ICAO SECURITY & FACILITATION

PKI Brazil at ICAO

Gastão Ramos

ITI CEO

Brasília, June 7

ITI Instituto Nacional de Tecnologia da Informação

BRASIL GOVERNO FEDERAL

Who are we?

The National Institute of Information Technology – ITI is a public agency tied with the Civil House responsible for implementing PKI Brazil digital certification policies, auditing and inspecting organizations of National System of Digital Certification. ITI is also the Root Certification Authority.

What's PKI Brazil?

Brazilian Public Key Infrastructure (PKI Brazil) is a set of licensed entities of National System of Digital Certification able to operate in PKI Brazil market. In Brazil was chosen the Root Unique model and the Government is in charge of this.

Our Business

- Digital Certification

- Attribute Certification

-Time Stamp

-Digital Signature

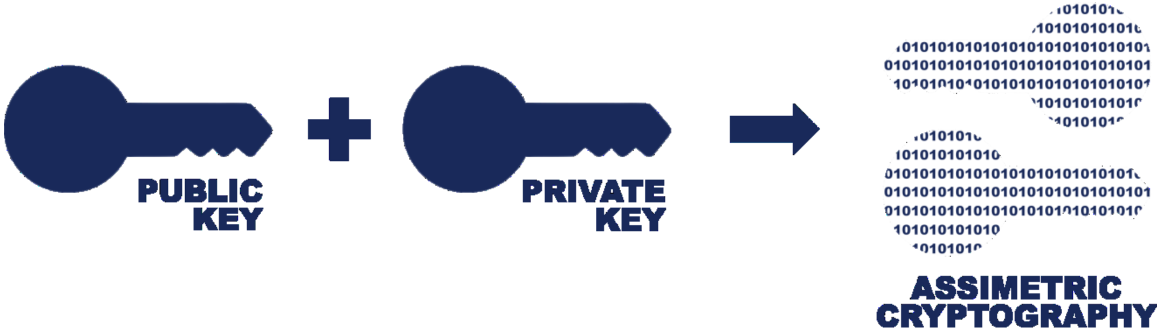
PKI Brazil Size

Nowadays PKI Brazil consists of:

- 16 CAs (first level)
- 83 CAs (second level)
- 10 TSA
- 41 SSP
- 5 BioSP
- 1 TSP

Digital Certification

In Brazil Digital Certificates are destinated for identify people, companies and devices.



PUBLIC KEY

PRIVATE KEY

ASSIMETRIC CRYPTOGRAPHY

Government applications

Important government applications use PKI Brazil certification as a safe mechanism and ID tool.

- Judiciary
- Health Sector
- FGTS
- Eletronic Bill of Sale
- Brazilian Payment System

- Denatran
- IBAMA
- Work Permit
- INPI
- BNDES
- Inmetro
- MEC
- Passport

PKI Brazil and ICAO

For integrating ICAO repository it was needed two important adjustments:

ICAO demands two verification levels (PKI Brazil has three at least)

Validity of the signer certificate that exceeds the validity of the passport (10 years)

Solutions

The Management Committee of PKI-Brazil authorized the creation of the MRE first level CA (self-signed). It's unique at National System of Digital Certification. This heed the ICAO two verification levels demand.

Creation of V4 Chain based in Elliptical Curve Cryptography (Brainpool Standard), approved by ICAO, internationally recognised, commercially viable and safe, 11 years of validity of the certificates provided.

Achievements

With the launching of the new passport Brazil joined to ICAO Public Key Directory.

The action have facilitated the authenticity checks of Brazilian Passport at migration control posts abroad and in Brazil in addition to providing greater security for the Brazilian travellers.

In 2015, the National Institute of Information Technology issued the Certificate of Certification Authority of the Ministry of Foreign Affairs - AC MRE.

Challenges

Creation of a new Elliptical Curve for ICAO submission

Participation as an effective member in the International WG on ICAO Travel Documents

ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters
Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

THANK YOU