

# FreeICP.ORG: Merging PGP & X.509 to get free trusted certs

**Marco "Kiko" Carnut, CISSP <kiko@tempest.com.br>**

Cristiano Lincoln Mattos, CISSP, SSCP <lincoln@tempest.com.br>

Evandro Curvelo Hora, M. Sc. <evandro@tempest.com.br>

Fábio Q. B. da Silva, Ph. D. <fabio@cin.ufpe.br>

*2nd PKI Research Workshop – NIST – April/2003*



## Agenda

- What we wanted to do
- Entry-Level Certificates & CAs
- Virtual Key Signing Parties → Verified Identity CAs
- The FreeICP project

## What we (initially) wanted to do

- Use PKC as stronger auth for some web apps
  - This means X.509 and its huge infrastructure
  - at least in theory **scalable for Musers**
- **Popularize client certs** by
  - Making them **easy, hassle-free to get**
  - Providing them for **free**, but with **decent identity guarantees**
- PGP has had the solution for years: **the web of trust**
- How can we **merge** the PGP WoT and the X.509 hierachy?

## Entry-Level (EL) Certs

- Make client certs as **easy, quick and simple to get** as PGP keypairs
- **Provisory, relatively short lived** (~3 months max)
  - “Just like provisory airline frequent flyer membership cards”
  - Users should expect that they’d have to “upgrade” them soon
- No **identity verification**, immediate issuance
- Compliant apps should treat them as “**guests**”
- An EL CA in **every corner** (or website/webapp/portal)
- EL Certs might provide an alternative to **roaming certs**

## Not-so-Express Certs: Usability

- You've got to install the FreeICP.ORG root cert first
- **Mozilla** proved a good express cert machine
  - Netscape slightly worst
- IE proved to be **an endless source of frustration**
  - XENROLL.DLL upgrades fail in many instances (old systems, restrictive policies)
  - Too easy to have passphraseless private keys
  - Confusing cert selection and management interface
  - ...and lots of other atrocities too numerous to fit in this slide
  - IE-based enrollments failed in >60% of the cases
- Bottom line: **none suitable** for general public use
  - Verisign and RSA know this already: PTA & Keon

## Verified Identity CAs

- VI CA is controlled by the **Trust Manager Web App**
- User enrolls in the TMWA and adds **Real-World IDs**
  - SSN, driver's licenses,... photo, PGP keys
- RWIDs checked either by
  - **robots** performing queries on public websites
  - **veteran users** acting as introducers, like PGP
- TMWA maintains three scores: **credibility, introduction** and **suspicion**
- That is: TWMA promotes the **virtual, web-based key signing party and conflict management**

## Verified Identity (VI) Certs

- Issued by the VI CA/TMWA when the user's credibility **exceeds certain thresholds** or other criteria
- Longer-lived: 6-12 months
- Compliant apps should give them **full privileges**
- VI CA also signs the user's PGP keys
  - PGP is **so much better** at protecting email
  - Act as a **bridge-CA** to make **user communities reinforce each other**
  - Our dab at Jon Callas' **format agnosticism**

## & more! read the paper and...

- Find out how **revocation** is an essential part of all this
- See our first subjective attempt at reasoning why this score system **may be sound**
- Witness your **privacy being respected** by having only nickname & email in the public certificate (just like PGP)
  - But we did find Mike Just's idea quite appealing
- Get a glimpse of **interop pitfalls** and **tough design decisions** we faced
- Gawk at how **incredibly more frustrating** IE proved to be

## The FreeICP Project

- Why Free**ICP**?!
  - FreePKI.ORG was **already taken**...
  - ICP ⇔ PKI in Portuguese...
- Open-source, reusable, embeddable Entry-Level CAs
- Public Verified Identity CA (also open-source)
- **Toolkits** to make easier for developers to add strong client cert based auth
- **Usable apps** (at least one now in alpha: PKI-TWiki)
- Lobby for usable, secure clients
- Find its way into **IPSec**, **IPv6** and **Internet2**
- Community building, etc.

## Subprojects

- The auditable open-source handheld **buried** CA for private key physical security...
- How about moving crypto e security UI **out of the browser**?: the rewriting proxy SSL “Auth Agent” idea
  - Why not merge with PGP and/or GPG?
- Sentinel: **generic reusable RBAC** system with digital cert-based authentication support

# Thank you!

---

## Questions?

contact, just in case: [kiko@tempest.com.br](mailto:kiko@tempest.com.br)

## Volunteers, anyone?

(perl) coders, doc writers, translators, evangelists, etc.,  
badly needed