Blockchain and Digital Certification Applications in the Cloud

Dr. Jean E. Martina
UFSC - Brazil

Problem Definition

- IoT of Metrological Devices requires a strong assumption on authentication.
- Standardised ways of achieving such authentication require the use of public key crypto
- In some scenarios it is infeasible to use standard crypto
    - battery powered systems
    - resource constrained components
- Some standards are questionable due to their history
    - NIST secp256 - Snowden revealed doubts regarding engineered backdoors
- Standards are moving to new crypto with more efficiency and security
    - TLS 1.3 goes for Edwards curves

The Brazilian PKI

- Brazil adopts by law a qualified digital certificate scheme for metrology
  - Identities are assured by the ICP-Brasil ecosystem
  - Government identity assurance
  - Strong guarantees similar to eIDAs
- INMETRO is part of the Brazilian PKI as a 1st level CA
- Brazil created a root CA targeted to the use on Metrological Devices
  - ICP-Brasil v6
  - Edwards Elliptic curves
    - Ed448
    - ED25516
- Basis for a series of regulations that will be enforced in the future

The Fuel Pump

- Brazil has an endemic problem of rigged fuel pumps that are tampered with in different levels
- INMETRO is proposing new regulations for using a secure element in these equipment:
    - These will have digital certificates issue by the Brazilian PKI
    - Will user Edwards elliptic curves
        - actually some use Brainpool elliptic curves due to the lack of certified edwards secure elements
- This initiative aims at reducing such fraud using perimeter security
- It is the first calibrated device that will use such tech

What else can we do with such infrastructure?

- One important thing is to be able to track the use of the equipment
  - This impacts on its calibration assurances
  - Helps to detect potential issues the may happen with the equipment
- Identity assurance on devices helps us to track ownership as well as responsibilities
- Maintenance and equipment history is easier to assure
- If we provide the device with connectivity the sky's the limit
  - Sending this data to the cloud helps us to get a bigger picture of potential fraud
  - Organising this data into a blockchain helps us to track the full history of an equipment.

Blockchain of Metrological Devices

- As devices have strong identity assumptions they can be easily identified
- They also have key pairs that can be used to sign blockchain transactions
- Our proposal is to establish a blockchain for metrological devices:
    - To track calibration at first
    - Then to track maintenance
    - And finally track use
- This will increase the reliability of the whole system
- It will also allow for other applications to consume such data for:
    - Statitics gathering
    - Fraud prevention

What he have so far

- A whole “clone” of the Brazilian Metrological PKI
  - With different key pairs obviously
- A hyperledger fabric implementation that deals with Brainpool based identities
- An ESP32 that emulates the Fuel Pump
- A smart contract that receives transactions signed from the ESPs

What we still pna to do

- A full implementation of a BCCSP that deals with Edwards curves
- More smart contracts for the 3 scenarios
- Test of other metrological devices
- Contracts that may integrate with other systems:
  - Revenue and Customs
  - Calibration tracking
- Tests on the wild using a phone app we are developing for INMETRO

Questions?