Physikalisch-Technische Bundesanstalt
National Metrology Institute

Working group 8.51 “Metrological Software”

Last revision: May 19, 2021

Leaflet:
Setup of live media

1 General

This leaflet serves as a supplementary document to the leaflet “Configuration of general-purpose operating systems for measuring instruments” [1]. The requirements of this leaflet are applied *additionally* or in *modified* form.

If an indication program and a cryptographic library are used for legally relevant purposes on the live medium, they must be tested against the requirements of the WELMEC 7.2 Software Guide [2] and the leaflet "Special requirements for cryptographic modules" [3]. The strength of integrity protection for the live medium depends on the chosen risk class for the associated measuring instrument.

Each of the following requirements must be met by technical measures at the operating system or software application level. The implemented protective measures must be documented by the manufacturer and must comply with the state of the art.

Additionally, for examination according to the WELMEC 7.2 Software Guide [2] in higher risk classes, files for the legally relevant configuration of the live system shall be provided.

For a more detailed distinction of the liability of requirements, see RFC 2119 [4].

Remarks for terminology:

- The live system stored in logical form (ISO image) or in physical form (data carrier) is referred to as live medium.
- The running operating system with the indication program, launched from a live medium, is referred to as live system.

2 Hardware properties

There are no requirements to be met by the host computer environment for executing the live system.

3 Boot process and loading of the legally relevant software

When configuring the start process for the live system, it is additionally important to ensure that no inadmissible interaction with the host computer exists.

1. The boot process of the live system must be configured in a way that only the live system is loaded into the Random-Access Memory of the host computer or its virtualized environment.
2. Reproducibility: The live system must always be recoverable from the live medium in an identical form.

Remark: The reproducibility feature replaces the trust anchor for permanently installed operating systems.

The documentation must also contain a description of the configuration of the start process of the live system and its protective measures.

4 Admissible components

The requirements of the chapter from the leaflet "Configuration of general-purpose operating systems for measuring instruments" [1] apply without restriction.

5 Protection during use

For the live system, the following requirements apply in addition:

1. After finishing the boot process, the live system should turn into kiosk mode.
2. The reloading and execution of software from other data storage devices must be prevented.
3. The legally relevant data transmitted to the indication program must have an integrity protection and a proof of origin.
4. After the live medium has been placed on the market, the live system must no longer be administrable.

Remark: Other data storage devices also include the storage devices on the host computer.

The documentation must also contain a description of the protection measures against inadmissible reloading and execution of software and a description of the technical means for permanently deactivating the administration of the live system.

6 Protective interfaces

The requirements of the chapter from the leaflet "Configuration of general-purpose operating systems for measuring instruments" [1] apply without restriction.

7 Testability and traceability

For the live system, the following requirements apply in addition:

1. On the live medium, integrity protection must be in place for the indication program and for the legally relevant parts of the operating system.
2. The user must be able to verify the integrity of the ISO image before running the live system.
3. In the event of a loss of integrity, the live system shall not perform any legally relevant functions.

Remark: Legally relevant parts of the operating system are at least the kernel, the bootloader, the interfaces, the services, the user account control, cryptographic libraries, and the legally relevant configuration files for the operating system.

The documentation must also contain a description of the protection measures to maintain the integrity of the live medium and the live system.

8 References

[1] Leaflet: Configuration of general-purpose operating systems for measuring instruments, Physikalisch-Technische Bundesanstalt, Working group 8.51 “Metrological Software“, in the current version

[2] WELMEC 7.2, 2015: Software Guide (Measuring Instruments Directive 2014/32/EU), WELMEC, 2015

[3] Leaflet: Special requirements for cryptographic modules, Physikalisch-Technische Bundesanstalt, Working group 8.51 “Metrological Software“, in the current version

[4] S. Bradner, RFC 2119 - Key words for use in RFCs to Indicate Requirements Levels, March 1997, URL: https://tools.ietf.org/html/rfc2119 (last accessed on March 4, 2021)