



Data Security Solutions



Identity Management: PKI

Roberto Gallo, CEO

Montevideo, UY

2011-11-08

- **Brazilian company**
 - Founded in 2003, Unicamp university spin-off
- **Data security solutions**
- **Regional leader on secure hardware**
 - Sole global dual-core secure processor
 - Sole global PKI-embedded HSM
 - Sole global high performance USB HSM
 - Sole regional certified HSM, with 100% regional development
 - Sole regional commercially available AES chip
- **RNP: strategic partnership for over 6 years**
 - With PKI solutions for RNP's ICP-EDU

- **Among final users, strong academic share:**
 - **ICTs/Universities:** Unicamp, UFF, USP, UFSC, UFV, UFMS, UFMG, FITec, CPqD, CTI/Cenpra...
 - **Government:** Brazilian PKI root CA, Intelligence, MRE, Defense, Army, Electoral Authority, IRS, Justice, ANSP/FAPESP
 - **Private:** CGI.BR, Itaotec, CPFL, Braskem, Lucent, Cambuci S/A (Penalty), RNP, Zetks,
- **KRYPTUS is a consistent supplier of both equipment and technologies for universities, R&D, government, and corporations**

- **Great exchange experience with universities and research centers**
 - Laboratory for Security – LabSec -USFC
 - Laboratory of Applied Cryptography - LCA-IC-Unicamp
 - Laboratory of Computer Networks-LARC / USP
 - Research Center for Communications Security – CEPESC-Abin
 - National Institute for Critical Systems – INCT-SEC
- **We are always open to academic cooperation**
 - Supplying
 - Co-development and licensing
 - Do you have any prototype or idea?

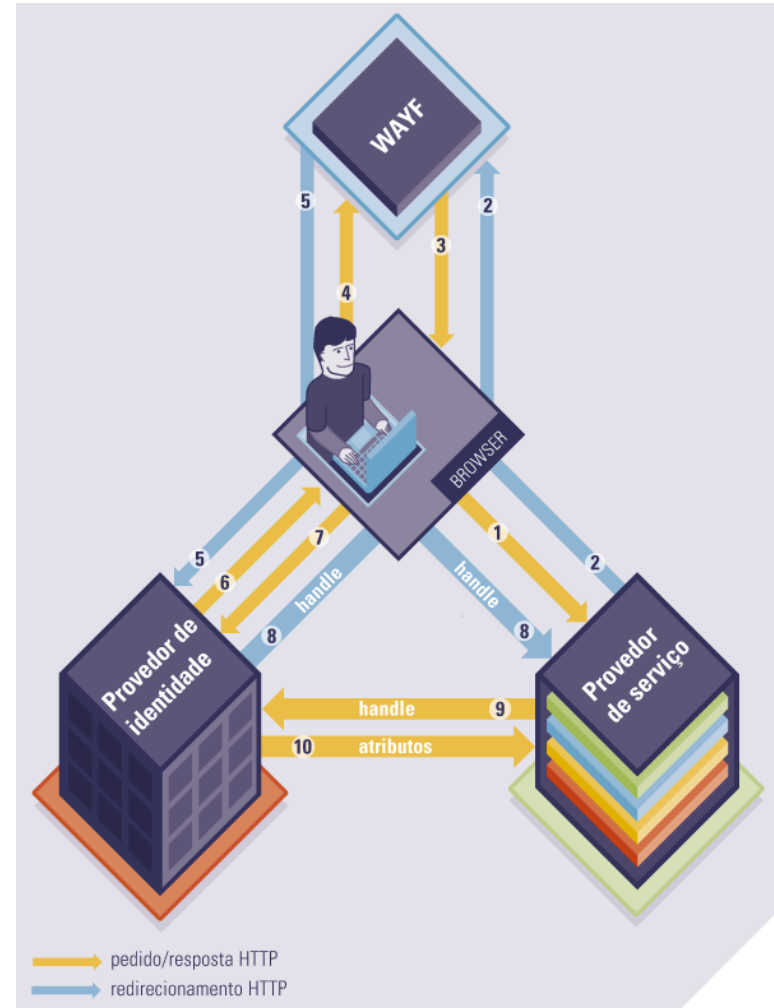
- **ASI-HSM at the root of ICP-Brazil**
 - IRS, Justice, SERPRO, Brazilian Electoral Authority
- **ASI-HSM at every node of RNP's ICP-EDU**
 - Many universities and R&D institutions
 - Digital certificates for everyone (students, staff)
- **Brazilian Voting Machines**
 - Extensive technology improvements
 - Over 200.000 DREs use our technology
 - 65 million voters in a single day
- **Ticketing with Zetks**
 - Over 3.000.000 physical access controls
 - Zetks sells nominal tickets; integrated with payment technologies
- **Public transportation**
 - User tickets control
 - Use, recharge, 10 million tickets per day

PKI as foundation for ID management – collateral gains and challenges

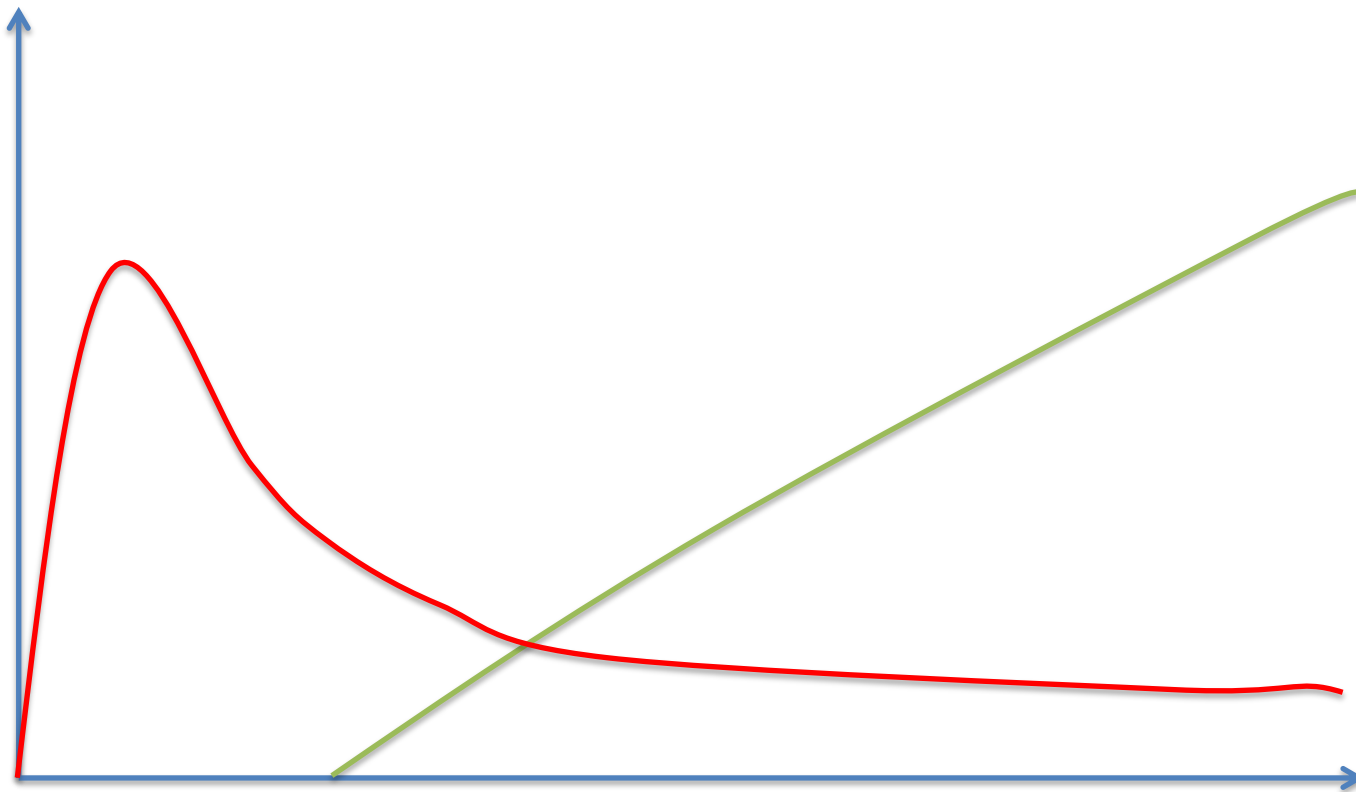
- **Extremely interoperable credential and authentication technology**
 - The facto standard for technological uses
 - IEEE 802.1X, SSL servers everywhere, VPNs, Windows & Linux user authentication, LDAP, VoIP...
 - Legal identification standard in many countries
 - Gov PKI: Brazil, Australia, Iceland, Japan, Saudi Arabia...
- **Strong authentication**
 - Via x509v3 certificates within smartcard or tokens
 - Fingerprint optional
 - Focus on human users and/or devices

- **Proof of origin and data integrity**
 - Via digital signatures
- **Non-repudiation**
 - Via appropriate certification policies and technologies
- **Confidentiality**
 - Especially useful for academic research and buying processes
- **Dematerialization of processes and documents**
 - Improved efficiency, economy and sustainability
- **Access control and frequency**
 - Possible use in distance education (for student tests and exams)
 - Use within federations, allows for secure billing

- **Federations allow for new levels of collaboration**
 - Users from different organizations can consume services from each other
 - Better resource utilization
- **Demands strong user authentication**
- **Highly heterogeneous environment**
 - Necessity to 100% public standards; PKI x509v3
- **Integration with**
 - SAML e Shibboleth



- **Concept is somewhat complex**
 - May be confusing for newcomers. Operation simple
- **Demands an unusual learning curve in technology**
 - Efforts are not proportional to the number of users
 - Mainly setup and procedural operations
- **Gains are perceived on medium term basis**
 - After a few months
- **Expenditures for very small deployments are non-negligible**
 - Although it quickly gets better with more users



How we can help you

Four key points where we help you


- **Reduce technical hassle**
 - Best in class user interface in our solutions
 - Highly integrated, they simply work
- **Ease the learning curve**
 - You don't need to be an specialist to operate the solutions
 - Easy to follow documentation
 - Support from people that know academia
- **Help you with procedural matters**
 - Pre-built ceremonial documentation
 - Usage scripts tailored to academic needs
- **Very competitive costs**
 - Fits the budget of regional academic and R&D organizations
 - Integrated solutions eliminate servers and workload, reduces TCO
 - No export controls – easy to buy







- **Hardware Security Module Solution**
 - Key generation, usage and storage. Perfect for CAs
- **Easiest U.I. in the global market**
 - Yet with the power you need
 - Multi platform
- **Secure: sole peer reviewed HSM**
 - At EuroPKI 2008, Euro PKI 2009, and NIST ID Trust
 - Used by Brazilian Gov root CA and all RNP's CA
- **Very competitive prices**
 - Great discounts for academia and R&D organizations



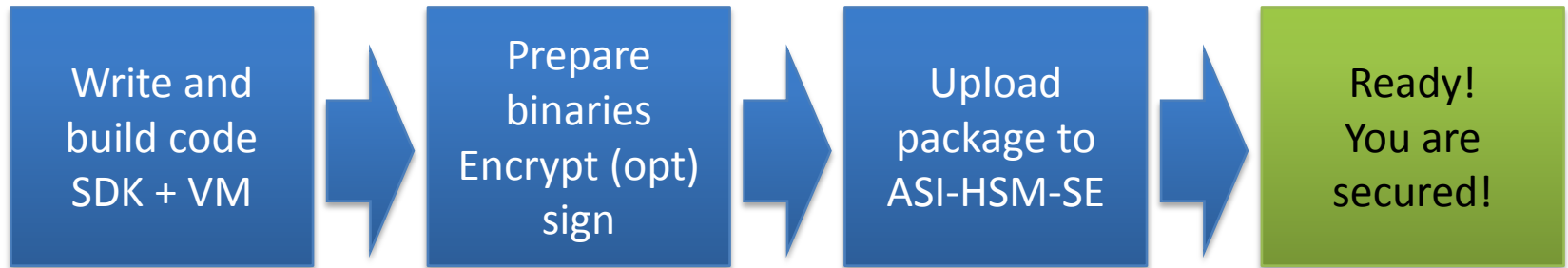
Root CA's

Common Name	Creation Date	Expiration Date	Status	Actions
AC Raiz	Nov 6, 2011 6:21:24 PM	Nov 3, 2021 6:21:24 PM	Active	
1 - 1 of 1 First < Previous Next > Last				

Intermediate CA's

Common Name	Creation Date	Expiration Date	Status	Actions
AC UFSC	Nov 6, 2011 6:22:06 PM	-	Pending	   
1 - 1 of 1 First < Previous Next > Last				

- **ASI PKI in a Box**
 - Fully integrated solution – PKI software (CA) embedded in a single rack device
 - Plug and play, no need to additional servers
 - Minimize configuration
- **Reduced TCO**
 - Required less people to operate
 - Guaranteed migration path
- **Operate remotely**
 - Web-base interface
 - Prevent constant data center accesses



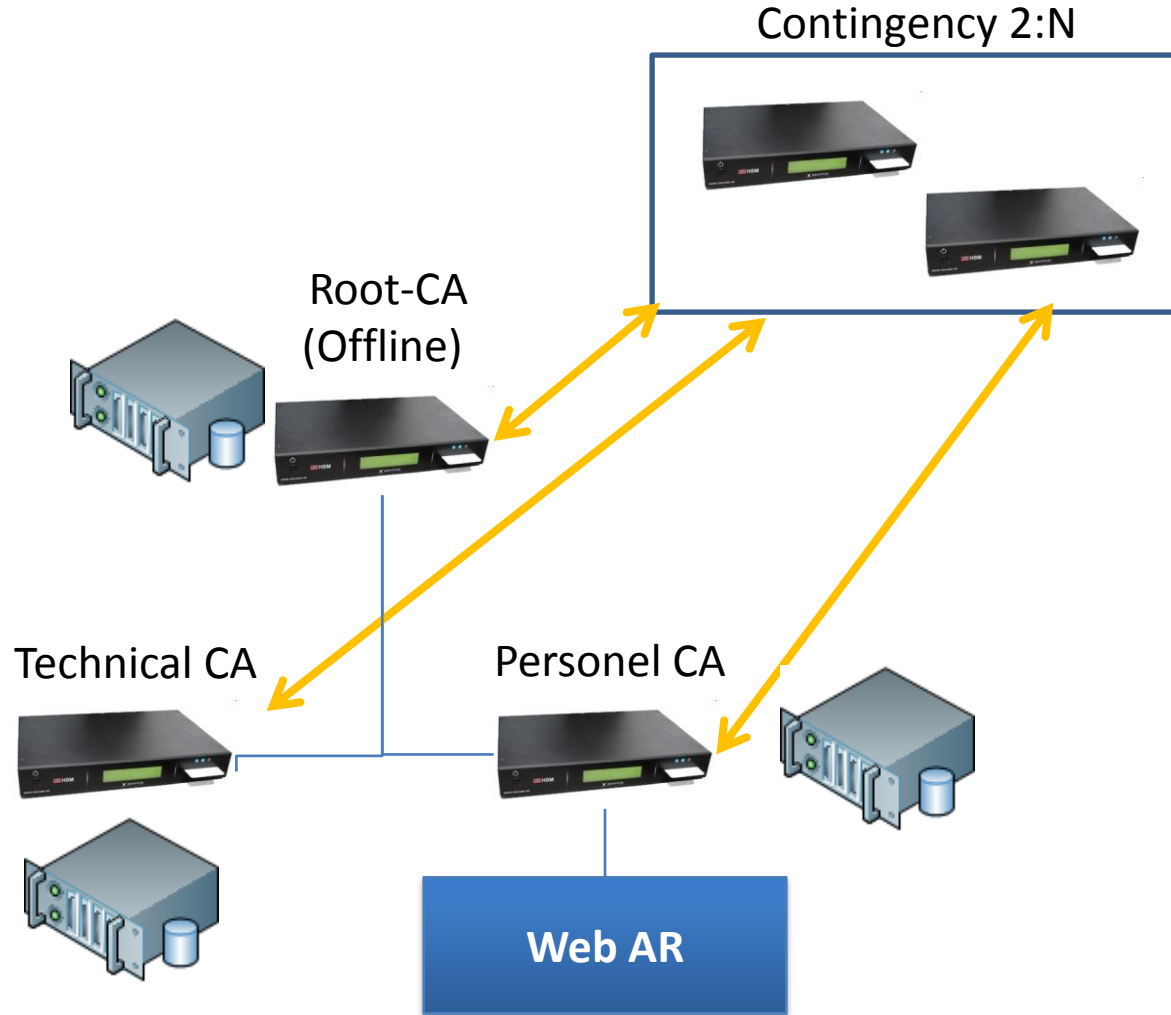
- **ASI-HSM for Secure Code Execution**

- Allows for in-house applications to run inside the secure environment
- Just in four easy steps
- Applications as credit control or proprietary protocols
- First class security
- Full copy protection

- **Great for R&D use**

- Trusted computing is an active research field
- Supporting literature
- Developed applications can be shared securely

Authorities and contingency



- **Crypto**
 - RSA (PKCS # 1 v2.1) - up to 8192 keys bits
 - ECDSA (NIST FIPS PUB 186-3)
 - SHA-1, SHA-256, SHA-512 (NIST FIPS PUB 180-2)
 - X509v3 Certificates
- **Software interfaces (APIs)**
 - OpenSSL, CSP, and PKCS # 11 JCA.
 - All modern Windows, Linux, FreeBSD
- **Real Time Clocks (RTC)**
 - Stability better than 99.9998%
- **Random Number Generator**
 - Hardware based RNG (TRNG)
- **Access Control**
 - User Groups: administrators, auditors and operators
 - Authentication type "k / m", via shared secret in hardware (type Blakely-Shamir) with smartcards
- **System backup**
 - Encrypted PKCS # 7
- **Monitoring and Auditing**
 - Persistent registry of events
 - State of equipment
 - User Access
 - Events of cryptographic keys
- **Proven compatibility with**
 - OpenCA, Newpki, PHP-CA Ywapa/Ywyr and RNP's SGCI
- **Physical and electrical characteristics**
 - 19"1U Standard Rack
 - Power Automatic selection: 100 ~ 240VAC 50/60Hz
 - Interfaces: USB, smart card reader, LCD display, Ethernet
- **Different performance versions**

- **CompactSHM**
 - Entry level HSM
 - High security with low form factor
 - 200 TTS (RSA 1024)
- **Extremely convenient**
 - USB connection allow for hot swap
 - Portability, virtual machine usage
- **Main cryptographic functionalities**
 - RSA 1028 to 4096 bits, ECDSA 512
 - AES, 128, 192, 256 bits
 - True random number generator
- **Very competitive prices**
 - Great discounts for academia and R&D organizations
- **Many uses**
 - Secure VPN with PKI with COTS servers
 - Mass signatures



- **You will never be locked in**
 - Contrary to other vendors, we believe you must have control over your keys
 - All key backup file formats are standard (PKCS#12)
- **You have a different profile usage**
 - We understand the academic and R&D use
 - Reduce the hassle of non-creative activities
 - Reduce the amount of total effort to you start you PKI
- **We believe that if you like, you spread the word**
 - So we try hard to match budget to costs



Thank you

Roberto Gallo
CEO

gallo@kryptus.com

+55-19-3289-4377

+55-19-9167-9080

kryptus.com