METROLOGIA
2023

Proposal for the use of checksum as an electronic sealing resource in legal metrology

Edísio Alves de Aguiar Júnior [1] and Davi Barbosa Rezende [2]

[1]Inmetro. Instituto Nacional de Metrologia, Qualidade e Tecnologia. Diretoria de Metrologia Legal (Dimel), Setor de Medição de Fluidos (Seflu). Av. Nossa Senhora das Graças, 50. Xerém, Duque de Caxias, Rio de Janeiro. CEP: 25250-020
[2]Strack Consultoria & Engenharia. Diretoria de Serviços e Produtos, Setor de Medição Fiscal. Rua Pandiá Calógeras, 88. Cambuí, Campinas/SP. CEP: 13024-170.

eajunior@inmetro.gov.br, engenharia@strack.com.br

Abstract. Sealing is a key aspect in the scope of legal metrology, strongly associated with verification activities. With the increasing number of instruments whose operation is based on software, conventional techniques, generally based on physical and mechanical seals, can be improved with the use of software techniques. The study presents a proposal based on the use of checksum as an electronic sealing tool. Suggestions are presented for inserting the checksum in type approval procedures and the conditions for its use as a sealing tool, in support of verification activities.

1. Introduction

According to the International Vocabulary of Legal Metrology Terms, published by Inmetro through Inmetro Ordinance No. 163 of September 6, 2005, legal metrology is the part of metrology related to activities resulting from mandatory requirements, referring to measurements, measurement units, measuring instruments and measurement methods, and which are developed by competent bodies [1]. It can also be understood as the area of metrology that is related to laws and regulations, that is, organized through a legal structure.

Among the requirements involving legal metrology activities, it is worth highlighting the importance of actions related to verification. The Verification of a measuring instrument consists of the Procedure comprising the examination, marking and/or issuing of a verification certificate and which verifies and confirms that the measuring instrument meets the regulatory requirements [1]. In other words, it aims to ensure the conformity of the instrument copy in relation to the approved model.

The marking procedure involves the affixing of marks, which can be verification, disapproval, model approval or sealing.

In particular, the sealing marks are intended to protect the measuring instrument against any unauthorized modification, adjustment, removal of components, etc. [1]. From a practical point of view, sealing marks typically aim to protect the instrument from alterations that may somehow influence the result of the measurement performed.

The practical realization of the concept of sealing marks typically involves the use of physical means, such as wire and numbered plastic seals, whose breaking allows detecting or suggesting possible access to set points of the operation and measurement results of the meter. It is common to find, for example, mechanical adjustment devices that receive sealing marks, in order to prevent them from being changed inadvertently, as shown in figure 1.

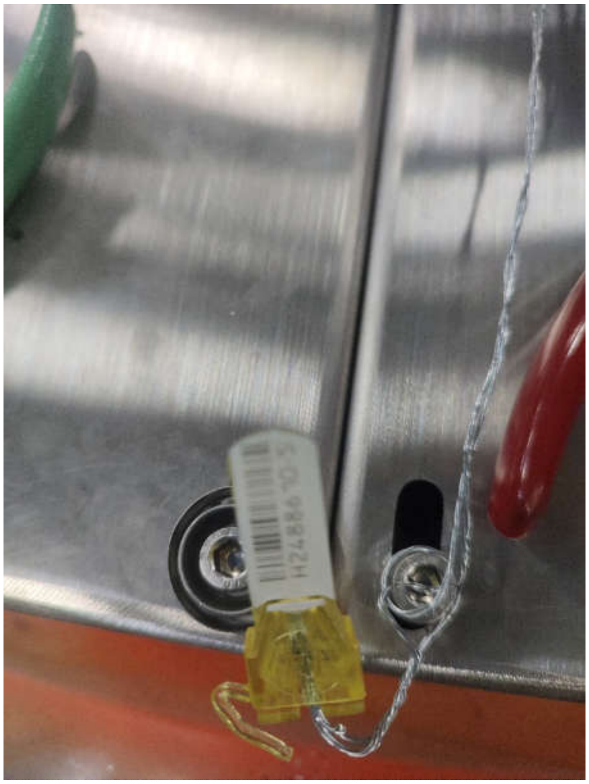


Figure 1: Plastic sealing mark, with metallic wire.
Source: Own elaboration.

Still from a practical perspective, in specific situations, the use of wire and physical seals, combined with potentially aggressive and/or corrosive atmospheres, can lead to an early breakage of the seals, even without user intervention.

The importance of verification activities, combined with the need for sealing resources and possible fragilities of the conventional model justifies the need to identify new sealing means, exploring, for example, the growing use of electronic instruments, strongly controlled by the use of software [2].

2. Methodology

The proposal addressed here consists of using checksum-type algorithms, typically associated with IT applications, however, increasingly present in electronic measuring equipment and instruments, controlled by software. Checksum algorithms typically aim to verify the integrity of data blocks, whether for storage or transmission [3]. They function as a type of “electronic signature”, which confirms that a certain piece of software or electronic file has not been altered.

Checksum, applied to an electronic sealing context, could be used in conjunction with physical/mechanical sealing. The logic consists of admitting that the same measuring instrument, if it does not undergo any change in its software, will be able to generate the same checksum value produced during an initial verification. This would be a way of guaranteeing that no parameter or part of the instrument's software has been changed.

For a real application, within the context of the current legal metrology regulation [4,5], first, the availability of the checksum resource must be informed by the applicant for the instrument model approval. This information, presented by the applicant, can be confirmed during the model evaluation tests and informed in the final ordinance.

In order for the checksum to be considered valid for the instrument model under test, in the ATM process, it will then be necessary to carry out tests, by the technician in charge, who must verify whether the change of parameters relevant to the operation of the instrument can generate different checksum m, and verifying that they are unique sequences [6] .

In other words, even if a parameter is changed to a value, and then changed back to the original value, the checksum algorithm will need to be able to generate unique sequences, not returning to the original value, as illustrated in figure 2, where 3 different checksums were generated, despite a parameter change and return to the original value.

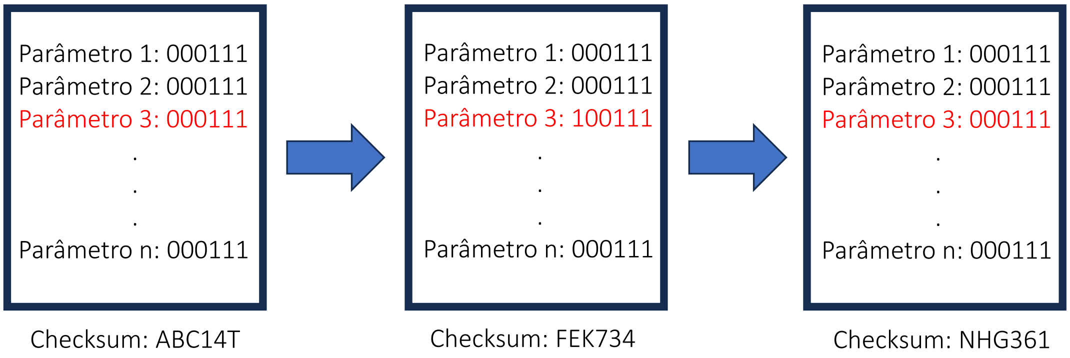


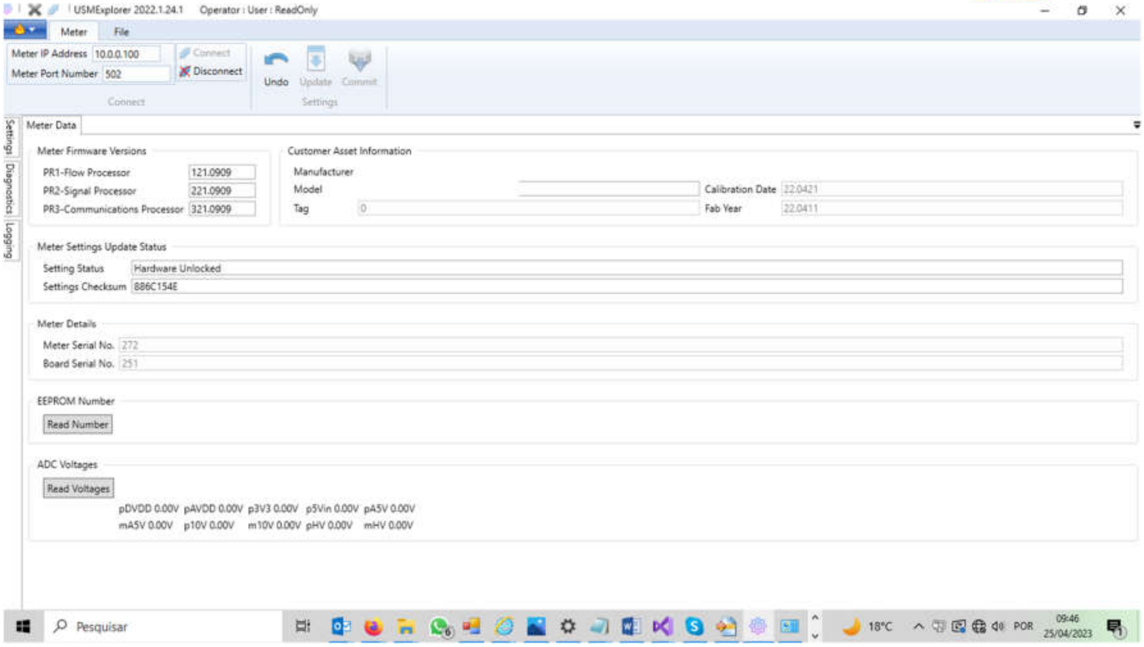
Figure 2: Changing parameters and generating a random checksum.
Source: Own elaboration.

This operating logic, where the checksum does not return to the initial value, even with the return of the parameters, allows using the checksum as a tool for detecting unwanted changes in the equipment's software, even if such changes are temporary or reversible. In the context of the proposal of this work, this test logic must be used in the model evaluation processes, varying metrologically relevant parameters of the meter, and observing if the checksum always presents different values, even with the return to the initial configuration of the test, then making it appear in the model approval ordinance that the meter has checksum support .

3. Discussion

A case study and test of the suggested methodology was carried out . To simulate the model evaluation procedure, an ultrasonic liquid meter was used, which currently already has a model approval ordinance, and as informed by the ordinance applicant, has a native checksum feature in its software.

First, through the meter management software, the initial value of the checksum was registered, as shown in figure 3, where the checksum value 886C154E was registered at the initial moment.



USMExplorer 2022.1.24.1 Operator : User : ReadOnly

Meter IP Address 10.0.0.100
Meter Port Number 502

Meter Data

Meter Firmware Versions
PR1-Flow Processor 121.0909
PR2-Signal Processor 221.0909
PR3-Communications Processor 321.0909

Customer Asset Information
Manufacturer
Model
Tag 0
Calibration Date 22.0421
Fab Year 22.0411

Meter Settings Update Status
Setting Status Hardware Unlocked
Settings Checksum 886C154E

Meter Details
Meter Serial No. 272
Board Serial No. 251

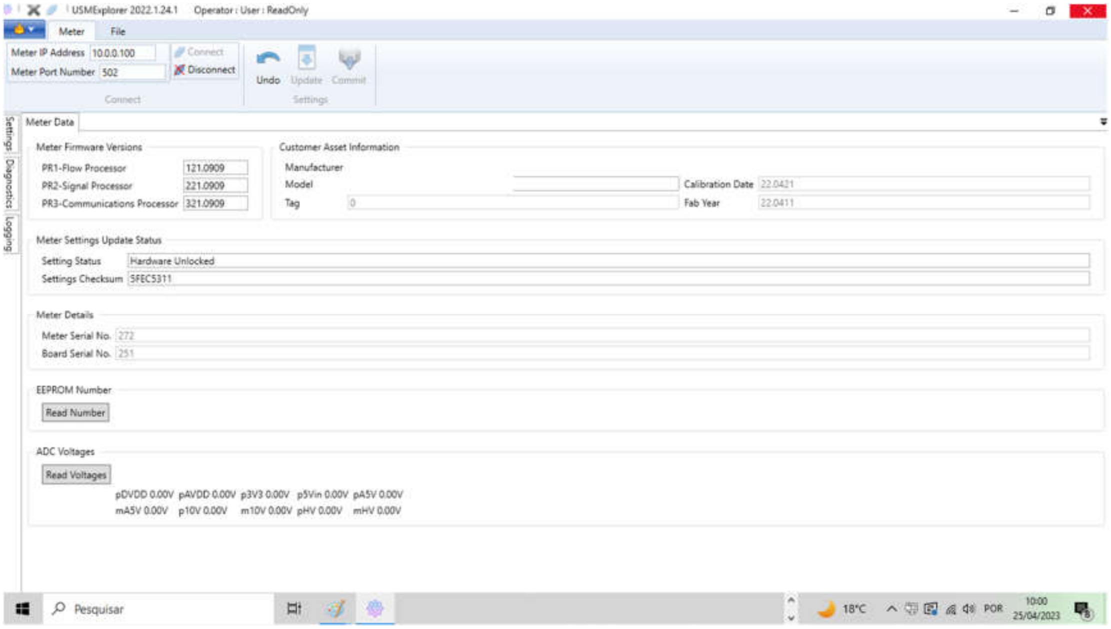
EEPROM Number

ADC Voltages
pDVDD 0.00V pAVDD 0.00V p3V3 0.00V p5Vin 0.00V pA5V 0.00V
mA5V 0.00V p10V 0.00V m10V 0.00V pHV 0.00V mHV 0.00V

18°C POR 09:46 25/04/2023

Figure 3: Configuration “as found” of the meter.
Source: Own elaboration.

Then, as it was an ultrasonic liquid meter, a metrologically relevant parameter was changed (the gain of one of the beams), and a new checksum value was recorded, 5FEC5311, illustrated in figure 4.



USMExplorer 2022.1.24.1 Operator : User : ReadOnly

Meter IP Address 10.0.0.100
Meter Port Number 502

Meter Data

Meter Firmware Versions
PR1-Flow Processor 121.0909
PR2-Signal Processor 221.0909
PR3-Communications Processor 321.0909

Customer Asset Information
Manufacturer
Model
Tag 0
Calibration Date 22.0421
Fab Year 22.0411

Meter Settings Update Status
Setting Status Hardware Unlocked
Settings Checksum 5FEC5311

Meter Details
Meter Serial No. 272
Board Serial No. 251

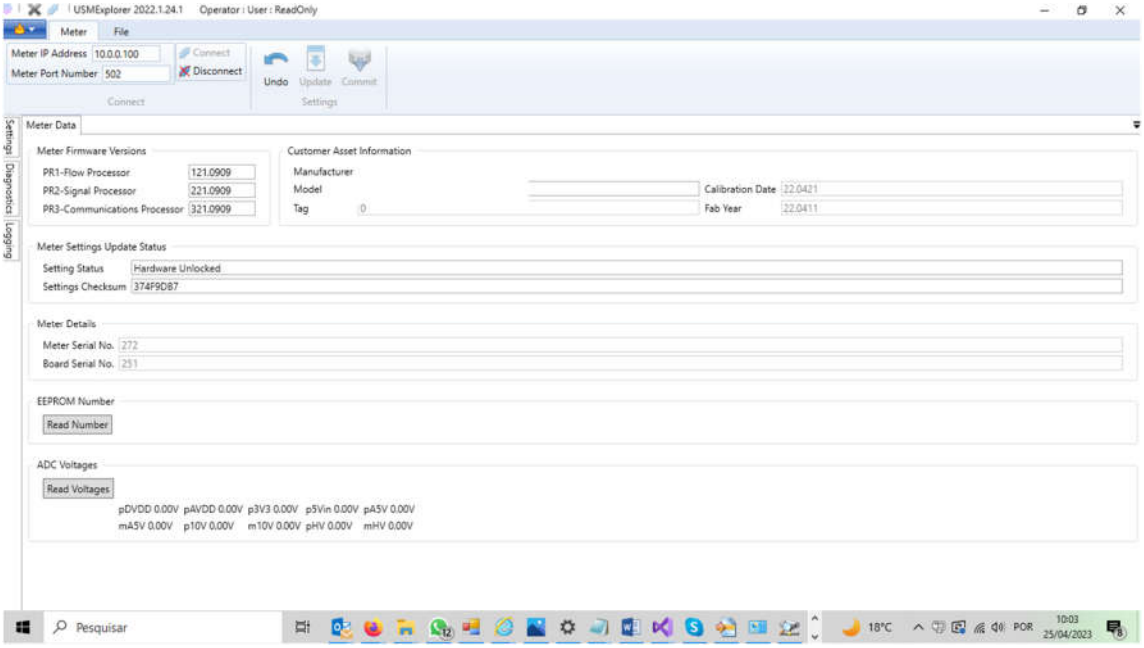
EEPROM Number

ADC Voltages
pDVDD 0.00V pAVDD 0.00V p3V3 0.00V p5Vin 0.00V pA5V 0.00V
mA5V 0.00V p10V 0.00V m10V 0.00V pHV 0.00V mHV 0.00V

18°C POR 10:00 25/04/2023

Figure 4: Meter configuration after changing a metrologically relevant parameter.
Source: Own elaboration.

The changed parameter (gain of one of the beams) was then set to its original value, and a new checksum was recorded (374F9D87), as shown in figure 5.



Operator : User : ReadOnly

Meter IP Address 10.0.0.100
Meter Port Number 502

Meter Data

Meter Firmware Versions
PR1-Flow Processor 121.0909
PR2-Signal Processor 221.0909
PR3-Communications Processor 321.0909

Customer Asset Information
Manufacturer
Model
Tag 0
Calibration Date 22.0421
Fab Year 22.0411

Meter Settings Update Status
Setting Status Hardware Unlocked
Settings Checksum 374F9D87

Meter Details
Meter Serial No. 272
Board Serial No. 251

EEPROM Number

ADC Voltages
pDVDD 0.00V pAVDD 0.00V p3V3 0.00V p5Vin 0.00V pA5V 0.00V
mA5V 0.00V p10V 0.00V m10V 0.00V pHV 0.00V mHV 0.00V

Figure 5: Meter configuration with parameter return to original value.
Source: Own elaboration.

The results obtained for the tested meter show that the checksum, even when recalculated, did not return to the original value. Under the logic of this work, this checksum calculation, if registered correctly in the initial verification, can be used as an electronic sealing parameter.

4. Conclusion

The checksum application model as an electronic sealing tool, presented in this study, is simple, and based exclusively on the functionality of the algorithms present in existing meters. It is not a resource capable of replacing physical sealing, but it can be seen as a complementary tool, considering that the generated checksums are unique, even if the parameter sets are reconfigured to original, previously known values.

The development of a more complete model of checksum use must consider not only the functionality aspects, employed in this initial model, but also the security and software integrity aspects, which were not addressed in this first approach, but which are of fundamental importance for the necessary reliability for the model approval and verification procedures.

Likewise, the requirements presented in OIML D-31 [7] must be considered in the constitution of a complete model, whose study and development is encouraged as a way of continuing this study.

References

[1] INMETRO. International Vocabulary of Legal Metrology – VIML, Inmetro Ordinance No. 163 of September 6 , 2005, 4th. Edition, 2005.

[2] RECCA, M.; TASCA, M.; MARTINO, G.; NAZZARRO, L.; AGOSTINO, L.; COPPOLINO, V. How legitimate is Legal Metrology Today ? The Case of Electronic Meters: Vacatio Legis. Management, Knowledge and Learning International Conference 2020. http://www.toknowpress.net/ISBN/978-961-6914-26-0/50.pdf Accessed on 5/30/2023.

[3] Checksums Advanced Topics , available at <https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html> Accessed 5/30/2023.

[4] RODRIGUES FILHO, BA; SORATTO, AN Legal metrology in Brazil and consolidation of the RBMLQ-I as a model for legal metrological control. Brazilian Congress of Metrology, 2013.

[5] SANDERS, R. Why do we regulating measuring instruments used for trade, 2011 OIML Bulletin Vol. LII no 2 13-15 .

[6] BENTO, LMS; COSTA, RO; BOCCARDO, DR; MACHADO, RCS; SA, VGP; SZWARCFITER, JL Software Fingerprinting and Applications to Legal Metrology. Available at: <https://www.cgti.org.br/publicacoes/wp-content/uploads/2017/09/Fingerprinting-de-Software-e-Aplica%C3%A7%C3%B5es-%C3%A0-Metrologia-Legal.pdf>. Accessed on: 06/12/2023.

[7] OIML Document 31, General requirements for software-controlled measuring instruments - Consolidated edition with Amendment 1. Available at: <https://www.oiml.org/en/publications/documents/en/files/pdf_d/d031-consolidated-e19.pdf>. Accessed on: 06/12/2023.