Implementing OM-BR Digital Certificates in Smart Meters

F P Agostini[1], **C E Galhardo**[1] **and R S Souza**[1]

[1] National Institute of Metrology, Quality and Technology, Duque de Caxias, 25250-020, Brazil

fpagostini@inmetro.gov.br, cegalhardo@inmetro.gov.br, rssouza@inmetro.gov.br

Abstract. As digital technologies pervading the metrological universe advance, a minimum guarantee of security in measurements becomes increasingly important. To strengthen the legal metrological control in measuring devices, the creation of a certificate policy for Metrological Objects (OM-BR) was approved. In this work, we discuss the implementation of OM-BR Digital Certificates in fuel dispensers.

1. Introduction

The automation and data exchange needs for Industry 4.0 leveraged the application of the Internet of Things (IoT) in critical infrastructures, such as power grids, gas pipelines, oil pipelines, transport networks, water supply, and so on. Especially in these critical sectors, the preservation of metrological characteristics and their traceability becomes a legal requirement, as well as cybersecurity [1]. Any vulnerability in the system in which the metrological network is inserted can have devastating consequences for the population and the environment. For example, the incident that occurred in May 2022 involving Colonial Pipeline, responsible for supplying almost 45% of the fuel on the East Coast of the United States, affected not only its computer infrastructure and pipelines but also the distribution and transportation of gasoline, causing panic in the citizens.

Tampering or modification are inherent risks in data captured by IoT devices. Metrology is responsible for the security of many critical operations, in which the origin and integrity of data are essential components [2]. According to [3], concerning a measuring instrument subject to legal control, objects that may be subject to these types of threats include:

(A) tampering measured values or assigning a measured value to an incorrect measurement;
(B) wrong measuring functions or parameters in the measuring instrument;
(C) inadequate or missing means of protection on the measuring instrument, facilitating the threats in (A) or (B).

Given that critical infrastructures in countries tend to be attractive targets for hackers, it becomes crucial to ensure security in IoT devices. One way to guarantee the integrity of a data source is through a digital signature with a cryptographic key [4]. When positioned as close as possible to the measurement consolidation, the digital signature provides a way to verify the accuracy of measurements, ensuring the legitimacy of the measurement [5].

An important application of digital signatures is public key certification, i.e., certifying that a public key belongs to a specific entity [6]. To ensure greater security in metrological devices, Inmetro defined the ICP-Brasil digital certification process in the signature of measurement records for metrological objects (OM-BR), established in document “Portaria Inmetro nº 103, de 08 de março de 2021”. In the

following sections, we will discuss in greater detail the OM-BR certification process and present a case study based on the experience gained with its insertion in liquid Fuel Dispensers.

2. Digital Certification of Metrological Objects (OM-BR)

As digital signatures only show the sender's private key used to produce them and do not prove the origin of the sender, the role of digital certificates [7] in our metrology applications becomes decisive. Digital certificates make it possible for digital signatures to be used as a way to formally validate the true owner of a public key. Certificate Authorities (CAs) are responsible for issuing digital certificates. A public key and the user's identity are bound in a certificate, which is signed with the private key of a trusted CA, certifying the accuracy of the binding. The digital certificate contains information such as the owner of a specific public key, the serial number of the certificate, the expiration date of the certificate, the issuer (i.e., the certificate authority), and the digital signature of the certificate authority.

As it is difficult to trust a single CA, multiple CAs are chained together to form a "chain of trust". There are two types of CAs - root CAs and intermediate CAs - chained together to link their digital certificates. Registration Authorities (RAs) assist CAs with the task of verifying user identities before issuing digital certificates. The endpoint of a chain is an end-user certificate. If a CA is untrusted, the certificates it issues are also untrusted. CAs can revoke a digital certificate for a diversity of reasons, including expiration, compromised private key, and policy violation. Anyone who needs a user's public key can obtain the certificate and verify that it is valid through the attached trusted signature. In fact, all intermediate certificates up to the root CA are required.

Many institutions, governments, and corporations can issue their own certificates. The model adopted in Brazil has a single root, with the ITI (National Institute of Information Technology) being the body responsible for playing the role of Root Certificate Authority (Root CA) in the Brazilian Public Key Infrastructure (ICP-Brasil).

Due to the need to strengthen legal metrological control in measuring devices, a certificate policy for Metrological Objects (OM-BR) within the scope of ICP-Brasil was made available, defined in the document “Resolução ITI nº 139, de 03 de julho de 2018”. Metrological objects are measurement devices regulated by Inmetro, such as water meters, gas meters, scales, fuel dispensers, energy meters, and so forth. The OM-BR is a special type of certificate to be installed in safe microprocessors or hardware modules, used for metrological purposes, issued exclusively for equipment regulated by Inmetro, creating a unique identifier for each device, in addition to guaranteeing correct measurement to avoid possible fraud. This certificate uses Elliptic Curve cryptography and is valid for 10 years. On May 11, 2022, the document “Ato Declaratório Executivo nº 1/ITI/PR” was published, in which the first cryptographic device for use in metrological objects compatible with the standards of the Brazilian Public Key Infrastructure (ICP-Brasil) was approved for issuing OM-BR certificates.

In this scenario, Inmetro, through the Division of Metrology in Information Technology and Telecommunications (DMTIC), starts to act as a first-level certificate authority of ICP-Brasil, using the SERPRO infrastructure as Support Service Provider (SSP). As it becomes ICP-Brasil's first-level certificate authority, it is responsible for providing the digital certification process, defining the criteria for accreditation at the Inmetro Certificate Authority (CA Inmetro) and describing the layout of digital certificates in the document "Portaria nº 103, de 8 de março de 2021". Inmetro will not provide digital certificates for metrological objects but will accredit other entities (second-level CAs) to issue OM-BR certificates. This means it is up to CA Inmetro to issue, distribute, revoke, and manage second-level CA certificates, providing users with a list of revoked certificates and other necessary information. Documentation regarding the digital certification processes conducted by CA Inmetro is available at https://www.gov.br/inmetro/pt-br/assuntos/certificacao-digital.

It is worth noting that the OM-BR certification process also includes the role of an Electronic Registration Authority, instituted by the document "Resolução CG ICP-Brasil nº 197", which amends DOC-ICP-03, DOC-ICP-04, and DOC-ICP-05. This technology allows the digital certificate to be generated autonomously and without the intermediation of a registration agent. In the case of OM-BR

certificates, it is a software component maintained by the CA, which must be used at the manufacturer's facilities to obtain data from metrological objects, command the generation of cryptographic keys, send requests to the CA system, and, finally, command the installation of the certificates issued in the respective metrological objects. Manual entry or manipulation of metrological object information in the certification process is prevented to avoid the possibility of human error or fraud. The manufacturer of the metrological equipment is the holder of the digital certificate installed in the metrological objects.

Although the cryptographic microprocessor with the OM-BR certificates adds an additional cost to the measuring devices, the digital certification of metrological objects brings the compensation of a more agile inspection, even allowing the participation of consumers in the fight against fraud.

3. Implementing OM-BR Digital Certificates in liquid Fuel Dispensers

At the same time as Brazil is part of one of the largest fuel markets in the world, it also accumulates losses due to a diversity of frauds in this sector. Frauds involving tampering (in measurement) of volume are of special interest to metrology and occur both due to the lack of protection of the measurement data that travels inside the instrument until the measurement value is presented in the indicating device and due to the lack of embedded software protection mechanisms [8]. In general, this type of fraud occurs with the interception of pulses regarding the fueling between the pulser (fuel dispenser measuring system) and the CPU, in order to tamper with the amount of fuel in the indicator device [9], resulting in damage to customers and consumers. However, it should be taken into account that there is a tolerance regarding the maximum errors allowed in fuel dispensers, as defined in the document "Portaria Inmetro nº 227 de 26/05/2022".

One way to provide greater security to the consumer is through a system that allows verification of the actual volume supplied. As we have seen, the digital signature is used exactly for this purpose, in order to make it impossible for an attacker to obtain a valid signature for a forged value. An architecture based on digital certificates for smart meters and applied to fuel dispensers was proposed in [10]. In addition, the first proposal for an ICP-Brasil OM-BR digital certificate was mentioned in the document "Portaria Inmetro nº 559, de 15 de dezembro de 2016", to ensure minimum reliability in liquid fuel dispensers concerning the possibility of fraud. For this reason, an ICP-Brasil OM-BR digital certificate must be stored in each transducer device (pulser), so that one can reference it without ambiguity. Considering that a fuel dispenser can contain several pulsers, a cryptographic chip containing the digital certificate must be added to each one of them. This document was revoked by document "Portaria Inmetro nº 227, de 26 de maio de 2022", approving the consolidated Technical Metrological Regulation (RTM) for liquid fuel dispensers. In addition to extending deadlines for compliance with the new regulation, the document also adds new software and hardware requirements to those already required by the documents "Portaria Inmetro nº 559/2016" e "Portaria Inmetro nº 294/2018".

By then, inspection of fuel dispensers involved a very complex process, difficult to verify locally, so, normally, proof of fraud required the seizure of electronic boards for laboratory analysis and generation of supporting material. This process could be quite time-consuming. However, the introduction of OM-BR Certificates at fuel dispensers brings the possibility of a faster and more efficient process. The signed measurement is made available through a Bluetooth module, allowing the quick verification of the digital signature and the pulser certificate, just by accessing a mobile device with a Bluetooth interface and an application capable of carrying out the verification. If any device involved in the supply has a verification failure, its operation is prevented until authorized maintenance is carried out by a technical manager authorized by the metrological body. In this case, an event is stored in the audit log.

To make possible the quick verification of signatures and certificates at fuel dispensers, accessible to inspectors and even consumers, the Computer Security Laboratory (LabSEC) of the Federal University of Santa Catarina, in partnership with Inmetro, has been developing the application " Medida Segura", capable of communicating with the new liquid fuel dispensers. Initially, the application performs a Bluetooth scan, displaying the fuel pumps in range. After selecting the desired fuel dispenser,

the pairing between the device and the fuel dispenser takes place. Then, the application receives some general data from the fuel dispenser and asks for the choice of the indicator device used for fueling. Finally, the application receives the data associated with the last supply of the indicating device. If the digital signature is invalid, the application displays an error message. If it is not possible to establish a network connection, checks for digital signatures are made locally and, therefore, it is not possible to check for revoked certificates.

Some fuel dispenser models have already been approved by accredited laboratories. Having carried out the necessary tests for type approval, the industries are authorized to commercialize these instruments. To close the cycle, Inmetro has been developing a training model for inspectors so that they can monitor the evolution of technologies and innovations employed.

4. Final Considerations

The use of OM-BR Digital Certificates in Smart Meters can drastically reduce fraud in measuring instruments through a reliable hardware-based module. However, the application of this technology requires that the instruments currently in use be changed or adapted. In the case of Fuel Dispensers, those approved in accordance with the document "Portaria Inmetro nº 23, de 25 de fevereiro de 1985" may be adapted to meet the requirements of the new regulation. However, the exchange must be made in case of proven fraud. There is, however, a concern not to burden the industry and the consumer too much, so these adaptations will be made gradually until 2033. Anyway, mechanical fuel dispensers will have to be withdrawn, as they cannot be updated to meet the new standards.

Another point to consider is that the period of validity of the OM-BR digital certificates contained in the cryptographic chips is 10 years and, after this period, equipment with an expired certificate will issue a validation error. Therefore, it is necessary to exchange the certificate after 10 years. Considering the case of Fuel Dispensers, it is necessary to change the pulser, containing a new certificate, after this period. In this case, it is estimated that the lifetime of the pulser is equivalent to the validity period of the certificate, so this would not generate a large financial impact.

Even taking into account that the use of digital certificates can bring some financial cost, it is estimated that the benefits of this technology can also bring a significant positive impact in the fight against tax evasion since fraud generates losses not only for citizens but also for the Brazilian tax system.

In this new architecture model developed for smart meters, the consumer also plays a relevant role in field surveillance. Having only a cell phone with an application, consumers can check the validity of a signature and digital certificate. The issue to observe here concerns the responsibility for maintaining and developing an application, which requires constant updates to adapt to new technologies. An important step in this direction would be the search for partnerships with the industry since Inmetro's infrastructure does not support the constant maintenance of these applications.

As we saw in the example of Fuel Dispensers, the Bluetooth interface is used to export the OM-BR Digital Certificates containing the measurement signatures. Although effective, this technology brings some inconveniences, such as the need to scan all available pumps and then select the desired pump. It is estimated that a technology that could more efficiently replace Bluetooth is the QR Code, which could bring more dynamism to the validation of certificates.

In the specific case of Fuel Dispensers, other technologies have also been studied, to inhibit fraud. Papers [11, 12] use IoT-based meters inserted in vehicles to estimate the amount of fuel received in fueling events, associated with Blockchain technology for a distributed and decentralized surveillance solution. Another approach is the use of a tool called SAT (Electronic Tax Coupons Authenticator and Transmitter System), which provides government authorities with the fuel values associated with each of the fuel dispenser nozzles; an indication of irregularity points to the need for inspection.

If, over time, the experience with Liquid Fuel Dispensers proves to be, in fact, successful, it may be expanded to other meters regulated by Inmetro, such as scales, energy consumption meters, and speed controllers, among many others, including equipment in the conformity assessment program.

References

[1] Aranha H, Masi M, Pavleska T and Sellitto G P 2021 Securing the metrological chain in IoT environments: an architectural framework *IEEE International Workshop on Metrology for Industry 4.0 & IoT* - MetroInd4.0&IoT, Rome, Italy, pp. 704-709

[2] Mustapää T, Autiosalo J, Nikander P, Siegel J and Viitala R 2020 Digital Metrology for the Internet of Things (1-6, 10.1109/GIOTS49054.2020.9119603)

[3] Thiel F, Hartmann V, Grottker U and Richter D 2014 IT Security Standards and Legal Metrology – Transfer and Validation *EPJ Web of Conferences* 77, 00001

[4] Diffie W, 1988 The first ten years of public-key cryptography *Proceedings of the IEEE*, vol. 76, no. 5, pp. 560–577

[5] Boccardo D, Machado R, Camara S, Prado C, Melo Jr W, Ribeiro L and Carmo L 2014 Software Validation of Medical Instruments *IEEE International Symposium on Medical Measurements and Applications* - MeMeA, Lisboa, Portugal, pp. 1-4, doi: 10.1109/MeMeA.2014.6860090

[6] Kurose J and Ross K 2021 Computer Networking: A Top-Down Approach (Pearson, 8th edition)

[7] Stallings W 2020 Cryptography and Network Security: Principles and Practice (Pearson, 8th edition)

[8] Andrade P, Marques L, Dias J, Diniz M, Signoretti G, Silva I, Melo W S and Galhardo C 2021 Uma Solução Baseada na Internet dos Veículos Inteligentes para a Vigilância Metrológica de Bombas de Combustível *XV Simpósio Brasileiro de Automação Inteligente* - SBAI

[9] Leitão F O, Vasconcellos M T and Brandão P C R 2014 Hardware and Software Countermeasures on High Technology Fraud at Fuel Dispensers under the Scope of Legal Metrology *IX Simpósio Internacional Metrologia*, Havana, pp. 1–10

[10] Melo W S, Machado R C S, Abreu B, Carmo L R and Ramos R 2019 Certificação Digital como Ferramenta de Segurança para Medidores Inteligentes *Anais estendidos do Simpósio Brasileiro de Engenharia de Sistemas Computacionais* - SBESC

[11] Melo Jr. W S, Tarelho L V G, Rodrigues Filho B A, Bessani A N and Carmo L F R C 2021 Field surveillance of fuel dispensers using IoT-based metering and blockchains *Journal of Network and Computer Applications* Volume 175

[12] Andrade P, Silva I, Signoretti G, Silva M, Dias J, Marques L, Melo W S and Galhardo C 2021 A Metrological Fuel Surveillance Application Based on Internet of Intelligent Vehicles, *IEEE International Workshop on Metrology for Automotive* (MetroAutomotive), Bologna, Italy, pp. 76-81, doi: 10.1109/MetroAutomotive50197.2021.9502890