INMETRO

OM-BR Digital Certificate

March/2021

Digital Certificate OM-BR

What is a PKI

- Public Key Infrastructure is a consolidated technology devoloped in the 70´s
- Make use of Digital Certificates and Assymetric Cryptography
- Centralized system with a Certification Authoritie (CA) that should be acepted by the peers and users
- In Brazil there is a governement CA that emits certificates in the ICP-Brasil chain. This certificates has legal value throughout the country
- It is used by persons, companies, justice, medical doctors, and others to digitally sign documents, also to web pages to be trusted in browsers and other internet aplications

Digital Certificate OM-BR

What is a certificate OM-BR

- The Brazilian Certification Authority of ICP-Brasil create in 2018 an special king of certificate to be installed in secured microprocessors or hardware modules, to be used for metrological purpose

- This kind of certificate is called Metrological Objects – BR (OM-BR), and use Elliptical Curves cryptography with validity of 10 years and expectation of 20 years robustness

- Inmetro is in the process of regulate the usage of this certificate, and by March 2021 it should be available to the industry and general public

- The first use case will be signing the measurement of gas pump pulser. This is the pilot project, and many other applications could be develop

Digital Certificate OM-BR

Motivation for the use of Certificates

- Many legal metrology devices has embedded electronic and software. For Type Approval is necessary a complex, expensive, intrusive, time consuming process of software evaluation
- With an architecture of a sensor, and just beside a cryptographic module with a digital certificate, it is not necessary to evaluate hardware or software after the point where the measurement is signed.
- This extremily simplifies the process of Type Approval, but it still necessary to verify physically the sensor and the microchip
- It is really not necessary to use a certificate in the Brazilian PKI ICP-Brasil, but doing this gives legal validation, with a small increase in the cost
- The price of the certificate could be very small, and the large cost is the cryptographic microprocessor

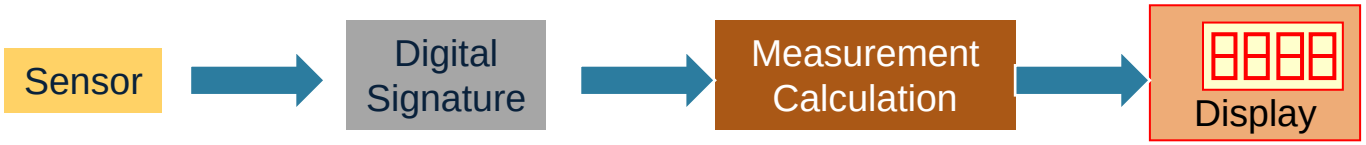
Digital Certificate OM-BR

Historical

- **There were a first trial 10 year ago with a electrical measurement system. Inmetro regulation #11 of 13 January 2009. At that time there was no use of cryptographic microchip or ICP-Brasil digital certificate**

The measurement system / instrument may use a digital signature mechanism to ensure the authenticity and irrefutability of the measurement information

The output quantities, that is, the accumulated value in kWh, or input quantities may be signed together with information that allows to reconstitute the value of the output quantity

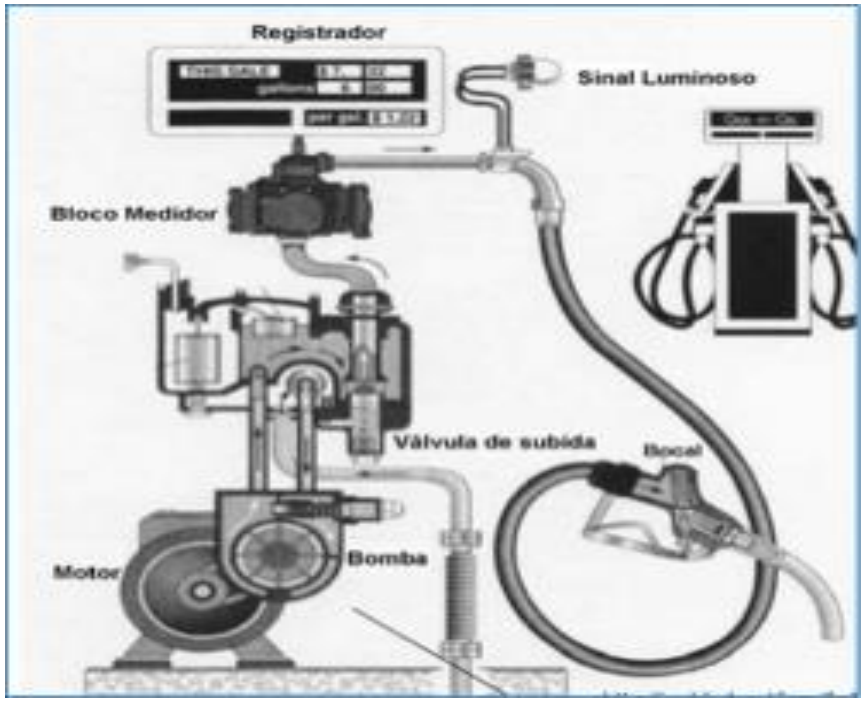


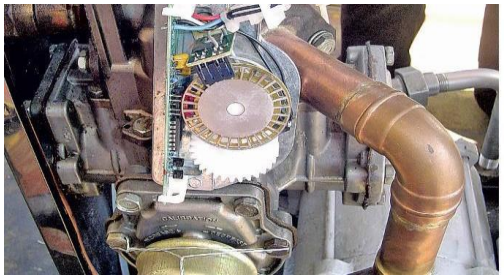
Digital Certificate OM-BR

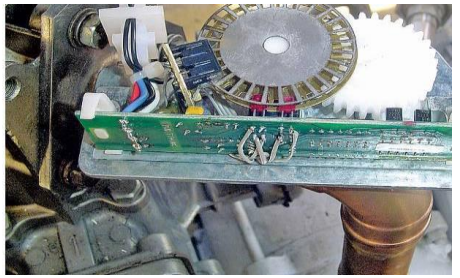
First use case – gas pump

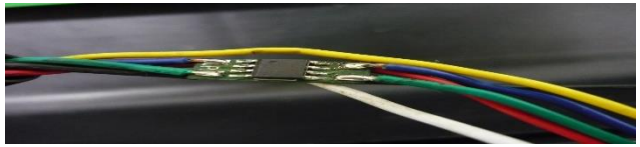
- The regulation is finished and publish, and the manufactures will have products ready to sell to gas stations in the beginning of 2021

- The measurement system – sensor – of the gas pump is the pulser, and the cryptographic microchip and certificate is inside each pulser. The gas pump normally has several pulsers









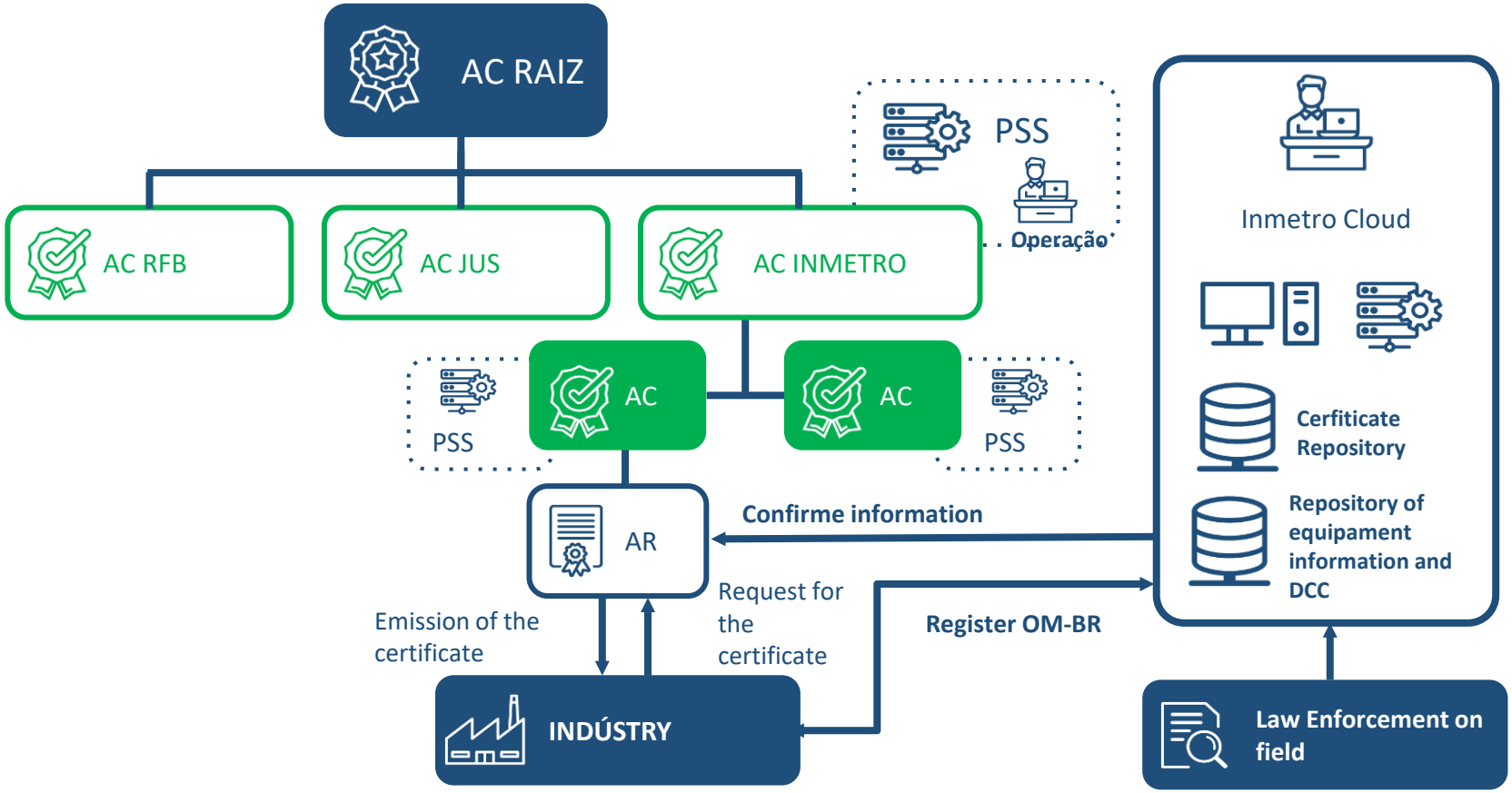
Digital Certificate OM-BR

Mobile Phone Integration

- An app for mobile phone that talks to gas pump using Bluetooth, or QR Code
- Basic and advanced functionalities for the consumers
- Verify the digital signed measurement
- Some other information could be stored in the gas pump, as the DCC
- Could also send the data to Inmetro, to prepair law enforcement actions
- Give the consumers tools to be the first tier or fiscalization and law enforcement

Digital Certificate OM-BR

Architecture of the Certificate Chain



Digital Certificate OM-BR

Many new Ideas/Projects

- **Smart Seal**
- **Unique identifier of any kind of metrological devices**
- **Integration with DCC and Digital Twin**
- **Blockchain of OM-BR certificates**

Digital Certificate OM-BR

OM-BR Certificate

- The digital certificate OM-BR creates a unique identifier of any device
- The cryptographical elliptical curve is robust for about 20 years against computers attacks
- The certificate OM-BR will sign the DCC, and this could be stored in the equipment, or in the Inmetro metrological cloud, or even both
- The digital twin will be univocally associated to the device with the digital signature OM-BR
- Any kind of mistake, adulteration, fraud could be easily checked with the validity of the certificate, and ICP-Brasil Chain

Another Solution for Metrological Device Identification

- **Real Problem – Half of the Market Scales in Brazil are ilegal, not registered not verified**

- **Digital Certificate could be expensive for this kind of product**

- **What is the solution ?????**

Digital Certificate OM-BR

OM-BR Certificate and DCC

- The QR Code should contain information of the equipment – model, serial number, calibration certificate number….
- It also contain position (lat, long) of the installed equipment – prevent copying
- It not really a unique ID, but a compliment of legal metrology seal
- Use of smartphone APP to read the QR Code, and validate the scale
- It not guarantee the measure value

Ouvidoria: 0800 285 1818

inmetro.gov.br / **facebook.com/Inmetro**

youtube.com/tvinmetro / **twitter.com/Inmetro**