Data Security Examination Certificate No CH-DS-24034-01

Applicant	**Iskraemeco d.d.** Savska loka 4 4000 KRANJ Slovenia
Requirements	Ordinance of 14 March 2008 on the Supply of Electricity (StromVV, SR 734.71) Art. 8*b* Richtlinien für die Datensicherheit von intelligenten Messsystemen; RL-DSP – CH, Ausgabe 2018 (www.strom.ch) Richtlinien für die Datensicherheit von intelligenten Messsystemen, Anhang 1; RL-DSP – CH, Anhang 1, Ausgabe 2018 (www.strom.ch) Prüfmethodologie zur Durchführung der Datensicherheitsprüfung für Smart Metering Komponenten in der Schweiz, Version 2.1, 1. Juli 2019 (www.swissmig.ch)
Type of instrument	**HES – Head End System**
Type designation	**SEP2W System 2020 R3** and **Symbiot HES**
Confirmation	The present Data Security Examination Certificate certifies that the mentioned element of an intelligent measurement system has been successfully examined and registered as compliant with the above-mentioned requirements.
Certificate valid until	2 April 2029
Issuing Authority	Conformity Evaluation Body METAS-Cert

3003 Berne-Wabern, 14 January 2025

Approved by	Gulian Couvreur, Head of sector METAS-Cert

1 Component description

1.1 Main properties of iMS component (overview)

Table 1 – Component details

Type (Name of component)	**SEP2W System 2020 R3** and **Symbiot HES**
iMS component type	HES - Head End System
Description	Server software system
Component details	
Software version	**2.40.XXX.X (SEP2W)** **3.20.XXX.X (Symbiot)**
Operating system	Microsoft Windows Server 2012....and above 64-bit
Component services	distributed on different servers: - Integration servers - Application servers (Core, Manager, Web client, etc.) - communication servers
Infrastructure services	AD, SMTP, PKI, HSM
Software base	based on .NET framework, service- oriented architecture in modular design
KS3 (WAN – mandatory)	WAN - DLMS/COSEM over IPsec (over APN carrier)
KS0 (local, management purposes only)	sub-local HMI - Management (Mgmt): KMS and HMIs - Data Transfer: CIM-RabbitMQ
Data communication	IPSEC + Cosem/DLMS Security suite 0 (HES)
Meter management (Firmware, …)	MDM over https

1.2 Picture / Schema of iMS component

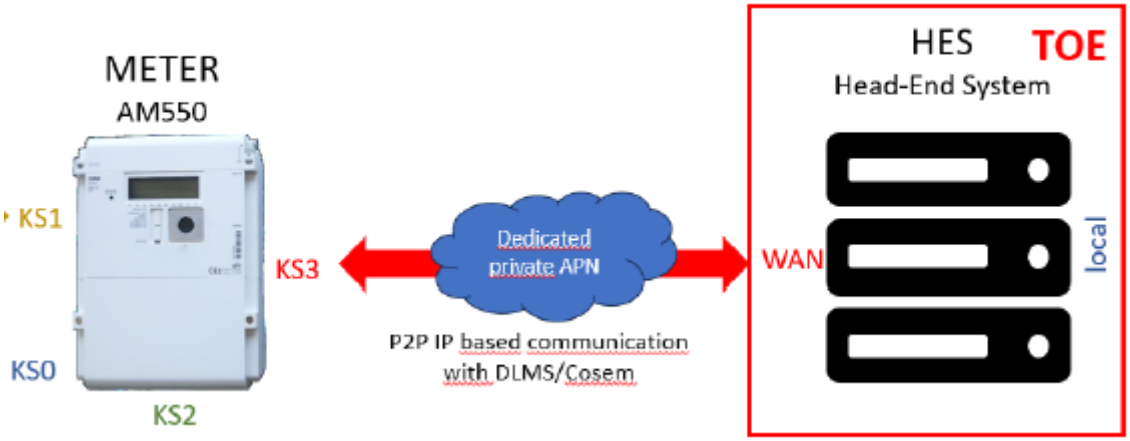

Fig. 1 – **Schematic picture of complete intelligent Measuring System (iMS) with iMS component SEP2W-HES (P2P connection)**

Fig. 2 – **Schematic picture of complete intelligent Measuring System (iMS) with iMS component SEP2W-HES (P2P connection via mobile router)**

1.3 Component specific Objects/Threats matrix (OT-Matrix)

For the Data Security Evaluation, the OT-Matrix helps to characterize the Devices under Test (DUT).

This Matrix was specified by the editors of the Testing Methodology (Swiss Manufacturer Association Swissmig) therein and is used in the SDCM-Document (SDCM = Smart Device Control Matrix).

Threats / Protected objects	B1: Unauthorized local modification of data	B2: Unauthorized remote modification of data	B3: Unauthorized time modification	B4: Unauthorized local data access	B5: Unauthorized remote data access	B6: Unauthorized data access of data stored on the device that is no longer processed	B7: Unauthorized operation of breaker	B8: Unauthorized operation of relay in Smart Meter	B9: Safe booting	B10: Restriction of data availability
O1: Meter	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O2: Visualization platform	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O3: KS0 Local administration interface	☑	☐	☐	☑	☐	☐	☐	☐	☑	☐
O4: KS3 interface WAN	☑	☑	☐	☑	☑	☐	☐	☐	☐	☑
O5: KS2 interface HAN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O6: KS1 interface LMN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O7: Crypto keys	☑	☐	☐	☑	☐	☐	☐	☐	☐	☐
O8: Firmware update	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐
O9: Firmware	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O10: Meter configuration data	☑	☐	☑	☑	☐	☐	☐	☐	☐	☑
O11: Time (system, RTC)	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐
O12: Grid data	☐	☑	☐	☐	☑	☑	☐	☐	☐	☑
O13: Workload, data in registers	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
O14: All data on Smart Meter	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑

1.4 Software / Firmware

- The software is installed on a specific server hardware, virtualized environment or as SaaS (Software/Sever as a Service) solution
- Software change/updated is done by updating relevant software component on the Head-End-System (HES)
- Indications of software version during start-up is not available (Server component)
- Current software version can be displayed/checked in the application

The approved software/firmware versions and their corresponding hash / signature / checksum are listed in following table:

Table 2 – Software/Firmware versions

Type	**Version**	**Signature** (certificate based) [SHA1 - Message Digest]	**Release date**	**Certificate Issue** [1]	**Valid**[2] **Y/N**
SEP2W	**2.40.XXX.X** (Major version)	0414 b651 d62a b2c8 9cce e599 0e24 326f 59dd 25f1 79c5 (for 2.40.476.1 - DUT version)	21.04.2021	00	Y
	2.40.476.1 (DUT version)				
Symbiot	**3.20.XXX.X** (Major version)	0414 658b b407 fb34 b7b3 946f 1b8f 416d c969 462e c76c (for 3.20.345.5 - DUT version)	11.12.2024	01	Y
	3.20.345.5 (DUT version)				

[1] Revision number of the type examination certificate

[2] Only valid software/firmware versions can be used

2 Evaluation Methodology / Evaluation results

Test laboratories evaluate single components as Targets of Evaluation (ToE) according following test methodology criteria:

1. Data Security Conception or Rationale

Outline of which vulnerable objects exist in a system, what threatens them from the point of view of data security (loss or restriction of confidentiality, integrity or availability) and which security functionalities should prevent this (correctness)

2. Product development, architecture, functionality

Description of the security architecture and security functionality of a system with regard to a correct implementation according to the data security conception (correctness)

3. Product Documentation

Guide, which enables operators - and particularly also test labs - to configure a system into a secure operating state

4. Product life cycle

Demonstration that all system components are identifiable and are protected against loss or restriction of confidentiality, integrity or availability in their complete lifecycles

5. Verification tests by the manufacturer (QM or similar) - voluntary

Proof that all security-relevant system components have passed acceptance tests with regard to correctness and effectiveness

6. Penetration tests of the test lab

Vulnerability analysis by a test lab to detect the presence of potential vulnerabilities (correctness) and to determine a measure of resilience of security against threats (effectiveness) equivalent to an attack potential of Enhanced-Basic according to the Common Criteria

3 Data security examination procedure and component documentation

The data security examination procedure is initiated by the applicant with an application to METAS-Cert specifying the element of an intelligent measurement system he wishes to have tested and the test laboratory with which he wishes to work. After successful review of the test object description and of the test laboratory qualification by METAS-Cert, the test laboratory is entrusted with the testing. The test laboratory submits a report to METAS-Cert on the testing conducted. METAS-Cert verifies the correctness of the test process and the results of the tests in compliance with the *Prüfmethodologie*. After this verification and consultation with the applicant, METAS issues the Data Security Examination Certificate.

All documents and drawings used for the data security examination procedure are deposited with METAS-Cert.

4 Conditions for market introduction

This Data Security Examination Certificate refers exclusively to the element of an intelligent measurement system described in paragraph 1. The holder of the certificate is obliged to ensure and on request to confirm that the marketed elements concerned (regardless, if via direct sales or reseller sales or system integrators) are conforming to the description in paragraph 1.

4.1 Specific obligations for market introduction (if any)

non

5 Requirements for production, commissioning and utilization

5.1 Information accompanying the component

The holder of this Data Security Examination Certificate is obliged to enclose information[3] and directions for use (operating manual) with the marketed equipment that enable the equipment users to operate the component in a secure way and in accordance with the regulations.

5.2 Disclaimer

This Data Security Examination Certificate certifies that the mentioned element of an intelligent measurement system has been successfully examined and registered as compliant with the above-mentioned procedural and content-related requirements at the date of issue of the present certificate. It does not cover the configuration and management of the other elements of an intelligent measurement system.

6 Validity of this Data Security Examination Certificate

During the period of validity of this Data Security Examination Certificate, the holder of this Data Security Examination Certificate shall inform METAS-Cert in respect of all occurrences that might jeopardise data security. METAS-Cert shall decide as to whether this calls for supplementary testing and a revision of this Data Security Examination Certificate. METAS may revoke this Data Security Examination Certificate during its period of validity if it must be assumed that data security is no longer guaranteed. METAS shall publish this Data Security Examination Certificate, as well as its revisions, revocation and expiration.

7 Certificate history

Issue	Date	Description
CH-DS24034-00	03.04.2024	- initial issue of certificate
CH-DS24034-01	14.01.2025	- addition of rebranded version "Symbiot"

Note: All revisions can be found on www.metas.ch/cs

[3] It is allowable to use a link (e.g. QR-Code) to a website, where the information can be downloaded. The holder of this Data Security Examination Certificate must ensure that the link works during ten years after the market introduction of the component.

8 Pictures and drawings

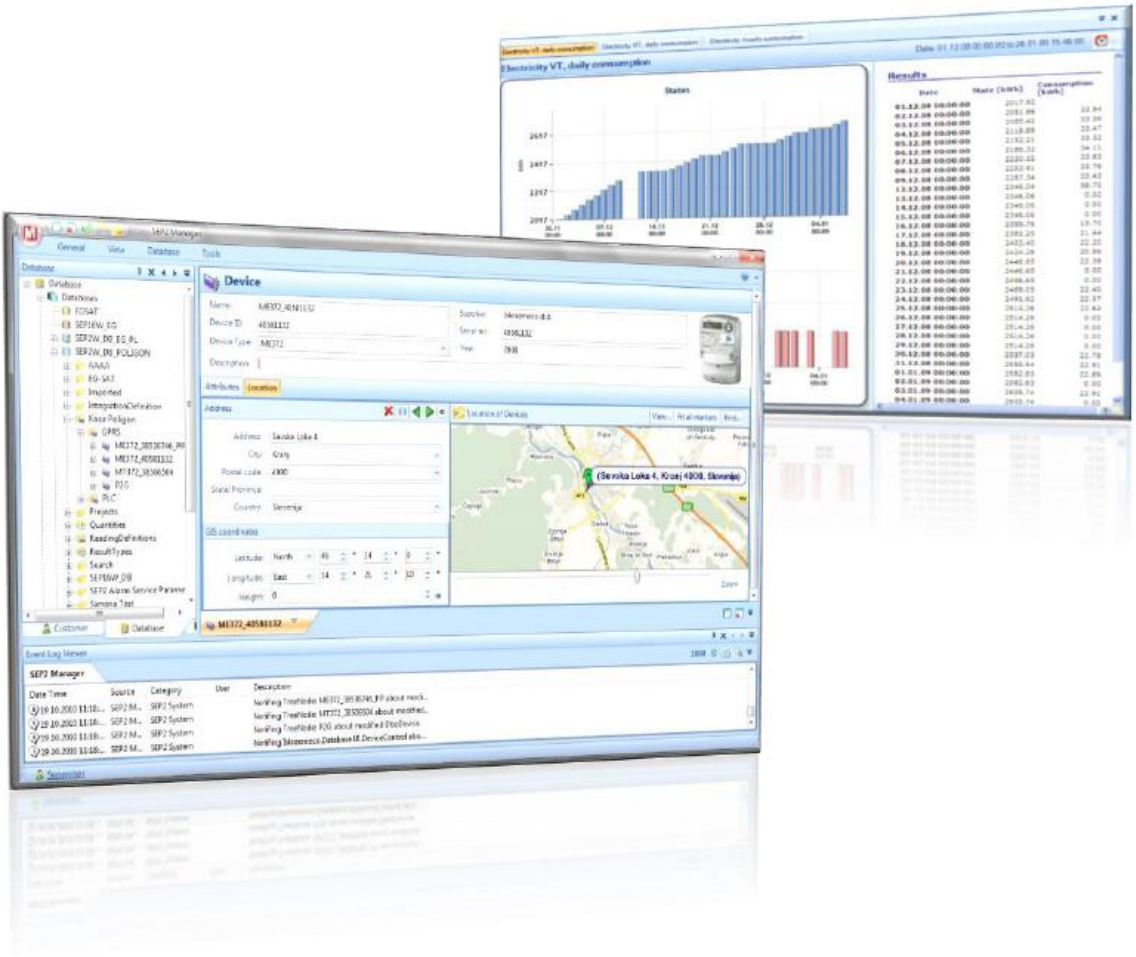

Fig. 3 – Example of a ISKRAEMECO HES type SEP2W

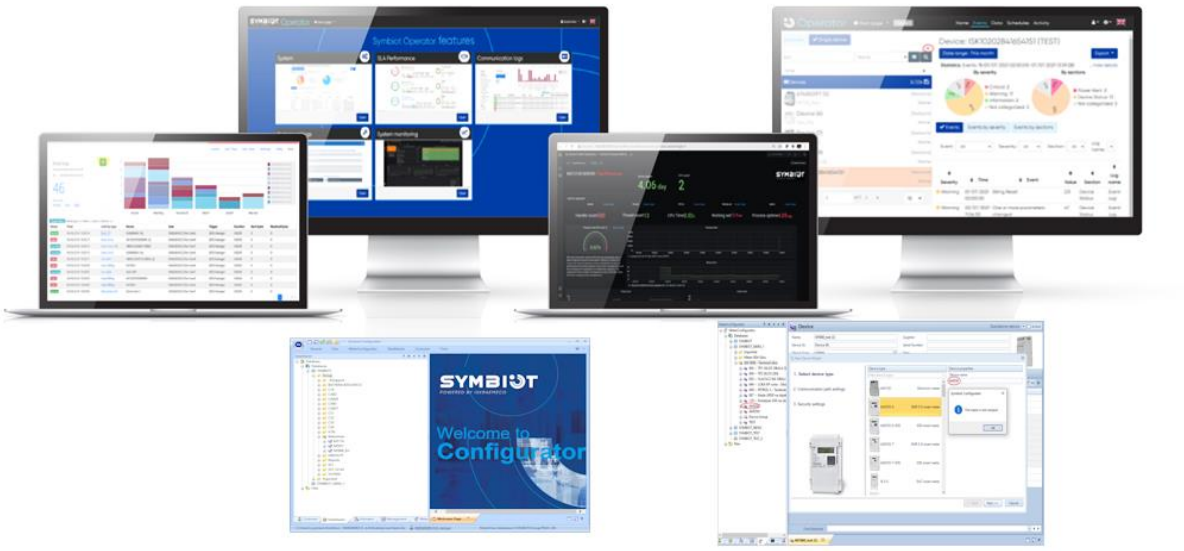

Fig. 4 – Example of a ISKRAEMECO HES type Symbiot