https://doi.org/10.17576/apjitm-2018-0702(02)-09

http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 7 No. 2-2, December 2018: 99 – 109
e-ISSN: 2289-2192

LEGALIZING SOFTWARE FOR MEASURING INSTRUMENTS: A PROPOSED PLAN FOR MALAYSIAN CASE STUDY

MUHAMMAD AZWAN IBRAHIM
ZARINA SHUKUR
NASHARUDDIN ZAINAL
NAZRI MARZUKI
OSMAN ZAKARIA
MARYATI MOHD YUSOF

ABSTRACT

Software has become one of the most critical parts of a measuring instrument. Despite the sophistication and complexity of measuring instruments, legal metrology framework on software remains poor. Several legal cases related to the manipulation and modification of software used in measuring instruments have been discovered in ASEAN countries, particularly in Malaysia. A survey has been conducted and findings show that most ASEAN countries have yet to implement and enforce legal metrology control on the software in their metrological system. This paper discusses an approach to legalizing software for measuring instruments in the Malaysian context.

Keywords: pattern approval, type approval, software examination, software testing, software verification, legal metrology.

INTRODUCTION

Most consumers are unaware of legal metrology control in measuring instruments applied in their daily activities, such as buying groceries, refueling car, or paying for utility bills. Legal metrology control is meant for ensuring that trade and business transaction are fairly conducted and profitable. This control not only covers end-user transaction but also involves various levels of business transactions, such as planting, harvesting, and manufacturing. Therefore, measuring and weighing instruments should undergo a process known as "pattern approval" or "type approval."

The International Vocabulary of Terms in Legal Metrology defines pattern approval as "decision of legal relevance, based on the review of the type evaluation report, that the type of a measuring instrument complies with the relevant statutory requirements and results in the issuance of the type approval certificate (OIML, 2013)."

Laws compliant with national certification bodies such as the National Metrology Institute, notified bodies, and/or pattern approver agencies are responsible for evaluating and issuing the pattern approval certificate (Said, Shukur, & Ibrahim, 2017). Instrument evaluation process for pattern approval, namely, pattern approval evaluation, is defined in the same document as "conformity assessment procedure on one or more specimens of an identified type (pattern) of measuring instruments which results in an evaluation report and/or an evaluation certificate (OIML, 2013)."

Pattern approval evaluation comprises the following:

1. Evaluation and assessment of the documents (test certificate and results) of the measuring instrument;

2. Assessment of the measuring instrument against legal standard requirements, such as those from the International Organization of Legal Metrology (OIML);
3. Test and evaluation of the measuring instrument against maximum permissible error (MPE) as stated in the legal standards.

An instrument that uses a software to control its operation is called a software-based device, which is defined as a "device used to compute and processes using software" (NIST, 2014). An advanced and precise measuring instrument, such as an electronic weighing scale in a market or small shop, relies on its software for measuring purposes (Ma, Lu, Mao & Shen, 2012). Therefore, software has become a critical element that must be evaluated in pattern approval process to ensure the reliability of instruments.

Studies show that traders tend to manipulate and cheat on measuring and weighing instruments. Mechanical methods were previously used to manipulate the readings of measuring and weighing instruments to gain additional profit. However, software has become the most vulnerable element to be manipulated in measuring instruments (Al-Wosabi, Shukur, Ibrahim, 2015). Numerous cases have been reported in Malaysia (Ibrahim, Shukur, Zainal & Al Wosabi, 2015).

Evaluation, verification, and assessment of software during pattern approval are critical for ensuring a credible and smooth operation related to weighing and measuring instruments and systems. The penalty for using fraudulent measuring instruments is stated in the Weight and Measures Act 1972 Section 17 (International Law Book Services, 2009) is as follows:

> Whoever is in possession of any weight or measure or instrument for weighing or measuring which he knows to be false and intending that the same may be fraudulently used or having fraudulently used such weight or measure or instrument for weighing or measuring shall be guilty of an offence and shall, on conviction, be liable to a fine not exceeding five thousand ringgit or to imprisonment for a term not exceeding four years or to both. Any weight or measure or instrument for weighing or measuring used or in any person's possession for use in contravention of this section shall be liable to be forfeited.

METHOD

The National Metrology Institute of Germany, namely, Physikalisch-Technische Bundesanstalt (PTB), in cooperation with the Metrology Enabling Developing Economies (MEDEA), has taken an initiative to conduct a 5-day training on "Software Testing for Measuring Instruments" in December 2017, which was jointly participated by all ASEAN countries, except for Singapore. During the training, participants were required to answer a questionnaire related to the legal status of software for measuring instruments in their respective country. Numerous countries, including Malaysia, Myanmar, the Philippines, and Indonesia, have generally implemented and enforced pattern approval but not on software (MEDEA, 2017). Software pattern approval was not implemented mainly due to the lack of knowledge and experience in software testing/verification, the absence of established procedure, and insufficient facility.

Three types of verification are generally required on the software: documentation, functional, and source code checking (Jacobson & Johansson, 2004). Documentation check is the basis of software examination; thus, our training was focused on software verification against the WELMEC 7.2 Software Guide document requirements (WELMEC, 2015). This document is actively being used by the European Union to support the Measurement Instrument Directive, which attempts to remove uncertainty over the interpretation of software requirement (Richter, Grottker, Talebi, & Schwartz, 2006).

LEGALIZING SOFTWARE IN MALAYSIA

Malaysia defined two acts related to weights, measures, and trades (Rahman, 2017): National Measurement System Act 2007 (Act 675) and Weights and Measures Act 1972 (Act 71). Act 675 described the establishment of the National Measurement Standards and the roles and responsibility of the National Measurement Standards Laboratory (NMSL) in realizing the metrology standard infrastructure, including reference material. Meanwhile, Act 71 is a regulation for trading purposes.

The key objective of Act 71 is to regulate the activities and instruments used in weighing and measuring for trades but is not limited to the following purposes:

1. To ensure the conformity of weights, measures, or weighing or measuring instruments to the patterns and specifications specified by the Custodian of Weights and Measures;
2. To ensure the verification of weights, measures, or the weighing or measuring instruments used for trade;
3. To regulate the licenses issued to manufacturers, repairers, and sellers of weighing or measuring instruments;
4. To regulate the licensed company that provides services in relation to the verification of any weight, measure, or weighing or measuring instrument.

Act 71 of the Malaysian National Legislation clearly states that every instrument used for trades must pass the pattern approval by the Custodian of Weight and Measures. Not using the measuring instruments in accordance with the pattern approval is an offence for traders. This practice is meant for ensuring that all measuring instruments used in trades are suitable and meet the standards and criteria set by the government, as well as for protecting consumers in their business transactions.

The National Metrology Institute of Malaysia (NMIM), previously known as National Metrology Laboratory (SIRIM Berhad), is a regulatory body appointed to be the Custodian of Weights and Measures of the NMSL under Act 675 as stated in the law of Malaysia and via notification in a Gazette (Adam, 2016) (International Law Book Services. 2011). The NMIM has been appointed as the NMSL by the government of Malaysia through the Ministry of Energy Science, Technology, Environment and Climate Change, previously known as the Ministry of Science, Technology, and Innovations. Therefore, the NMIM plays the role of NMSL as the custodian of Act 71 as stated in the law, including pattern approval activities.

ISSUANCE OF APPROVAL CERTIFICATE

Pattern approval certificate will be issued by the NMSL after an instrument has satisfactorily passed all the requirements, testing, and assessment. The approval certificate often comprises three sections:

1. Description of the measuring instrument, conditions, and advice/recommendation of the approval;
2. Technical specification (which may include illustrations) describing the pattern approval;
3. Evaluation report describing the conducted test of the instruments and applicable MPE.

The approval certificate will follow the legislation requirements and includes the following:

1. Name and address of the NMSL;
2. Pattern identification number;
3. Pattern description;
4. Statement of approval stating that the pattern of the measuring instrument is suitable for use in trade or as a legal measuring instrument;

5. Condition of approval;
6. Date of issued certificate
7. A statement that the certificate is suitable for use in trade with respect to its metrological characteristic and the validity period of 10 years.

SUPPORTING DOCUMENTS

The supporting documents shall be submitted during pattern application. The documents shall comprise the following:

1. Detailed drawings, diagrams, and operating and service manual;
2. A declaration of safety relevant to the Malaysian Safety Standard and, where appropriate, compliance with the relevant test scheme;
3. Sufficient photographs, screenshots, and descriptions for a complete understanding of the construction method of operation;
4. A completed test report (where available) and documentation files.

REVIEW OF APPROVAL CERTIFICATE

The validity of pattern approval as stated in the pattern approval certificate is 10 years on condition that non-modification has been made to the patterned instruments. The period has been stated in Rule 11 of the Regulations Weight and Measures (Duties and Powers of the Custodian), 1981. The instruments are subject to re-examination and re-evaluation after the expiry of the pattern validity.

The NMIM has the capability to conduct pattern approval for weighing and measuring instruments as stated under Act 71. However, the NMIM is developing the capability to conduct pattern approval for software, which is crucial in the current situation. This study focused on the software used in weighbridge as a case study. Weighbridge is a machine for weighing vehicles by using a metal plate set into a widely used road in the palm oil industry and trading in Malaysia.

FINDINGS

Three Malaysian agencies are responsible for regulating the legal domestic trade framework as depicted in Table 1.

TABLE I. Regulatory body associated with domestic weight and measure in Malaysia

Body/Agency	Role/Function
Ministry of Domestic Trade and Consumer Affairs (KPDNHEP)	Government authority for domestic trades. Implements the regulation on metric weights and measures.
National Metrology Institute of Malaysia (NMIM)	Provide national traceability for measurement and pattern approval service.
Metrology Corporation Malaysia (MCM)	Conduct regular inspection, verification, and post-market surveillance under appointment of the Minister (KPDNHEP).

Weighbridge has been widely used throughout the country without proper legal control on the measuring software. The roles, function, and work nature of the three agencies must be analyzed for proper plan execution. The table shows that each of the agencies has their own roles and responsibility in the legal enforcement framework under Act 71.

The strategic planning in realizing the pattern approval certification plan has been prepared by using strength, weaknesses, opportunities, and threat (SWOT) method/analysis. The SWOT analysis was developed from the early perspective of the NMIM. Various parameters, such as resources, cooperation, work nature, and networking, have been identified and listed accordingly. Table 2 tabulates the details in the SWOT analysis.

TABLE 2. SWOT Analysis

Strengths	Weaknesses
• Expert staffs in metrological field. • Experienced in verification and pattern approval of measuring instruments. • Experienced in the enforcement operation with KPDNHEP related to software manipulation for weighbridge in the field. • Established relationship with CyberSecurity Malaysia. • Established relationship with Universiti Kebangsaan Malaysia (UKM). • Good relationship with PTB, Germany as an expert in software verification of legal instruments. • Good networking and relationship with ASEAN countries in the field of Legal Metrology • Good relationship with Mettler Toledo Malaysia (measuring instrument manufacturer). • Good relationship with KPDNHEP, which is the owner of Act 71.	• Lack of experience and specific expertise in the field of software inspection, analysis, and verification for legal instruments. • No established procedures and guidelines. • Inadequate skills and knowledge of enforcement officer and legal inspectors in software inspection and verification. • Unspecific department or unit to enforce.
Opportunities	**Threats**
• Certification procedure similar to JAKIM's Halal Certification and MQA academic qualification. • Expertise development through training in software testing, secure software development, and digital forensic.	• The industrial readiness in terms of knowledge and human capital and economies to comply with the new regulations. • No exact information regarding the number of software for weighbridge use in the market. • Possibility of various types of requirements for software for weighbridge due to a variety of weighbridges and software types.

The plan and strategy has been developed using threat, opportunity, weakness, and strength (TOWS) analysis to identify the strategic options of external–internal analysis to form an actionable approach. Table 3 tabulates the details on the TOWS analysis.

TABLE 3. TOWS Analysis

	Opportunities (external, positive)	Threats (external, negative)
Strength (internal, positive)	• To identify UKM cooperation opportunities with MSTB and software experts. • To adapt Halal procedure from JAKIM and MQA accreditation in developing the legal software metrology certification. • To prepare the training in software verification, software testing, and digital forensic with PTB, CyberSecurity Malaysia, and UKM. • UKM provides post-graduate research project to solve challenges in legal software verification needs in the future. • To utilize relevant OIML and WELMEC documents and checklist.	• To obtain early information regarding industrial readiness in the aspects of knowledge and finance from the relevant non-government organization related to trades. • The number of premises could be identified based on the enforcement of hardware inspection and experience. • Different requirements of weighing instruments shall be referred to OIML-D31 and WELMEC 7.2.

Weakness (internal, negative)	• To appoint third-party verification body and expert from the industry and high learning institution. • Metrologist to attend training on software testing conducted by PTB/UKM/MSTB. • To utilize references from OIML, WELMEC, Halal, and MQA certification checklist. • Enforcement officers to attend digital forensic training conducted by UKM/CyberSecurity Malaysia.	• To increase the knowledge of metrologist for various requirements of software and instruments.

PROPOSED PLAN

We compared the plans designed on the basis of SWOT and TOWS analyses with two previous successful certification implementations in Malaysia, namely, Halal and MQA (Khan & Abid, 2016) (International Law Book Services, 2007). As Malaysia is a corresponding member of OIML, the requirements for software verification will be mainly based on OIML-D31: General requirements for software-controlled measuring instruments (OIML, 2008). The OIML D documents are informative documents intended to harmonize and improve work in the field of legal metrology across members (OIML, 2012). New software is subjected to new regulations and shall obtain pattern approval certification to be allowed for utilization in the market. The designed enforcement plan is inapplicable to new software, whereas the plan for existing software comprises three phases: registration, certification, and enforcement phase (Figure 1).

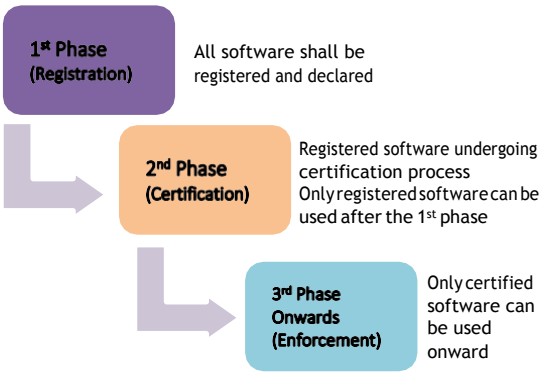


FIGURE 1. Existing software enforcement plan.

REGISTRATION PHASE

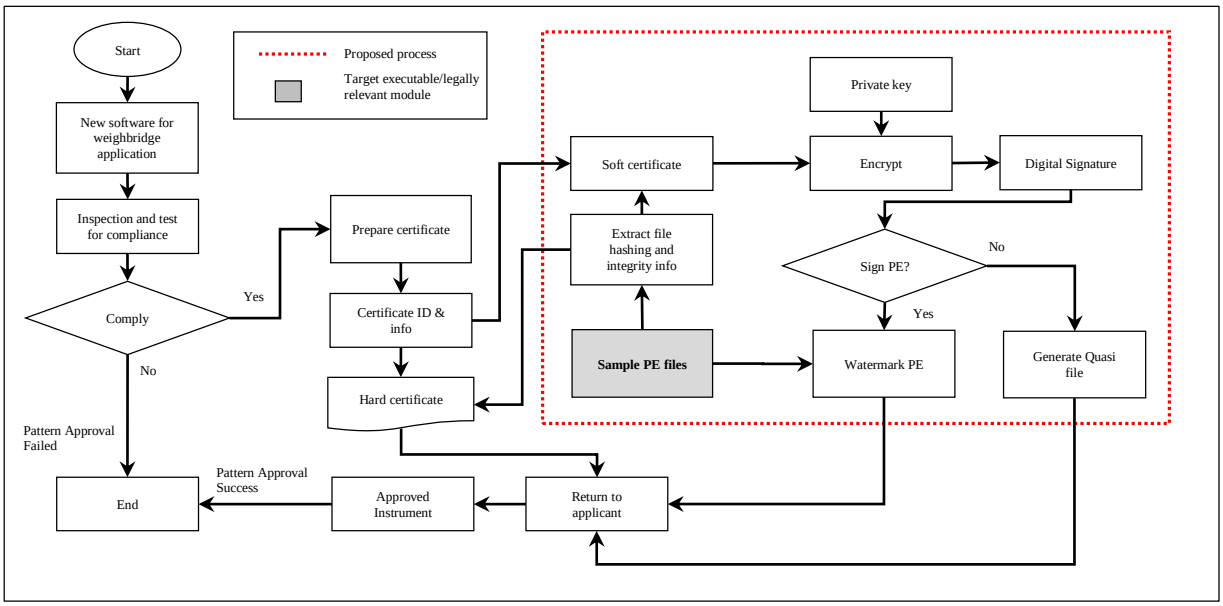
Registration is the first phase in the enforcement plan, where all software for weighbridges shall be declared and registered into the pattern approval provider database. This step is crucial to gain early information regarding the status, variants, and types of software used in the market. The updated information from the related ministry and department will be used to identify weighbridge owners throughout the country. Only registration and declaration are required in this phase. The weighbridge owner will be granted sufficient time to register the software with the pattern approval provider. After successful registration, the applicant will be issued a temporary certificate with limited validity time to allow software usage before proceeding with the pattern approval process.

PATTERN APPROVAL PHASE

After the first phase is completed, the pattern approval phase requires obtaining a registered software pattern approval within the allowable time frame. Starting from this phase onward, every unregistered and unidentified software will no longer be allowed to be used for trades

and will be regarded as an "illegal software." Figure 2 shows the software preparation for weighbridge in the pattern approval phase for illegal software detection.

FIGURE 2. Preparation of illegal software detection during pattern approval



ENFORCEMENT PHASE

The final phase is enforcement, where full action will be executed and illegal software will be identified through regular inspection. Any unidentified and tampered/modified software will be subjected to penalty as stated by the law. In this phase, legal inspectors/enforcers will be provided with special tools to assist them in the identification of illegal software.

SOFTWARE CERTIFICATION REQUIREMENTS AND PHASES

The submitted applications shall be attached to all related documents, diagrams, and complete specifications and instructions. The pattern approval certification has four phases.

DOCUMENT CHECKING PHASE

Document availability attached to the instruments that must be approved will be examined on the basis of the following conditions:

1. Information and all software security are available;
2. Information in the documents will be thoroughly and adequately checked;
3. The document will be examined by either an internal or external examiner;
4. Interview method with the applicant can be performed during document inspection.

If any of the requirements are not fulfilled, then the documents will be returned back to the applicant.

VERIFICATION AND SOFTWARE CERTIFICATION PHASE

The risk level and scope will be determined by NMSL. Verification has three types:

1. Document verification
2. Dynamic black-box testing
3. Source code examination

INFORMATION RECORDING PHASE

Additional information (apart from the documents attached during application) will be recorded when the scope has been approved for certification, as follows:

1. SHA values or checksum
2. Watermarking information

CERTIFICATE REWARDING PHASE

Successful application with the approved pattern will be awarded with a printed certificate, and the status of the pattern will be published on the pattern approval provider website.

DETECTION OF ILLEGAL SOFTWARE

Upon pattern approval, illegal software will be detected in the market. This detection can be conducted via regular inspection performed by a third-party agency appointed by the government (as in the current situation). The three aforementioned regulatory bodies associated with the domestic trades in Malaysia carry their own roles in implementing the national regulatory framework. All mentioned regulated bodies independently work; therefore, a new approach must be adopted to realize the new software regulations and illegal software detections further efficiently. Additional steps will be proposed into the legal framework for implementation in the following stages.

PATTERN APPROVAL STAGE

At the pattern approval stage, the pattern approval provider will generate two types of certificates: hard and soft certificate. Figure 3 shows the details on the preparation of illegal software detection. Hard certificate is a printed document produced by the pattern approval certification body; this certificate contains all the necessary pattern information with a unique certification ID. This certificate will also be kept by the applicant for future use, especially during regular inspection by legal inspectors/enforcers. A soft certificate is an encrypted data containing related information from the hard certificate, such as certification ID, and additional hashing and integrity information from the relevant portable executable (PE) files and the supporting legally relevant modules (where applicable). Depending on the situation, the soft license will either be injected as a digital signature into the main executable file using watermark technique or will be generated as a standalone encrypted file (quasi) and placed on the installation folder of the main executable file.

REGULAR INSPECTION STAGE

At the regular inspection stage, the inspector/enforcer will reveal the digital signature using special tools provided and compare this signature with the hard copy of the actual certificate of the approved pattern. If the identification from the soft certificate extraction information did not match the printed information on the hard certificate, then the inspection will be considered a failure. Furthermore, the inspector/enforcer shall log a special report on the findings for further investigation.

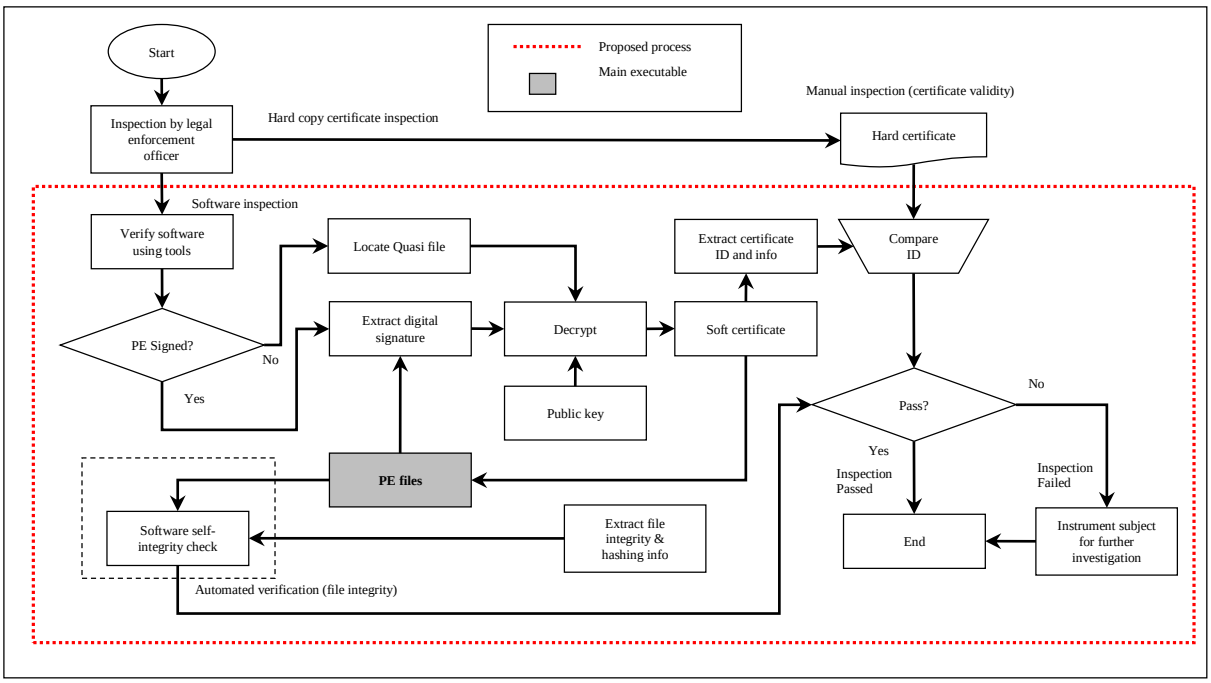
SOFTWARE INSPECTION AND FINDINGS

Two components must be checked and verified during regular inspection: certificate validity and software integrity.

CERTIFICATE VALIDITY

Mechanisms have been developed to validate the hard certificate against its software. The hard certificate will be equipped with security features for the document to be secured and fool-proofed, whereas a clear certificate–software pairing scheme will be established for the soft certificate through watermarking and public cryptography technique.

FIGURE 3. Illegal software detection during regular inspection.



SOFTWARE INTEGRITY

After the software–certificate pairing has been validated, the integrity of the software is ensured. This aspect is a key requirement in software pattern approval as stated by WELMEC (2015) and OIML (2008) to protect several areas of the software from tampering or modification (i.e., using the same piece of code/binary sent for approval without compromising tampering or modification), especially those with sensitive legally relevant parts. The importance of the two requirements in the aforementioned inspection can be attributed to the following illegal software cases, which might be expected in the enforcement phase:

1. Unapproved software: Software that is not approved in pattern and did not undergo/pass the pattern approval process;
2. Fake hard certificate: Manipulation of hard certificate to match with soft certificate that may confuse the legal inspector/enforcer;
3. Fake soft certificate: Unapproved software where the hacker may attempt to inject a fake soft certificate into the software to match the genuine hard certificate;
4. Compromised integrity: Approved software wherein the integrity of the files and/or relevant legally modules are invalid.

Our initial prototype of software tampering detection via the digital signature of Portable Executable (PE) shows positive results. Soft certificates have been injected into various PE files, including executables and libraries, and tampering incidents have been successfully detected. A number of interviews and meetings with the KPDNHEP officials and experts acknowledged the effectiveness of the proposed technique in assisting the legal officers to perform enforcement.

FUTURE WORK

Further study will address tools and watermark that are suitable with the working environment of interest. Numerous aspects will be considered in designing the software detection scheme concerning the targeted legal framework. One of the focuses will be on strengthening the soft certificate via public key cryptographic technique. Field simulation and evaluation on the usability of the proposed technique will be implemented in terms of human, organization, and technology.

CONCLUSION

This paper discussed the software for measuring instrument, especially in ASEAN countries, the situation in Malaysia, and an overview of the legal framework in Malaysia. This study proposed an action plan in legalizing the software used for weighbridge, especially in the Malaysian working context, to detect illegal software effectively.

ACKNOWLEDGMENT

This project is a collaboration between the NMIM and UKM. We would like to thank the KPDNHEP as the main stakeholder of the research and the MCM for their interest and support toward the success of this research. Finally, special gratitude to the PTB for their knowledge sharing, technical support, and advice.

REFERENCES

Al-Wosabi, A. A., Shukur, Z. & Ibrahim, M. A. 2015. Framework for software tampering detection in embedded system. International Conference on Electrical Engineering and Informatics (ICEEI). Denpasar, 259–264.

Adam, A. 2016. APLMF Economy Report: Malaysia. 23rd APLMF Meeting Tokyo, Japan, 1-11.

Ibrahim, M. A Shukur. Z., N. Zainal, & Al Wosabi. A. A. 2015. Software Manipulative Techniques of Protection and Detection: A Review. ARPN Journal of Engineering and Applied Sciences, 10(23): 17953– 17961.

International Law Book Services. 2007. Act 673: Malaysian Qualifications Agency Act 2007. The Commissioner of Law Revision. Malaysia.

International Law Book Services. 2009. Weights and Measures Act 1972 (Act 71). Kuala Lumpur.

International Law Book Services. 2017. Act 675: National Measurement System Act 2007. The Commissioner of Law Revision. Malaysia.

Jacobson, J. & Johansson, B. 2004. Methods for Validation and Testing of Software. MID Software. https://pdfs.semanticscholar.org/b2a9/06f851d0eef939f10ae3a83b9e52e4450185.pdf.
[1 December 2018].

Khan, M. I. & Abid, H. 2016. Understanding 'Halal' and 'Halal Certification & Accreditation System' - A Brief Review. Saudi Journal of Business and Management Studies, 1(1): 32–42.

Ma, B., Lu, P., Mao, X. & Shen, Y. 2012. Software Check of Measuring Instrument According to Welmec and Oiml Files. Zhejiang Province Institute of Metrology. Hangzhou, 3–5.

MEDEA. 2017. Software Testing for Measuring Instruments. Nilai: PTB.

NIST. 2014. NTEP Software Sector Meeting Summary. https://www.nist.gov/document/ncwm-2014-annual-report-sp-1193-ntep-appendix-e [1 December 2018].

Organisation Internationale de Métrologie Légale (OIML) (International Organization of Legal Metrology). 2008. OIML D31: General requirements for software controlled measuring instruments., 2008(31): 1-53.

Organisation Internationale de Métrologie Légale (OIML) (International Organization of Legal Metrology). OIML. 2012. OIML D1: Considerations for a Law on Metrology, 2012(1): 1-54.

Organisation Internationale de Métrologie Légale (OIML) (International Organization of Legal

Metrology). 2013. International Vocabulary of Terms in Legal Metrology. http://viml.oiml.info/en/index.html [1 December 2018].
Rahman, A. 2017. APLMF Economy Report: Malaysia. 24th APLMF Meeting. Siem Reap, Cambodia, 1-14.
Richter, D. Grottker, U., Talebi, D. and Schwartz, R. 2006. The new European software guide for legal metrology: Basic principles. Computer Standards & Interfaces, 28(3): 270–276.
Said, I. O. Shukur, Z. & Ibrahim, M. A. B. 2017. Certification criteria for software of measuring instruments based on Malaysian environment. 6th International Conference on Electrical Engineering and Informatics (ICEEI). Langkawi, 1–5.
WELMEC. 2015. WELMEC 7.2 Software Guide. WELMEC Secretariat, 7(2): 1–114.

Muhammad Azwan Ibrahim
Nazri Marzuki
Osman Zakaria
National Metrology Institute of Malaysia
Sepang, Malaysia.

Zarina Shukur, Nasharuddin Zainal, Maryati Mohd. Yusof
Universiti Kebangsaan Malaysia
Bangi, Malaysia.

Received: 31 July 2018
Accepted: 1 September 2018
Published: 31 January 2019