Public Key Infrastructure for Legal Metrological Control

Marcos T. Vasconcellos
Head of Supervision in Legal Metrology - INMETRO

Teamwork

José Carlos da Silva Neto

Marcos Trevisan Vasconcellos

Osvaldo Prisciliano - IPEM/SP

INSTITUTO DE PESOS E MEDIDAS DO ESTADO DE SÃO PAULO

IPEM-SP 50 ANOS

Objectives

This platform aims to increase security in Legal Metrology and ICT security, providing confidence, authenticity, integrity and non-repudiation of measurements even in hostile environments.

Provide advanced technological support for new applications in Legal Metrology, including Smart Cities, Smart Grid and IoT.

To ensure the use of the cloud, conference and display measurements, real-time monitoring, online conference digital certificates.

Implement Metrology NPL for 2020 in Legal Metrology

- Measuring at borders
- Intelligent and interconnected measurement
- Built-in and ubiquitous measurement

Motivation

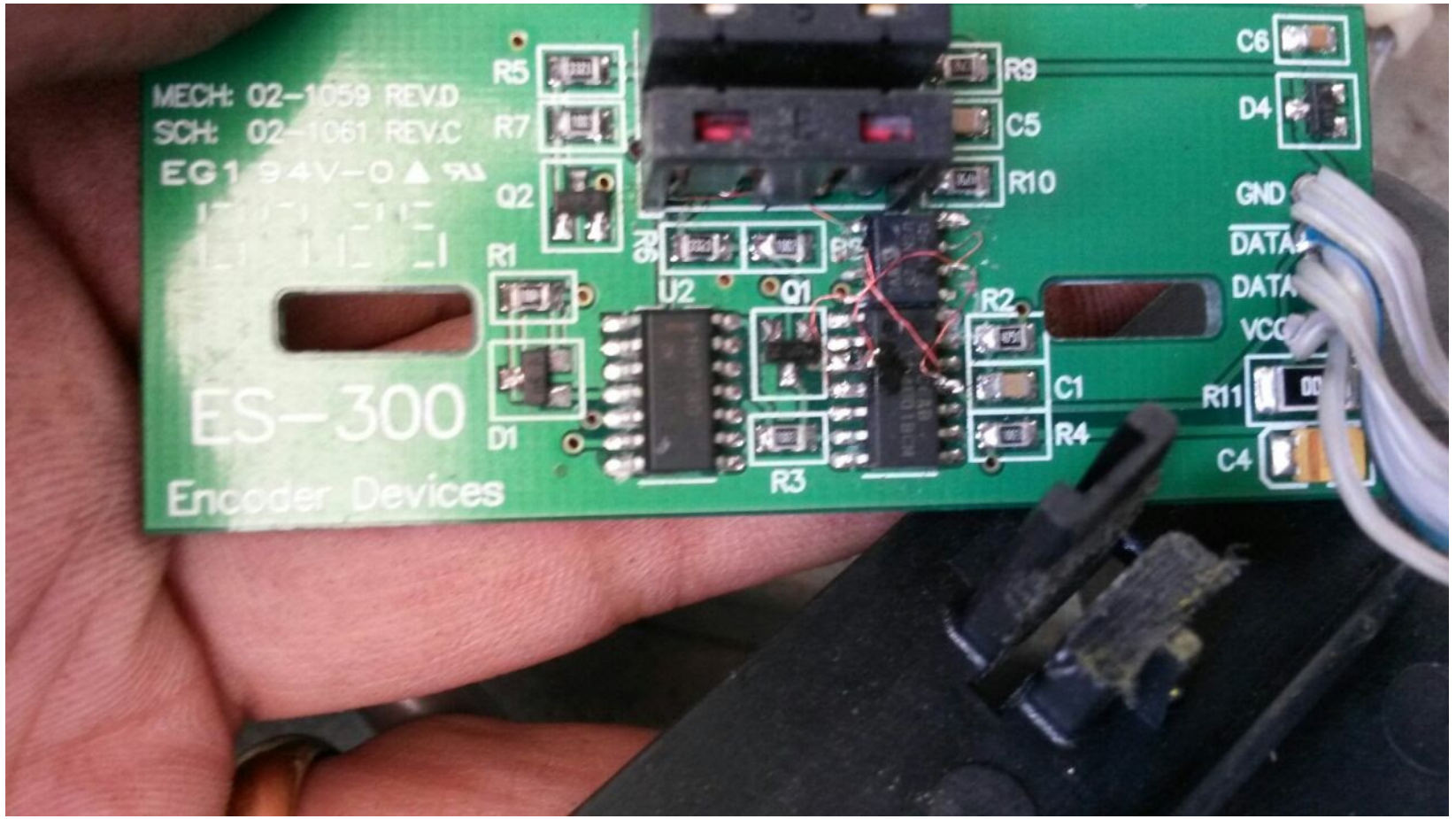
More and more fraud in metrological equipment using almost invisible digital interfaces

Example:
Frauds on fuel dispensers:

- Fuel dispensers are tampered to deliver less fuel than displayed;
- It envolves PCB and encoder tampering, insertion of ICs on communication line,
- Brand new PCBs are produced to fraud the consumer;
- Remote controlled (wirelessly);
- Hard to find and detect.

And others frauds

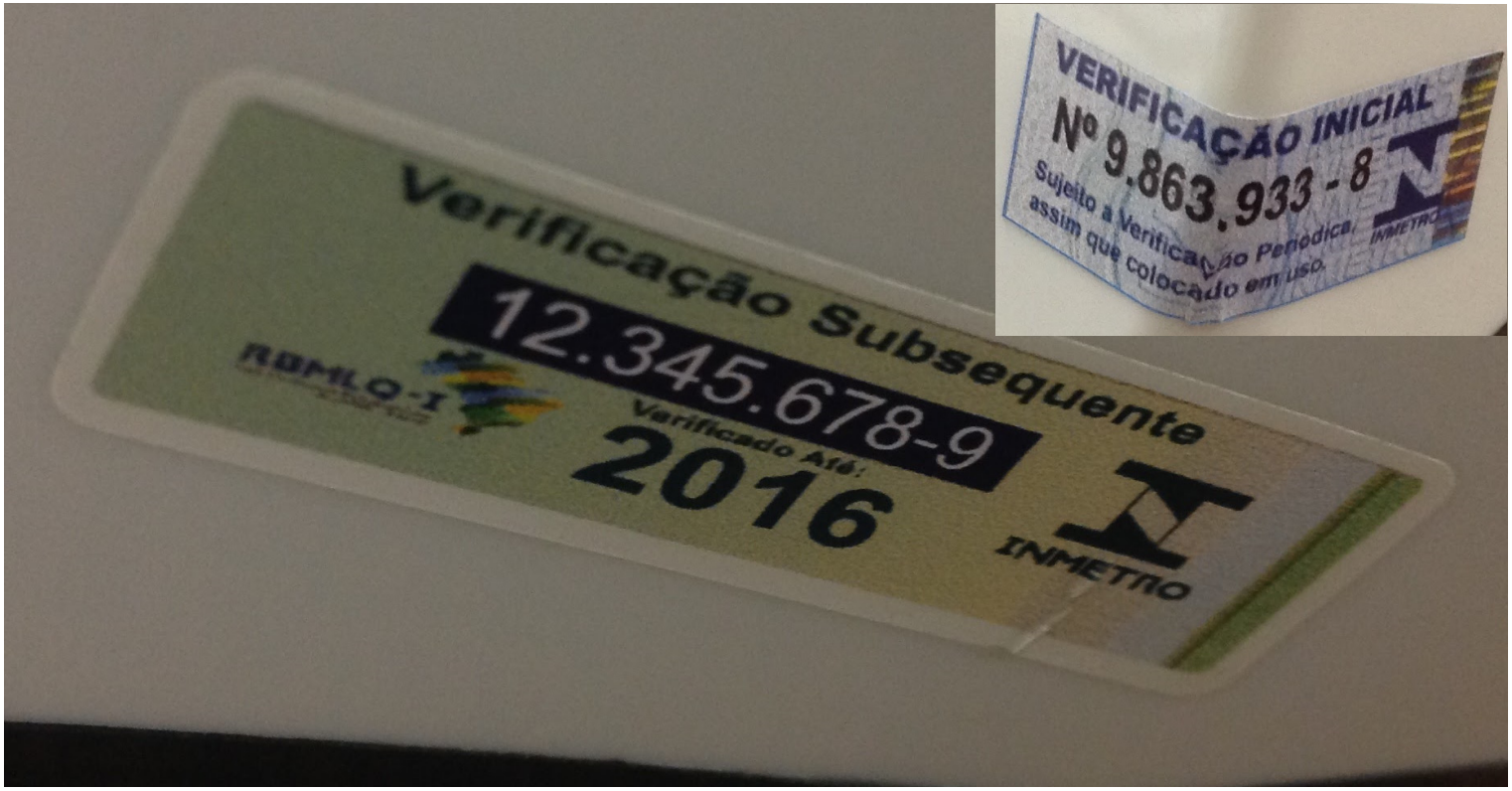
Tampered encoder



ICs on communication line

PCB tampering

Frauded marks on scale



Challenges

Lowest possible cost
Regulatory compliance
Standardization and interoperability of secure technology
Traceability of information
Remote inspection of equipment
Guarantee of the data transported from the equipment to the customer or the database
Adequate to the law of transparency (any citizen can request any public information and the form that was obtained)

The transparency law requires public information to have:
Availability, authenticity: integrity, primary.

Brazilian Transparency Law

The transparency law requires public information to have:

I - **availability**: quality of information that may be known and used by authorized individuals, equipment or systems;
II - **authenticity**: quality of information that has been produced, issued, received or modified by a particular individual, equipment or system;
III - **integrity**: quality of unmodified information, including origin, transit and destination;
IV - **primary**: quality of information collected at source, with the maximum possible detail, without modifications.

Secure Platform

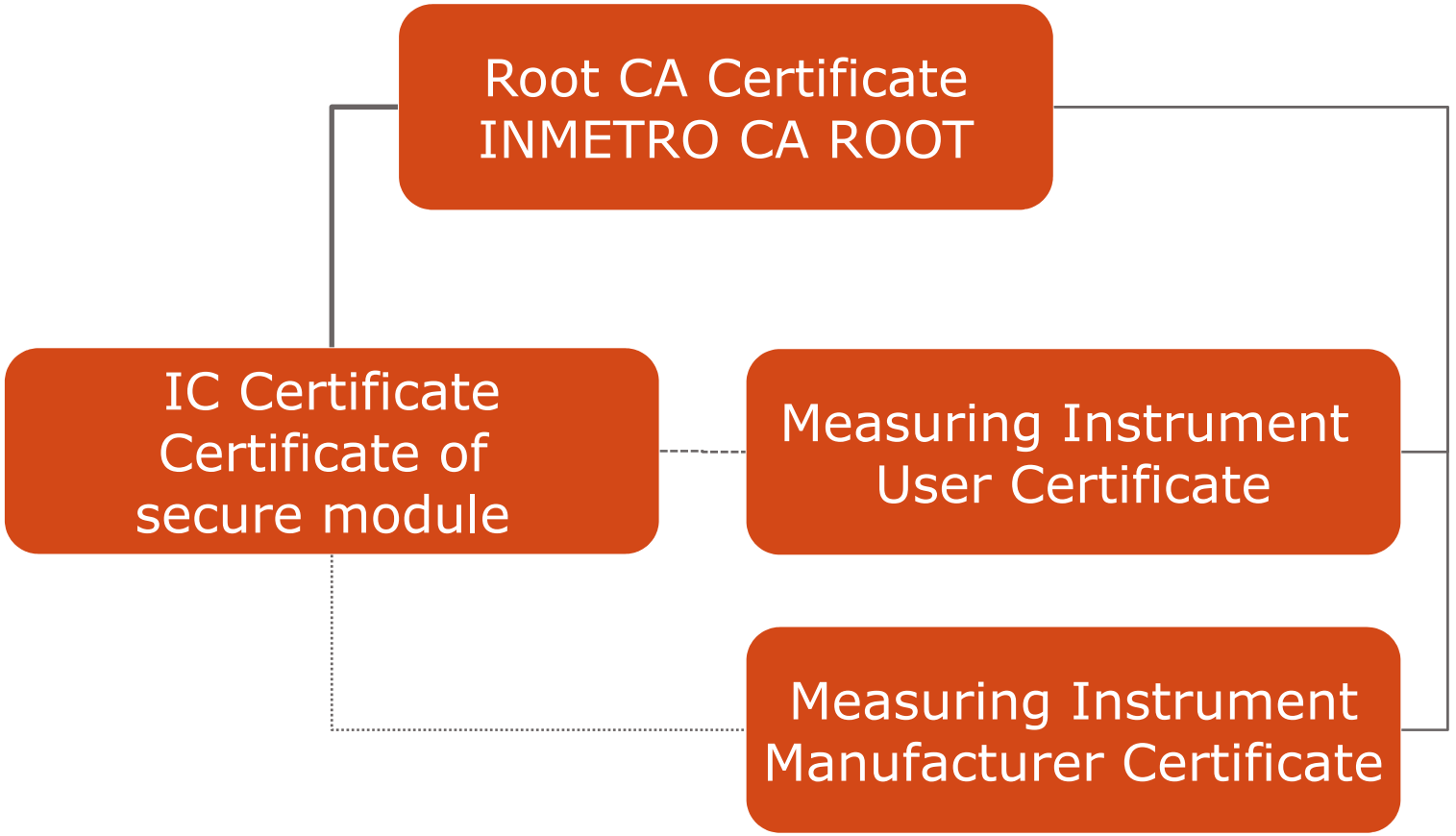
The platform designed to address this issue was the adoption of secure chip modules and a public key infrastructure controlled by INMETRO (PKI-INMETRO)

Public Key Infrastructure

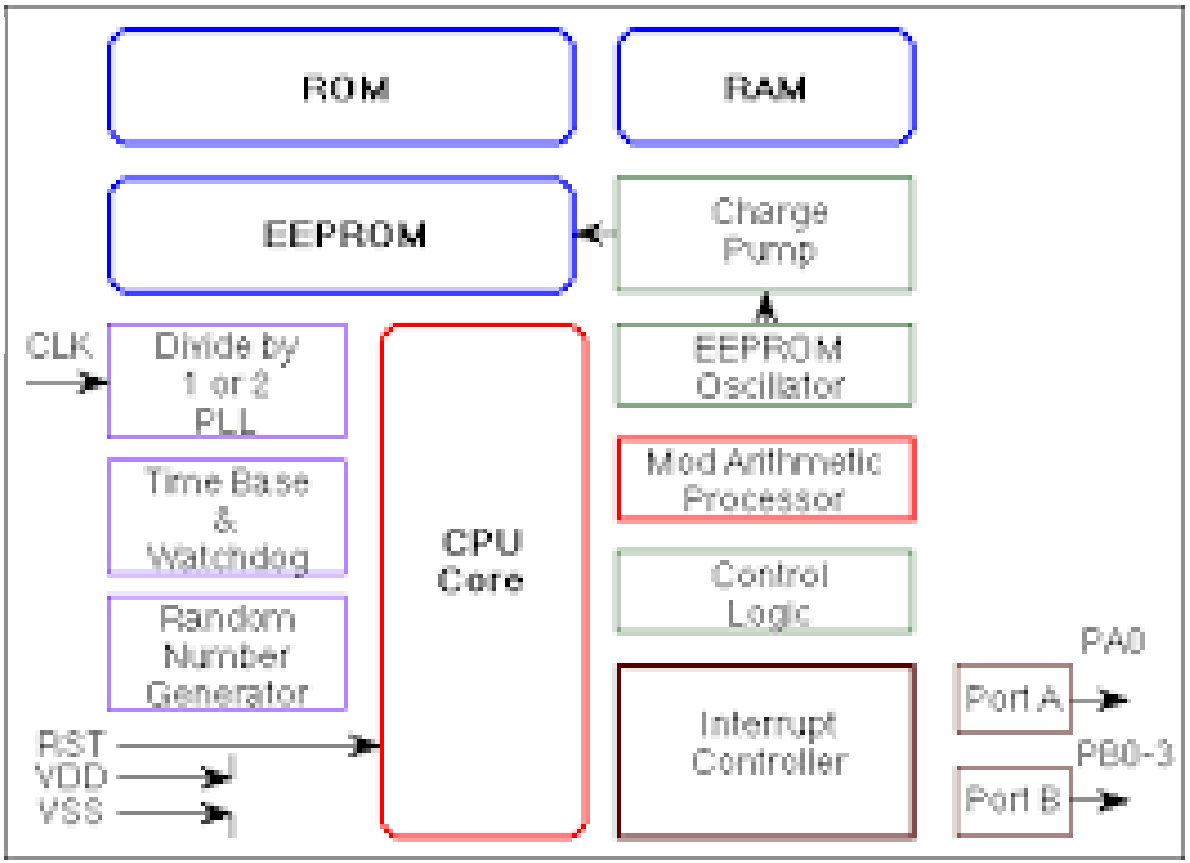
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

It provides confidence in the transaction between two parties, assuring inequivocaly autentication, integrity and non repudiation to messages exchanged in activities such as e-commerce, internet banking and confidential email.

Three-level digital certificate



Cryptographic Modules



Digital Certificate X.509

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Standard & Interchange commands

ISO/IEC 7816

ISO/IEC 7816 is an international standard related to electronic identification cards with contacts, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Most used parts of ISO 7816

7816-4: Organization, security and commands for interchange
7816-15: Cryptographic information application

PKCS

In cryptography, PKCS stands for "Public Key Cryptography Standards". These are a group of public-key cryptography standards devised and published by RSA Security Inc, starting in the early 1990s.

The PKCS #11 standard defines a platform-independent API to cryptographic tokens, such as hardware security modules (HSM) and smart cards. Most commercial certificate authority software uses PKCS #11 to access the CA signing key or to enroll user certificates.

The PKCS #15 defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of PKCS #11 or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15.

OIDs

In computing, object identifiers or OIDs are an identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.[1]

An OID corresponds to a node in the "OID tree" or hierarchy, which is formally defined using the ITU's OID standard, X.660.

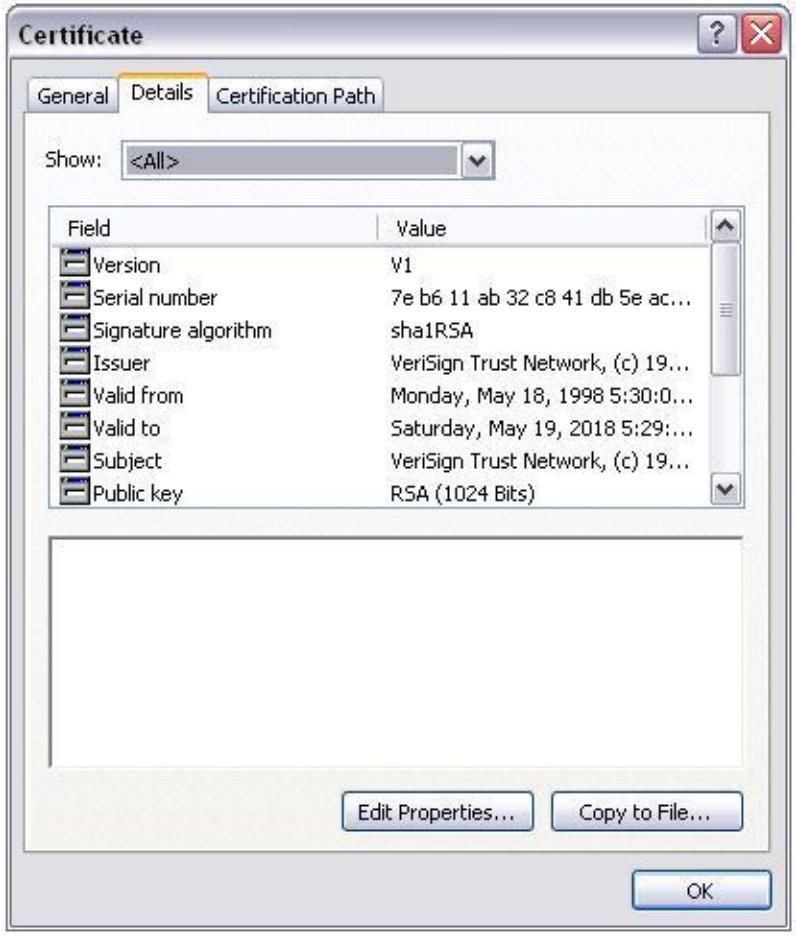
Inmetro OID
1.3.6.1.4.1.49713

Crypto Module/Common Criteria/FIPS 140-2/ISO 7816

Random Number Generator
Key protection
- physical
- logical

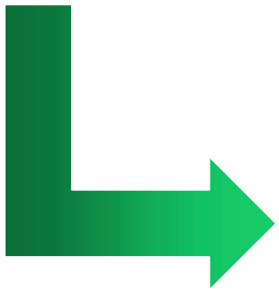
Standard API
OID - object identifier
Three level digital certification

Digital Certificate X.509




```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

PKI



Measuring Instrument

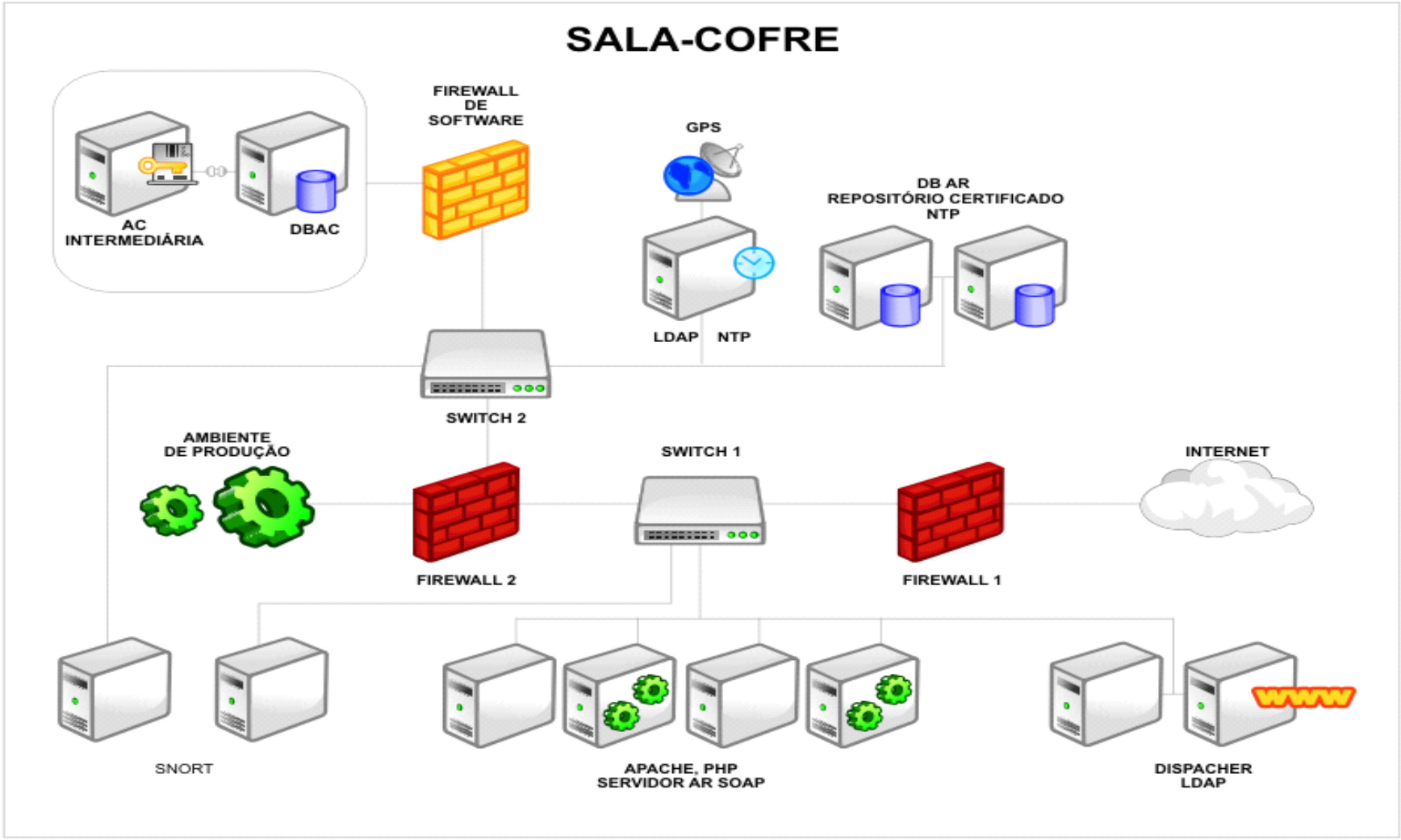
Cryptographic Module

PKI for Legal Metrology

Confidence in measurements;
Use of insecure or shared communication channels;
Identification for measuring instruments for:

- Smart Grid;
- Smart Cities;
- IoT;

Use of cloud computing and storage;
Emergence of new services for legal metrology;
Elimination of physical seals and marks;
Prevent and eliminate frauds


SALA-COFRE
AC INTERMEDIÁRIA
DBAC
FIREWALL DE SOFTWARE
GPS
LDAP
NTP
DB AR
REPOSITÓRIO CERTIFICADO
NTP
SWITCH 2
AMBIENTE DE PRODUÇÃO
FIREWALL 2
SWITCH 1
FIREWALL 1
INTERNET
SNORT
APACHE, PHP
SERVIDOR AR SOAP
DISPACHER
LDAP
WWW

Marcos T. Vasconcellos

mtvasconcellos@inmetro.gov.br
Voice +552126799820
+ 5521981455666

José Carlos da Silva Neto

j.neto@grupocermob.com.br
Voice +553125113881
+ 5531991072162

Títulos (fonte Arial Bold - corpo 32 a 36)

Subtítulos (fonte Arial Bold - corpo 25 a 28)

Cor: Azul marinho

Texto (fonte Arial Bold - corpo 18 a 21)

Texto para tabelas (fonte Arial Bold Italic - corpo 16)

Cor: Preto ou cinza

Cor para linhas e setas

Cores para aplicações em gráficos e desenhos:

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a NIST U.S. government computer security standard used to approve cryptographic modules.

This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing levels of security. The security requirements cover areas related to the secure design and implementation of a cryptographic module, such as cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.