Working group 8.51 „Metrological Software“ Last revision: November 05, 2018

Leaflet:
Special requirements for cryptographic modules

Supplement to metrological and security requirements for conformity assessments according to Module B.

In this text, cryptographic modules are understood as all components, assemblies and software modules with cryptographic functions that are part of measuring instruments.

For conformity assessments according to Module B, metrological or functional requirements of the respective instrument type, as well as security and software requirements of WELMEC Software Guide 7.2 [1] apply to cryptographic modules (as to all other measuring instrument’s components).

In addition, there are metrological and security requirements resulting from the specific task of the cryptographic module in the measuring instrument.

This present list of requirements covers these specific metrological and security requirements**,** derived from the Measures and Verification Act [2].

It is assumed that, depending on the area of application, a medium or high level of protection shall be guaranteed. This corresponds to the risk classes B-C (medium) and D-F (high) respectively in the WELMEC Software Guide 7.2 [1].

Requirements

K1 Documentation

Protection level medium	Protection level high
Requirement K1: **The cryptographic module shall be documented.** Details: 1. The documentation shall name the type and the manufacturer of the cryptographic module. 2. The documentation shall describe the attributes of the cryptographic module that are essential for its use.	

Explanations:

1. This requirement is checked according to the WELMEC Requirement P1/U1 if necessary.
2. Essential attributes include: the functions, the implemented algorithms with key lengths and other parameters, the implemented cryptographic standards and rules, the components (cards, libraries, operating system, ...), as well as access rules.
3. Of all the attributes of the cryptographic module, only those that are used in the measuring instrument or that can be accessed from outside the measuring instrument need to be described.

K2 Identification

Protection level medium	Protection level high
Requirement K2: **The software of the cryptographic module shall be identifiable.** Details: 1. The software of the cryptographic module shall have an identification that can be easily checked if necessary. 2. The identification shall not be changeable. 3. The identification shall be unambiguous.	
Explanations: 1. This requirement is checked according to the WELMEC Requirement P2/U2 if necessary. 2. The identification of the software of the cryptography module is used to determine the conformity of the serial instrument with the type. The identification of the software of the cryptographic module is part of the identification of the measuring instrument of which it is part. 3. The kind of identification is not prescribed.	
-	4. The identification shall be suitable for checking the applicability of the submitted security certificates.

K3 Functional requirements

In the framework of conformity assessments according to Module B, the functions for the protection of the measurement data and (optionally) the functions for the evaluation of software downloads are considered.

K31 Presence of all required functions

<table>
<tr><th>Protection level medium</th><th>Protection level high</th></tr>
<tr><td colspan="2">Requirement K311:
For the protection of the measurement data, the cryptographic module shall have a key generation or a key loading function.

Details:</td></tr>
<tr><td>1. The measuring instruments have individual or identical keys / key pairs.
2. For signing, symmetric and asymmetric encryption methods are allowed.
3. If necessary, a new key / a new key pair can be generated in the cryptographic module or loaded into the cryptographic module. The documentation contains the corresponding instructions.</td><td>1. The measuring instruments have individual key pairs.
2. For signing, only asymmetric encryption methods are allowed.
3. During putting into market and when needed, a new key pair can be generated in the cryptographic module. The documentation contains the corresponding instructions.</td></tr>
<tr><td colspan="2">4. The renewal of the key / key pair is only possible after externally visible violation of a protective measure (seal).
5. If the cryptographic module does not have the function for security reasons, this shall be documented.
6. In case of asymmetric encryption, the public key can be presented if needed. The documentation contains the corresponding instructions. If no presentation is possible, this shall be documented.</td></tr>
<tr><td>-</td><td>7. A valid security certificate for the cryptographic module proves that the key generation feature is present and certified.</td></tr>
<tr><td colspan="2">Explanations:

1. Renewal of the key / key pair may be necessary if the measuring instrument has been compromised.
2. The presentation of the public key can be achieved by display, printouts, the export of key certificates or the export of signed data that contain the key.</td></tr>
<tr><td>3. In cases where the signatures are also to be used for the proof of origin of the signed data, individual keys / key pairs shall be used.</td><td>3. A test, as to whether the documented instructions actually trigger a key generation, is part of Requirement K34.</td></tr>
</table>

Protection level medium	Protection level high
Requirement K312: **For the protection of the measurement data, the cryptographic module shall have the signature creation function and, if necessary, the signature verification function.** Details: 1. The cryptographic module creates a security feature that is attached to measurement data and that can be tested in the measuring instrument or by external software. 2. The documentation states that the security feature is a signature. 3. The presentation of measurement data with valid signature differs clearly from the presentation of measurement data with invalid signature. The documentation describes the differences.	
-	4. A valid security certificate for the cryptographic module proves that the signature generation function and, if necessary, the signature verification function are present and certified.
Explanations: 1. The signature verification function is only required if the measuring instrument needs to be able to verify the signatures itself. Often the verification of the signatures is not done by the measuring instrument, but by an external program. 2. For measurement data with an invalid signature, an error message is the preferred output, instead of the measurement data.	
-	***3.*** A test, as to whether the documented functions actually generate or verify a signature, is part of Requirement K34.

Protection level medium	Protection level high
Requirement K313: **If the cryptographic module is used to evaluate software downloads, it shall have the signature verification function.** Details: 1. The cryptographic module verifies the security feature that is attached to the downloaded software. 2. The documentation states that the security feature is a signature.	
-	3. A valid security certificate for the cryptographic module proves that the signature verification function is present and certified.

Explanations: 1. The requirements for the download are described in requirements set D (Download) of Welmec Guide 7.2 [1].	
-	2. A test, as to whether the documented functions actually verify a signature, is part of Requirement K34.

K32 Cryptographic strength of the functions

Protection level medium	Protection level high
Requirement K32: **The used cryptographic functions of the cryptographic module shall be cryptographically strong.** Details:	
1. The algorithms, key lengths and other parameters used shall conform to the requirements of the Rule Determination Committee according to §46 of the Measures and Verification Act [2] or be generally recognized as secure.	1. The algorithms, key lengths and other parameters specified in the security certificate shall comply with the current specifications of the institutes responsible for data security.
Explanations: 1. For unknown or newly developed algorithms or unusual key lengths or parameters, an evaluation of the vulnerabilities by the specialist public is lacking.	
	2. Current specifications of the institutes responsible für data security (BSI, BNetzA, NIST, ..) are e.g. the Technical Guideline of BSI TR-02102 [3] or the BNetzA Announcement concerning electronic signatures [4].

K33 Correct implementation of the cryptographic functions

<table>
<tr><td>Protection level medium</td><td>Protection level high</td></tr>
<tr><td colspan="2">Requirement K33:
The used cryptographic functions shall be correctly implemented.

Details:</td></tr>
<tr><td>1. The correct implementation is proven by tests done by the manufacturer of the measuring instrument.
2. The documentation contains a description of the performed tests, the arbitrary-precision (bignum) library, the random number generator and, if necessary, the primality tests.</td><td>1. A valid security certificate for the cryptographic module proves the correct implementation.</td></tr>
<tr><td colspan="2">Explanations:</td></tr>
<tr><td>1. The documentation shall include at least the following tests:
• Tests that prove that calling the key generation function multiple times will produce new, different keys / public keys each time,
• positive and negative tests that show that signature creation and signature verification match each other,
• individual tests of hash value calculation, encryption and decryption, as well as comparison of outcomes with publicly available expected results.
2. The test descriptions include: Test objective, tested software / hardware, inputs, expected outputs, actual outputs, date.
3. The documentation shall include at least the following descriptions:
• a description of the used arbitrary-precision (bignum) library, in particular its quality or its proven-in-use,
• a description of the used random number generator, in particular its statistical quality,
• For asymmetric procedures, a description of the used primality tests.</td><td>1. For certificates according to the Common Criteria [5] (CC certificates), assurance level EAL 4 or higher can be valid proof.
2. For certificates according to the Information Technology Security Evaluation Criteria [6] (ITSEC certificates), evaluation level E3 (high) or higher can be valid proof.</td></tr>
</table>

K34 Correct implementation of the interfaces to the cryptographic functions

Protection level medium	Protection level high
Requirement K34: **The interfaces between the cryptographic module and the measuring instrument's calling program shall be correctly implemented.** Details:	
1. The correct implementation is proven by tests done by the manufacturer of the measuring instrument. 2. The documentation contains a description of the performed tests.	1. The documentation contains the description of the programming interface of the cryptographic module as well as the calling code.
Explanations:	
1. The performed tests for requirement K33 can be designed to include the interfaces. If this is not the case, the software included in the tests needs to be extended and the tests need to be repeated.	1. The interfaces are subjected to code inspection. The calls to the cryptographic functions shall correspond to the programming interface description of the cryptographic module with respect to the parameter list, return values, pre-/post-processing and error evaluation.

K4 Security requirements

K41 Protection of the cryptographic module against defects and manipulation

Protection level medium	Protection level high
Requirement K41: **The cryptographic module shall be protected against defects and manipulation.** Details:	
1. The cryptographic module shall have protective measures that protect functions, parameters, and measurement data from defects and manipulation or make them evident. The documentation shall describe these protective measures.	1. A valid security certificate for the cryptographic module proves protection against defects and manipulation.
Explanations:	
1. The protection shall cover the code and the relevant parameters (keys, hash-method parameters, encryption and decryption parameters, credentials, ...).	1. The protection shall cover the code, the relevant parameters (keys, hash method parameters, encryption and decryption parameters, credentials, ...) and, if

2. This requirement is checked according to the WELMEC Requirements P3-P7/U3-U7, L, and T if necessary.	necessary, the relevant temporary data (data to be hashed, hash values, calculated signatures). 2. For CC certificates, proof is provided by the security objectives of the associated security target (integrity protection for the above-mentioned information). 3. In the case of ITSEC certificates, proof is provided by the certified minimum strength of the algorithms "high" (E3 high).

K42 Confidentiality of the key and other information

Protection level medium	Protection level high
Requirement K42: **The confidentiality of the key or private key and comparable parameters shall be ensured.** Details:	
1. The cryptographic module shall have protective measures that ensure the confidentiality of key or private key and similar parameters. The documentation shall describe these protective measures. 2. For cases of symmetric keys, the confidentiality of the key shall be ensured at storage location and at its location of use, outside of the cryptographic module, too.	1. A valid security certificate for the cryptographic module proves the confidentiality of private key and similar parameters.
Explanations: 1. The protection shall cover the key or the private key for the protection of measurement data, and, if applicable, access data or credentials.	
2. The protection of the key outside of the cryptographic module shall be secured by additional technical or organizational protective measures if needed.	2. For CC certificates, proof is provided by the security objectives of the associated security target (confidentiality for the above-mentioned information).

References

[1] WELMEC Software Guide 7.2 (Measuring Instruments Directive 2014/32/EU), WELMEC, 2015
[2] Mess- und Eichgesetz (MessEG; Measures and Verification Act). Bundesgesetzblatt 2016. Part I, No 43.
[3] BSI TR-02102 Cryptographic Mechanisms, 2018
[4] BNetzA, Bekanntmachung zur elektronischen Signatur (Übersicht über geeignete Algorithmen), (Announcement concerning electronic signatures (Overview of applicable algorithms)), 7. Dezember 2016
[5] ISO/IEC 15408:2008 Information technology – Security techniques – Evaluation criteria for IT security, International Organization for Standardization, Geneva, CH, Standard, August 2008
[6] Information Technology Security Evaluation Criteria, 1991