CACert

A Community-driven Certification Authority

Juanjo Amor

jjamor@opensistemas.com
OpenSistemas

29 Abril 2011

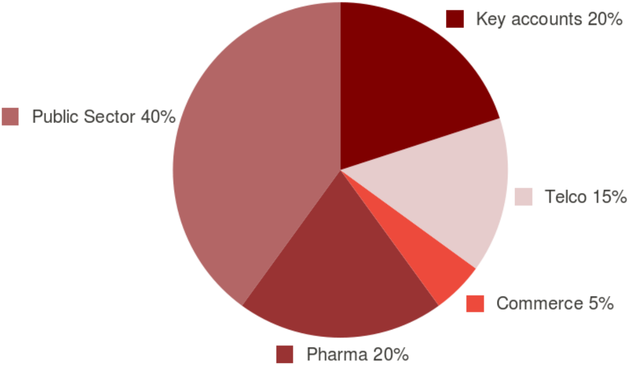
About Opensistemas

Opensistemas is an international company highly specialized in offering global IT solutions based on Open Source and Linux platforms.

About Opensistemas

- Our Vision: To become the international leader in Open Source Technologies.
- Our Mission: Apply our knowledge of the opportunities offered by Open Source to deliver effective solutions and innovation to our customers while promoting the professional development of our employees and building value for shareholders.
- Our Values:
  - Deliver effective solutiosn to our customers.
  - Corporate social responsibility.
  - Commitment to Open Source.
  - Ethics and Respect for individuals.
  - Research and Innovation.
  - Teamwork.
  - Commitment to the development of a society connected by information and knowledge.

About Opensistemas



Our Markets

About Opensistemas

- RedHat
- SGI
- Openbravo
- Typo3
- IBM
- Ingres
- Novell
- Zimbra
- Citrix
- Sybase
- HP

Our Partners

About Opensistemas

Opensistemas is present in nine locations over five countries: Spain (Madrid, Valencia, Barcelona, Sevilla, Zaragoza), Chile (Santiago), Colombia (Bogotá), United Kingdom (London) and China (Shanghai).

About Opensistemas

Contact Information

- www.opensistemas.com
- info@opensistemas.com
- +34 902 107 396

PKI concepts

PKI meaning...

- PKI = Public Key Infrastructure
- *a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates*

PKI components...

- CA = Certification Authority
- RA = Registration Authority
- VA = Validation Authority
- Public keys (person, server and authority certificates)
- Policies and procedures

PKI

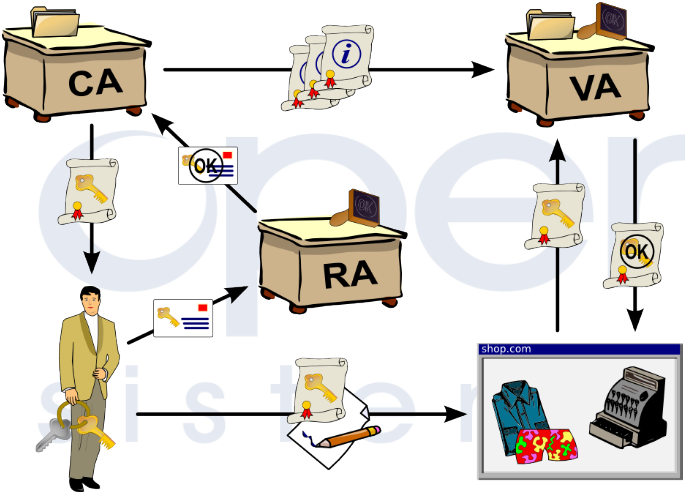


diagram of a public key infrastructure

PKI example 1: Standard CA

Standard CAs such as Thawte, Verisign...

- CA: Joins the CA, RA, VA.
- Our navigator trusts in signed certificates by that CA
- The certificate chain informs browser about VA

Example: Try to get certificate information by using Thawte SSL Ca

PKI example 2: The FNMT CA

Spanish FNMT CA

- CA: Joins CA and VA.
- RA: Delegated to other institutions such as AEAT, city councils...
- CA certificate is not directly recognized by standard browsers so we should import CA certificates into it.
- This is one of first certificates acknowledged for legally identifying people or enterprises in Spain.

Example: Import FNMT certificate and then get its information.

PKI example 3: The DGP CA

Spanish DGP (Police) CA

- CA: At DGP headquarters
- RA: At DGP DNIe offices
- VA: Delegated to third parties (FNMT, for example)
- This is the CA for spanish electronic ID (DNIe). Also acknowledged for legally identifying people.

Example: Import DGP certificate and then get its information.

Web of Trust

Web of trust

- Concept created by PGP creator.
- Instead of having a "central" CA, we can build a trust network of signed public keys.
- If A signs B, and C trust A, then C could trust B.
- CACert uses a variant of trust network...

CACert PKI

What is CACERT?

- A community-driven certificate authority.
- CACERT issues public key certificates to public (server, people) freely.
- Robot CA: Certificates are automatically signed. These certificates are considered weak because CAcert does not emit any information in the certificates other than the domain name or email address (the CommonName field in X.509 certificates).
- Web of trust: Meetings, Assurance points, Prospective Assurers and Assures.
- Assured users can get, for example, email certificates with a complete CommonName field.

CACert inclusion status

Can we use CACert server certificates with some browser?

- Yes, we can import CA certificate and go. . .
- Yes, my Linux distro (Debian, etc) includes CA certificate in ca-certificates package.
- No, my browser does not recognize the certificates and I cannot trust to a strange CA.crt file! (Like a self-signed certificate)
- Although Mozilla started a process to include the certificate, an audit suspended the process, because CACert needed to improve their management system.

CACert web of trust

When you create a new CACert account:

- Only your email can be verified

By meeting other CACert assurers you can get some points:

- for including your real name to your account,
- to generate *better* certificates, and finally,
- to be also a CACert assurer.

CACert web of trust

Some rules:

- An assurer can issue you upto 35 points.
- You need at least 50 points to have your full name assured
  . . . so you need to be assured by, at least, two existing assurers
- With 100 points you can also be an assurer
- . . . but you also need to pass an "assurer challenge"

More rules: When you are promoted to assurer:

- Initially, you can issue 10 points to other people, and get 2 *experience points* when you assure somebody
- After you got 10 experience points, then you can issue 15 points to others . . .
- When you got 50 experience points, then you can issue to others the maximum per session: 35 points
- But in any case, you can, if you want, to issue less points than your maximum

CACert client certificates

A client certificate is used to:

- Identify yourself to a web site
- Email signing
- . . .

When you create a CACert account, you can get client certificates:

- Only the email is certified (by using email-ping)
- With 6 month expiration

When you are assured (50 points) you also get

- Name and email certified
- 24 month expiration

CACert server certificates

A server certificate is used to:

- Secure website: identify a server to you

When you create a CACert account, you can get server certificates:

- With 6 month expiration

When you are assured (50 points) you also get

- 24 month expiration

In all cases, you need to be able to ping DNS name by receiven a postmaster email from DNS owner, and only website DNS name is assured, because CACert assurers are not able verify legal owner.

Questions

Questions?

Exercises

Final exercises

1. Creating your CACert account.
2. Creating your email certificate, with browser and then with openssl
3. Creating a web certificate, with openssl and apache
4. Want to be assured?