed.	X	X	X
46.	SECSTR-4	Protection of personal data is ensured in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).	X	X	X
47.	SECSTR-5	The IoT device, including the cloud infrastructure that ensures access to the data, stores only the amount of data needed for its operational operation.	X	X	X
48.	SECSTR-6	The IoT device can store data locally encrypted.	X	X	X
49.	SECSTR-7	Remote system elements related to the IoT device (e.g. cloud) store the data in an encrypted form.	0	X	X
50.	SECSTR-8	Sensitive safety parameters are stored in persistent storage.	0	X	X
51.	SECSTR-9	System and user data are placed on separate partitions.	0	X	X

52.	SECSTR-10	Secure data backup is ensured.	0	X	X
53.	SECSTR-11	User data stored locally on the IoT device can be easily and irrecoverably deleted.	X	X	X
54.	SECSTR-12	User data stored by remote system elements associated with the IoT device can be easily deleted.	0	X	X
55.		Secure data transfer	-	-	-
56.	SECDT-1	The data flow on the input and output interfaces of the IoT device is secure.	X	X	X
57.	SECDT-2	The cryptographic algorithm for secure data transmission can be configured.	0	X	X
58.	SECDT-3	The IoT device has protection against unauthorised access and modification in the data connection environment.	X	X	X
59.	SECDT-4	The IoT tool checks the integrity of the transmitted and received data by using a cryptographic solution.	0	X	X
60.		LOGICAL ACCESS TO INTERFACES	-	-	-
61.		Support for identification	-	-	-
62.	AUTH-1	The IoT tool supports authentication methods.	X	X	X
63.	AUTH-2	The IoT tool is capable of requiring an authentication method to build connections, especially in the case of remote connections.	X	X	X
64.	AUTH-3	For specific user populations the IoT tool supports a multi-factor authentication method.	0	X	X
65.	AUTH-4	If your IoT device uses factory default passwords, they are unique for each device.	0	X	X
66.	AUTH-5	When generating factory default passwords, the IoT tool uses a generation algorithm that reduces the risk of automatic attacks.	0	X	X
67.	AUTH-6	Changing a credential corresponding to the authentication mechanism in use is simply ensured to the user.	X	X	X
68.	AUTH-7	The IoT tool hides the data during the authentication process.	X	X	X
69.	AUTH-8	The IoT tool supports a standardised, uniform authentication method. (e.g. SAML, OAuth2)	0	X	X
70.	AUTH-9	For remote access, the IoT device checks the authentication data per operation.	0	0	X
71.	AUTH-10	By providing a hidden feedback of the information contained in the feedback of the authentication method, the IoT device ensures that authentication identifiers do not get known to and cannot be reused by unauthorised persons.	X	X	X
72.		Identification configuration	-	-	-
73.	IDENT-1	Throughout the life cycle of the IoT device, the methods, rules, and restrictions of authenticity can be set and changed.	0	X	X

74.	IDENT-2	The IoT tool supports account management in an automated way.	0	0	X
75.	IDENT-3	The number of failed identification attempts can be configured, after which the IoT device prohibits the user for a specified set time period.	0	X	X
76.	IDENT-4	The IoT tool supports the restoration of an account that is prohibited due to unsuccessful identification attempts with an alternative method of identification.	0	0	X
77.	IDENT-5	The IoT tool provides feedback on the date of the last successful authentication.	0	X	X
78.	IDENT-6	The IoT tool supports the log-out of inactive accounts, the duration of which can be configured.	X	X	X
79.	IDENT-7	The IoT device automatically prohibits temporary user accounts in a configurable way.	0	X	X
80.	IDENT-8	The IoT tool logs unsuccessful login attempts,which can be reported.	X	X	X
81.	IDENT-9	The IoT device indicates the number of unsuccessful login attempts to the user during the next successful login.	0	X	X
82.	IDENT-10	The IoT tool supports the authentication of external users and systems.	X	X	X
83.	IDENT-11	Access to user accounts, external users and systems can be revoked, in which case the IoT device breaks down the existing connection.	0	X	X
84.	IDENT-12	The IoT tool supports the setting of an expiration date for accounts, which will ensure that the account is blocked beyond the expiration date.	0	X	X
85.		User notification	-	-	-
86.	NOTIF-1	The status of the IoT device can be visually easily identified by checking the status indicators.	X	X	X
87.	NOTIF-2	The information displayed on the IoT device display can be configured.	0	X	X
88.	NOTIF-3	The IoT tool can send (in a configured way) notifications to users.	X	X	X
89.	NOTIF-4	The entire content of notifications with personal data and that of security notifications can only be disclosed after identification, and sensitive data will not be displayed in the warning message.	0	X	X
90.	NOTIF-5	The content of messages displayed by the IoT device can be configured.	0	X	X
91.	NOTIF-6	If the warning message appears on the IoT device display, the IoT device ensures that the message remains on the display until a user interaction.	0	X	X
92.		Support for access management	-	-	-
93.	ACCESS-1	The IoT device is resilient to unauthorised operations.	X	X	X
94.	ACCESS-2	The IoT device is capable of identifying authorised users and processes (e.g. connecting systems).	X	X	X
95.	ACCESS-3	The IoT device distinguishes between authorised and non-authorised users.	X	X	X
96.	ACCESS-4	Certain functions that can be defined by the operator are available without identification.	X	X	X

97.		Role support and management	-	-	-
98.	ROLE-1	The IoT device can manage multiple types of user accounts.	X	X	X
99.	ROLE-2	The IoT tool will separate at least the following types of user accounts: personal accounts (general and privileged), split privileged accounts.	0	X	X
100.	ROLE-3	The IoT tool supports the addition of user accounts.	0	X	X
101.	ROLE-4	Roles can be assigned to user accounts.	0	X	X
102.	ROLE-5	User accounts are provided with a unique identifier.	0	X	X
103.	ROLE-6	The IoT tool performs role-based logical access control.	0	X	X
104.	ROLE-7	Functions and processes that can be accessed by an administrator user with the roles may be configured.	0	X	X
105.	ROLE-8	Roles are compatible with standardised, unified authorisation methods, matching can be configured (e.g. LDAPS).	0	X	X
106.	ROLE-9	An administrator user can configure a new role.	0	0	X
107.	ROLE-10	By default, roles are designed according to the principle of minimum authorisation.	X	X	X
108.	ROLE-11	Configuration of access management to audit logs and security settings is supported.	0	X	X
109.	ROLE-12	The IoT tool allows you to set restrictive conditions for each type of user (e.g. time-based limitation, IP limit).	0	0	X
110.	ROLE-13	Authorisations and entitlements assigned to roles are checked in the case of user interactions which are aimed to achieve privileged functions and processes.	0	0	X
111.	ROLE-14	The authentication methods used for the various user accounts can be configured.	0	0	X
112.	ROLE-15	In the case of split accounts, permission for simultaneous log-in can be configured per account (prohibited in factory state).	0	X	X
113.	ROLE-16	The IoT device is able to enforce pre-set restrictions when using the device.	0	X	X
114.		External connections, interface control	-	-	-
115.	INTCTRL-1	The IoT device provides connection to external 3rd party systems with the use of a secure method.	X	X	X
116.	INTCTRL-2	The use of components of the IoT device may be restricted (ports, functions, input and output devices).	X	X	X
117.	INTCTRL-3	Physical or logical interfaces that are not necessary for the operation of the IoT device may be disabled.	X	X	X
118.	INTCTRL-4	Only the minimum logical and physical interfaces required for installation and putting into service are allowed in the factory default state.	X	X	X
119.	INTCTRL-5	In the factory default state, the IoT device protects against the retrieval of security information without identification.	X	X	X

120.	INTCTRL-6	The hardware does not expose physical interfaces to unnecessary risk.	0	X	X
121.	INTCTRL-7	The use of the services of the IoT tool may be restricted.	0	X	X
122.	INTCTRL-8	External access to the management interface may be disabled.	0	X	X
123.	INTCTRL-9	Access to the logical interfaces of the IoT device can be controlled.	X	X	X
124.	INTCTRL-10	The IoT device supports wireless connection, the secure and authorised authentication protocol of which can be configured.	X	X	X
125.	INTCTRL-11	If your IoT device has a debug interface, it is prohibited by software.	0	X	X
126.		SOFTWARE UPDATE	-	-	-
127.		Update capabilities	-	-	-
128.	UPD-1	The software of the IoT device can be safely updated as provided for by the software or through an interface.	X	X	X
129.	UPD-2	The software update can be done with an identified, authorised user account, supported by a secure and configurable mechanism.	0	X	X
130.	UPD-3	The current version of the software of the IoT device can be queried.	X	X	X
131.	UPD-4	Authorised accounts can restore the software to an earlier software version.	0	X	X
132.	UPD-5	Software updates come from an authoritative source and compliance with this condition is verified by the IoT device.	X	X	X
133.	UPD-6	Software updates do not cause a decrease in cyber security preparedness for the IoT device, and the IoT tool has a built-in method to verify this requirement.	0	X	X
134.		Management of updates through application support	0	0	0
135.	UPDCTRL-1	The IoT tool checks the authenticity and integrity of updates.	X	X	X
136.	UPDCTRL-2	You can turn off the automatic update of the IoT device.	X	X	X
137.	UPDCTRL-3	Manual and automatic update methods are supported.	X	X	X
138.	UPDCTRL-4	The update method can be selected.	X	X	X
139.	UPDCTRL-5	The software checks the availability of a new update at intervals which may be specified.	X	X	X
140.	UPDCTRL-6	New software versions are notified by the IoT device, but this function can be turned off.	X	X	X
141.	UPDCTRL-7	New software versions are notified by the IoT device, and the scope of those to be notified can be configured.	0	0	X
142.	UPDCTRL-8	The IoT device informs the user if the update poses a risk to the essential functioning of the IoT device.	0	X	X
143.		SUPPORT FOR EVENT MANAGEMENT	-	-	-

144.		Logging	-	-	-
145.	LOG-1	The IoT tool is capable of logging events.	X	X	X
146.	LOG-2	The IoT device supports an external logging system connection.	0	X	X
147.	LOG-3	The minimum content of the log entries is as follows: unique identifier of the IoT device, time signal, event source, event type, event classification, user ID or process identifier, event description.	0	X	X
148.	LOG-4	The IoT device is capable of logging network communications.	0	X	X
149.	LOG-5	The IoT device is able to log changes in the device configuration.	0	X	X
150.	LOG-6	The IoT device is able to log successful and unsuccessful access attempts.	X	X	X
151.	LOG-7	The IoT device is capable of logging its own state and that of its sensors.	0	X	X
152.	LOG-8	Based on the list of events that can be logged, the events to be logged can be configured.	0	0	X
153.	LOG-9	The status of the IoT device can be queried via the interface.	0	X	X
154.	LOG-10	You can set the maximum retention time of events, the number of log events stored, and the maximum size of the log file.	0	X	X
155.	LOG-11	Complete deletion of log files beyond the retention criteria on the IoT device is ensured.	0	X	X
156.		Time signal management	-	-	-
157.	TIMESTP-1	The time-signalling of events logged by the IoT device shall be accurate to at least seconds.	0	X	X
158.	TIMESTP-2	The IoT device supports an NTP network protocol.	0	X	X
159.	TIMESTP-3	A reliable time source can be configured.	0	X	X
160.	TIMESTP-4	The IoT device uses a standard time signal that can be traced back to UTC.	0	X	X
161.		Support for event management	-	-	-
162.	INC-1	The IoT device sends a warning about configured incidents that are considered a security incident.	0	X	X
163.	INC-2	The IoT device sends a warning about configured incidents that are considered to be security incidents to the associated information systems.	0	0	X
164.	INC-3	The warning mode can be configured.	0	0	X
165.	INC-4	The IoT tool supports an alternative logging solution in the event of a failure of the primary logging mechanism.	0	0	X
166.		ASSET SECURITY	-	-	-
167.		Secure communication	-	-	-
168.	SECCOM-1	The initiation and closure of a connection with other devices is done securely.	X	X	X

169.	SECCOM-2	The IoT device is capable of enforcing traffic management rules.	0	X	X
170.	SECCOM-3	The IoT device uses standardised protocols during communication.	X	X	X
171.	SECCOM-4	The IP address of the IoT device can be set.	X	X	X
172.	SECCOM-5	The ports of the IoT device interfaces can be configured.	0	X	X
173.	SECCOM-6	The IoT device has DNS support.	X	X	X
174.		Safe use of resources	-	-	-
175.	RESRC-1	The IoT tool is able to share resources.	0	X	X
176.	RESRC-2	The IoT device can assign memory areas to processes.	0	X	X
177.	RESRC-3	The various processes do not reach the memory area assigned to another process.	0	X	X
178.	RESRC-4	The memory area is only accessible through the kernel.	0	X	X
179.	RESRC-5	Memory is protected by hardware-based access control.	0	X	X
180.	RESRC-6	Quotas can be allocated to the use of disks.	0	0	X
181.	RESRC-7	In case of loss of network connection, limited operation is ensured.	X	X	X
182.	RESRC-8	The IoT device supports compressed data storage.	0	0	X
183.		Integrity protection	-	-	-
184.	INT-1	The IoT device has protection against running a unique code from a non-authoritative source.	0	X	X
185.	INT-2	The IoT device has the ability to detect unwanted hardware and software modification.	0	X	X
186.	INT-3	The IoT device has a security compliance check function for base configuration.	0	X	X
187.	INT-4	The IoT device has an integrity check function.	0	X	X
188.	INT-5	The IoT tool checks its software by using secure system boot mechanisms.	0	X	X
189.	INT-6	If the IoT device detects unauthorised changes to the software, it alerts the user or administrator of the problem and does not connect to networks wider than those required for the alert function.	0	X	X
190.	INT-7	The IoT tool is capable of detecting manipulation during the development life cycle of the system.	0	0	X
191.	INT-8	The running environment is stored on read-only media.	0	X	X

Annex 3 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)

Requirements affected by vulnerability testing

A vulnerability test shall be carried out for the following requirements of Annex 2 during the assessment:

	A	B
1.	**Identifier**	**Description**
2.	DEVID-3	It is possible to define the unique identifier and model marking of an IoT device that can be remotely controlled.
3.	DEVID-4	The IoT tool should provide for the possibility to add a unique physical identifier to which authorised entities have access.
4.	DEVOP-3	Non-authorised users cannot become aware of the unique logical IoT device identifier.
5.	IDSUPP-2	Verification of the authenticity of other IoT devices is ensured.
6.	IDSUPP-3	In the case of network and remote network connections, the IoT device performs cryptographic bidirectional identification before building the identified connection.
7.	IDSUPP-4	The IoT tool supports certificate-based identification and authentication.
8.	DEVCONF-1	The configuration of the logical access rights, the configuration of the IoT device, as described in the ‘Logical access to interfaces’ section, is only possible through privileged users.
9.	DEVCONF-2	Only authorised users can configure the IoT device identification policy and the access restrictions lists. As described in the ‘Logical access to interfaces’ section.
10.	DEVCONF-3	Only authorised users can configure the logical and physical interfaces of the IoT device, in accordance with the ‘Logical access to interfaces’ section.
11.	CRYPT-1	The IoT tool provides a cryptographic algorithm of sufficient strength and efficiency to protect the data.

12.	CRYPT-2	The IoT tool is capable of validating individual certificates.
13.	CRYPT-3	Digital signature verification is ensured.
14.	CRYPT-4	The IoT tool can run Hash algorithms.
15.	CRYPT-6	The source code of the device does not contain any hard-coded critical safety parameters.
16.	CRYPT-7	The critical safety parameters, which are used to verify the integrity and authenticity of software updates and to protect communication with related services in the device software, shall be unique for each device and produced with a mechanism that reduces the risk of automated attacks against asset classes.
17.	CRYKEY-1	The IoT device manages cryptographic keys securely.
18.	CRYKEY-2	The IoT tool is capable of generating key pairs.
19.	CRYKEY-3	The IoT device stores the cryptographic keys securely.
20.	CRYKEY-4	The IoT device makes changes to the cryptographic keys securely.
21.	CRYKEY-5	The IoT tool checks the cryptographic keys generated by external systems.
22.	SECSTR-1	The IoT device does not store and transmit passwords, excluding the storage of the hash value generated from the password with the irreversible cryptographic splitting function.
23.	SECSTR-4	Protection of personal data is ensured in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
24.	SECDT-3	The IoT device has protection against unauthorised access and modification in the data connection environment.
25.	SECDT-4	The IoT tool checks the integrity of the transmitted and received data by using a cryptographic solution.
26.	AUTH-3	For specific user populations the IoT tool supports a multi-factor authentication method.

27.	AUTH-5	When generating factory default passwords, the IoT tool uses a generation algorithm that reduces the risk of automatic attacks.
28.	AUTH-7	The IoT tool hides the data during the authentication process.
29.	AUTH-8	The IoT tool supports a standardised, uniform authentication method. (e.g. SAML, OAuth2)
30.	AUTH-9	For remote access, the IoT device checks the authentication data per operation.
31.	AUTH-10	By providing a hidden feedback of the information contained in the feedback of the authentication method, the IoT device ensures that authentication identifiers do not get known to and cannot be reused by unauthorised persons.
32.	IDENT-10	The IoT tool supports the authentication of external users and systems.
33.	NOTIF-4	The entire content of notifications with personal data and that of security notifications can only be disclosed after identification, and sensitive data will not be displayed in the warning message.
34.	ACCESS-1	The IoT device is resilient to unauthorised operations.
35.	ROLE-12	The IoT tool allows you to set restrictive conditions for each type of user (e.g. time-based limitation, IP limit).
36.	INTCTRL-2	The use of components of the IoT device may be restricted (ports, functions, input and output devices).
37.	INTCTRL-3	Physical or logical interfaces that are not necessary for the operation of the IoT device may be disabled.
38.	INTCTRL-4	Only the minimum logical and physical interfaces required for installation and putting into service are allowed in the factory default state.
39.	INTCTRL-5	In the factory default state, the IoT device protects against the retrieval of security information without identification.
40.	INTCTRL-8	External access to the management interface may be disabled.
41.	INTCTRL-9	Access to the logical interfaces of the IoT device can be controlled.

42.	INTCTRL-10	The IoT device supports wireless connection, the secure and authorised authentication protocol of which can be configured.
43.	INTCTRL-11	If your IoT device has a debug interface, it is prohibited by software.
44.	UPD-4	Authorised accounts can restore the software to an earlier software version. (e.g. downgrade attack)
45.	UPD-5	Software updates come from an authoritative source and compliance with this condition is verified by the IoT device.
46.	SECCOM-2	The IoT device is capable of enforcing traffic management rules.
47.	RESRC-3	The various processes do not reach the memory area assigned to another process.
48.	RESRC-4	The memory area is only accessible through the kernel.
49.	RESRC-5	Memory is protected by hardware-based access control.
50.	INT-1	The IoT device has protection against running a unique code from a non-authoritative source.
51.	INT-2	The IoT device has the ability to detect unwanted hardware and software modification.
52.	INT-4	The IoT device has an integrity check function.
53.	INT-5	The IoT tool checks its software by using secure system boot mechanisms.
54.	INT-6	If the IoT device detects unauthorised changes to the software, it alerts the user or administrator of the problem and does not connect to networks wider than those required for the alert function.

<u>*Annex 4 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)*</u>

Evaluation methodology

1. The IoT device to be tested

1.1. The VE to be tested is a specific IoT tool which must be assessed in accordance with the provisions of this certification scheme. The manufacturer or conformity assessment body carrying out the assessment is able to control VE through the available interfaces and, based on the information provided in the MD, is partially aware of its design (grey box testing). The VE shall be in serviceable condition during the assessment and other related services shall be operational even if they are not verified by the manufacturer or by the conformity assessment body.

2. Document underpinning the assessment

2.1. The EMD mentioned in Annex 1 shall be prepared by the manufacturer with regard to the capabilities implemented and supported in VE, in accordance with the provisions of this certification scheme. In the EMD, the manufacturer shall declare that all the requirements set out in Annex 2 for the examined assurance level have been met.

3. Implementation document

3.1. The manufacturer shall prepare an MD as set out in Annex 1, which shall contain further and more detailed information to carry out the assessment. The MD is an underlying basis for the assessment methodology and includes some design details for the conformity assessment body.

3.2. The manufacturer shall provide complete, detailed and correct information when filling in the MD.

3.3. When completing the MD, the manufacturer may also refer to existing documentation, in which case it shall make the reference documentation available to the conformity assessment body.

4. The manufacturer's tasks and duties

4.1. The manufacturer, as the organisation initiating the assessment, requests the examination of a given VE under this certification scheme. The manufacturer will be the single point of contact for the conformity assessment body and shall be responsible for coordinating with parties involved in the VE's supply chain and ecosystem, in particular component manufacturers, service providers and application developers.

4.2. Third-party assessments of existing safety certificates or parts of VE may be used in part as evidence of compliance in order to reduce the resources and time needed for the assessment. In this case, the manufacturer shall indicate in the EMD that conformity has already been assessed, together with a reference to appropriate evidence. Furthermore, the manufacturer shall provide the conformity assessment body with all the information necessary for the verification of the evidence, in particular the details of the certification and the assessment reports. During the assessment, the conformity assessment body shall verify that the evidence is able to demonstrate compliance with the requirement set out in the said Annex 2.

5. The conformity assessment body's tasks and duties

5.1. The testing laboratory involved by the conformity assessment body shall carry out the VE's conformity assessment. The evaluation shall also take into account links with related services and the development and management processes of VE. In the case of conformity self-assessments, for the purposes of point 6, the conformity assessment body shall be understood as the manufacturer.

6. The evaluation procedure

6.1. The stages of the evaluation process are as follows:

6.2. For each of the requirements designated as 'Applicable and fulfilled' in the EMD, a conformity assessment body shall record the test cases in accordance with point 7 and develop a test plan for VE and perform the tests.

6.2. For each of the requirements indicated in the EMD, multiple test cases shall be tested in accordance with points 6.2.1 to 6.2.5.

6.2.1. Test case: *<requirement ID>-T0 – Applicability*

The purpose of the test:
The purpose of this test case is to assess the applicability of a specific requirement set out in Annex 2.

Test units:

a) A conformity assessment body shall verify that the manufacturer has designated the requirement as 'Applicable and fulfilled'.
b) Where the requirement has been classified as 'Applicable and fulfilled', a conformity assessment body shall examine whether the manufacturer has indicated the method of performance.
c) Where the requirement has been classified as 'Not applicable', the conformity assessment body shall examine and assess its justification.

Decision:
A 'Pass' decision may be made if:

- In case of the classification 'applicable and fulfilled', the 'Method of performance' has been completed.
- In case of the classification 'not applicable', the statement of reasons is well founded.

Otherwise, the decision is 'Fail'.

6.2.2. Test case: *<requirement ID>-T1 – Documentation*

Pre-requisite:

the requirement set out in Annex 2 is ‘Applicable and fulfilled’ pursuant to EMD and the previous test case (<requirement identifier>-T0) is assessed as ‘Pass’.

The purpose of the test:
The purpose of this test case is to establish that a specific Annex 2 requirement is documented. The test case is applicable to all assurance levels.

Test units:

> A conformity assessment body shall verify that compliance with the requirement has been properly documented by the manufacturer, identifying the MD elements that can be used to demonstrate compliance with that requirement.

Decision:
A ‘Pass’ decision can be made if the MD contains all the relevant information concerning the requirement.
Otherwise, the decision is ‘Fail’.

6.2.3. Test case: *<requirement identifier>-T2 – Conceptual testing*

Pre-requisite:
the requirement set out in Annex 2 is ‘Applicable and fulfilled’ pursuant to EMD and the previous test case (<requirement identifier>-T1) is assessed as ‘Pass’.

The purpose of the test:
The purpose of this test case is to establish the conceptual conformity of compliance with the Annex 2 requirement of the documentation. The test case is applicable to all assurance levels.

Test units:
A conformity assessment body shall verify that, on the basis of the information identified in the <requirement identifier>-T1 test case, VE conceptually meets the requirement set out in Annex 2.

Decision:
A ‘Pass’ decision may be made if, on the basis of the information identified in the <requirement identifier>-T1 test case, VE is conceptually compliant with the requirement set out in Annex 2 and the applied security control and implementation are risk-proportional to the assurance level.
Otherwise, the decision is ‘Fail’.

6.2.4. Test case: *<requirement identifier>-T3 – Implementation test*

Pre-requisite:
the requirement set out in Annex 2 is ‘Applicable and fulfilled’ pursuant to EMD and the previous test case (<requirement identifier>-T2) is assessed as ‘Pass’.

The purpose of the test:
The purpose of this test case is to establish compliance with the Annex 2 requirement by the documentation. The test case is applicable to all assurance levels.

Test units:

A conformity assessment body shall verify that the implementation has taken place in accordance with the information identified in the <requirement identifier>-T1 test case.

Decision:
A ‘Pass’ decision can be made if the implementation has been carried out on the basis of the information identified in the <requirement identifier>-T1 test case.
Otherwise, the decision is ‘Fail’.

6.2.5. Test case: *<requirement identifier>-T4 – Vulnerability test*

Pre-requisite:
the requirement set out in Annex 2 is ‘Applicable and fulfilled’ pursuant to EMD and the previous test case (<requirement identifier>-T2) is assessed as ‘Pass’.

The purpose of the test:
The purpose of this test case is to assess the requirement set out in Annex 3 with a vulnerability test method. The test case shall be applied at least at a ‘significant’ assurance level.

Test units:
The conformity assessment body shall verify whether there is a known vulnerability in respect of the solutions used and shall verify the fulfilment of the safety objective by means of a manual vulnerability test.

Decision:
A ‘Pass’ decision may be made if no vulnerability can be identified on the basis of the test.
Otherwise, the decision is ‘Fail’.

7. Result of assessment

As a result of the assessment, the test case results are recorded on a test case basis. The conformity assessment body shall draw up an assessment report on the implementation of the test cases, which shall include:

- the information recorded in the EMD,
- the test case identifiers for each requirement,
- the way test cases are evaluated,
- the facts underlying the decision concerning the test case,
- in the case of a test case for vulnerability testing, the test report,
- the decision concerning the test case,
- an overall assessment of the requirements.

Assessment of the requirement:

- ‘Fulfilled’ if all test cases related to the requirement ‘Pass’,
- The assessment brings a ‘Not fulfilled’ result if one of the test cases related to the requirement ‘Fail’.

A conformity statement or a national cyber security certificate may be issued if the VE is assessed as ‘Pass’ for all the requirements set out in the EMD.

Annex 5 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)

Declaration of Conformity

NATIONAL CYBER SECURITY CONFORMITY STATEMENT

Name of manufacturer:
Address of manufacturer:

Iot device	
name:	
version number:	
model number:	
assurance level:	

Other technical specifications, standards and procedures:

Scope and circumstance-based restriction:

Period of validity: **day**

I declare that the product described above complies with the requirements of the Decree of the Supervisory Authority for Regulatory Affairs on the national cyber security certification scheme for IoT devices.
I hereby declare that only *[name of manufacturer]* is authorised to issue this statement.

Date of issue: Click here to enter a date.

----
manufacturer's authorised signature

....
To be filled in by SZTFH.

Date of registration:	
Registration ID:	

SZTFH Supervisory Authority for Regulatory Affairs

Annex 6 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)

National CYBER SECURITY Certificate

NATIONAL CYBER SECURITY

CERTIFICATE

<Name of the conformity assessment body> (registered address), registered by the Supervisory Authority for Regulatory Affairs under registration number <registration number> as **a conformity assessment body** fulfilling the criteria to issue cyber security certificates at <assurance level> assurance level pursuant to the SZTFH Decree on the cyber security certification of information and communication technologies, **certifies** that the following IoT device, which was produced by

<name of manufacturer>,

namely

<IoT device name

meets the requirements set out in the Decree of the Supervisory Authority for Regulatory Affairs on the national cyber security certification scheme for IoT devices, at

<assurance level>

assurance level.

This certificate was issued on the basis of assessment report number <number>.

Created on behalf of the <Client's name> (registered office).

Period of validity: day

Date of issue: Click here to enter a date.

--- --

professional certifier of conformity assessment conformity assessment body

authorised signature

....

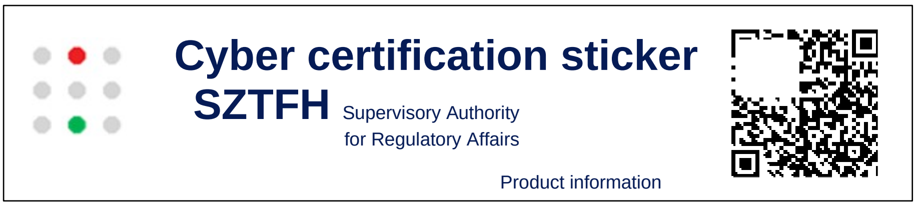
To be filled in by SZTFH.

Date of registration:	
Registration ID:	

Supervisory Authority
for Regulatory Affairs

Annex 7 to Decree No …/2024 (… …) of the Supervisory Authority for Regulatory Affairs (SZTFH)

Label and marking



Cyber certification sticker

SZTFH Supervisory Authority
for Regulatory Affairs

Product information