WELMEC

European cooperation in legal metrology

WELMEC Software Guide 7.2, draft 2019

A draft of document WELMEC Software Guide 7.2, 2019 is now in approval process. The draft includes editorial changes concerning translation comparison and house-keeping. Application of Extension T was clarified. Further amendments were done at requirements P6, U6 and T6. Reorganization between „Acceptable solution“ and “Specifying Notes” on each requirement took place. Chapter 11.1 “Information to be included in the type examination certificate” was adapted.

It will be issued after final approval.

Overview of more significant changes:

P2 (Software identification): The specifying note that the identifier(s) shall be displayed permanently on a secure plate, on command or on start-up was added.

P6 (Protection against inadmissible intentional changes): A specifying note for risk classes C and D was revised: if a checksum is used the algorithm shall have a key length of at least 4 bytes.

U2 (Software identification): The specifying note that the identifier(s) shall be displayed permanently on a secure plate, on command or on start-up was added.

U5 (Protection against accidental or unintentional changes): The specifying notes was added: Where the operating system allows it, it is recommended that all user rights for the deletion, moving or amendment of legally relevant software is removed, and access is

controlled via utility programs. And access control to legally relevant software by the use of passwords is recommended, as is the use of read-only mechanisms.

U6 (Protection against inadmissible intentional changes): A specifying note was revised: if a checksum is used the algorithm shall have a key length of at least 4 bytes.

L4 (Traceability of stored measurement data): The requirement L4 was reformulated. Stored measurement data shall be capable of being traced back to the measurement and measuring instrument that generated them. A prerequisite of the linking is an identification of measurements and an identification to the measuring instrument.

Extension T (Transmission of Measurement Data via Communication Networks): Application of Extension T was clarified. The specific requirements of this chapter only apply if measurement data is transmitted via communication networks to a distant device where it is used for legally relevant purposes at the receiver.

T4 (Traceability of transmitted measurement data): The requirement L4 was reformulated. Transmitted measurement data shall be capable of being traced back to the measurement and measuring instrument that generated them. A prerequisite of the linking is an identification of measurements and an identification to the measuring instrument.

T6 (Receiving, verification and handling of transmitted measurement data): The requirment was reformulated. There shall be legally relevant software for receiving, verifying and handling transmitted measurement data. Received measurement data shall indicate an eventual violation of authenticity traceability and integrity.

U6, L3, I5, T3, T4, T5, D2, D3: For risk class D: Concerning algorithms and minimum key lengths, that are applied as protection against intentional changes or as a quarantee of authenticity, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.

Chapter 11: Information to be included in the certificate

Information to be included in the type examination certificate was adapted. These information concerning software should be included in the certificate:

1. **Software type**
   - Indicate the version of WELMEC Guide 7.2, Type (P or U), the Risk Class (A to E) and the applicable Extensions (L, T, S , D, Ix)

Risk class [A-E] _	P ☐	U ☐	L ☐	T ☐	S ☐	D ☐	Ix ☐ [1-6] _

2. **Software identification**
   - Indicate the validated value(s) of the legally relevant software identifier(s).
   - Describe how to view the legally relevant software identifier(s).

3. **Integrity software verification**
   - **For risk classes C and more**, indicate the checksum or alternative method with the same level of requirement.
   - **For risk class C and more**, describe **precisely** how to view the checksum or alternative method with the same level of requirements.

Note: A reference to a document (e.g. user manual) is not suitable.

- Describe how to view the event counters / event loggers, if applicable.
- Description of hardware sealing(s) and other types of sealing(s) in relation with software, if applicable.
- Other means of integrity protection, if applicable.

4. Software environment short description

- Indicate relevant information concerning:
  - Software operating environment necessary to operate the software (e.g. Operating System).
  - Software modules under legal control (if software separation implemented).
  - Hardware and software interfaces (e.g. infrared, Bluetooth, Wireless LAN…).
  - Electronic (hardware) parts references and their locations in the measuring instrument including its securing, if needed.