CAcert

A Community-Oriented Certificate Authority

Evaldo Gardenali

CAcert, Inc.

VI International Conference of Unix at UNINET

Outline

Digital Certificate

- Binds a cryptographic public key to a user or service
- Carries a digital signature from the issuing Authority
- Limits the authorized uses for the key
- Limits the validity period of the key

Digital Signature

- Source Authenticity Validation
- Binding to a Real-World person or entity
- Integrity of signed data
- Non-Repudiation

Privacy

- Emails are "Digital Postcards"
- In several countries, email and transit providers are allowed to "read" your email, or even required by law to store your emails for 2+ years.
- Encryption can be used to reach acceptable levels of privacy

Cryptography

- Keeps important data safe from intruder's sight
- Can be used for secure communications on insecure media like the Internet
- X.509 and OpenPGP are based on open standards, enabling interoperation.

Certificate Sign On

- Sign-On to services using cryptographic challenges
- Automatic sign-on with loaded credentials
- Multi-way authentication can be established by the use of secure devices
- Passwords are a weak form of authentication

Tokens and SmartCards

- Devices specialized for storage and processing of cryptographic keys
- Built-in random number generation
- On-device signing and decryption to avoid key exposure
- Protection against retrieval of the private keys
- Tamper-reactive ("self-destruct")
- Tamper-evident (Not serviceable)
- Small and Portable
- Generally targeted at individual certificates
- Limited storage capacity (normally from 4KB to 200KB)
- Cost a few tens or hundreds of dollars

Hardware Security Modules

- Enterprise-Class hardware
- Very fast cryptographic processing
- Higher amount of on-board tamper-reactive devices
- Generally Non-portable
- Strict environmental requirements (temperature, pressure, humidity, radiation)
- Fine-Grained Access Control
- Cost a few thousand dollars

X.509 Applications

- Digital signatures and message cryptography
- Secure Services based on SSL/TLS (https)
- Code Signatures (Java, ActiveX, Cellphones)
- Single Sign On
- Virtual Private Networks

CAcert.org

- Issues digital certificates for Free!
- Platform Independent
- Technology Neutral
- Operating since 2002

Why CAcert.org?

- Commercial certificate costs were about USD 200 per certificate per year.
- What does it help being able to afford a commercial certificate if others can't?
- CAcert separates Assurance (identity verification) from certificate issuing.
- Unlimited amount of client and server certificates.
- Organization Certificates available via special Organization Assurance.

Certificate Authority

- Hosted in Secure datacenters
- Source Code is available for audits
- Instant revocation lists and On-Line Certificate Status
- X.509 Certificates
  - Server Certificates
  - Client Certificates
  - Code Signing (Java, ActiveX, Cellphones)
  - IDN Domains
- OpenPGP
  - OpenPGP Key Signatures

CAcert Web of Trust

- Users are assured by checking their identification documents and transferring them Assurance Points.
- Users with enough Assurance Points may assure other users, giving them more Assurance Points.
- To have an "Assured" status, one needs to undergo at least two assurances, minimizing the chance of flaws.
- Assurance forms are retained by the assurer, and might be requested by CAcert Quality Assurance.
- Features restricted to minimum amount of points.

Understanding Assurance Points

Points	Access
0	Unassured. Able to create certificates, name is not included.
1-49	Unassured. Unable to change personal details after being assured.
50-99	Assured. Certificates may include user's name, extended validity. OpenPGP Key Signatures are allowed.
100	Assurer status is granted for up to 10 points. Allowed to apply for Code Signing Certificates.
110	Can assure up to 15 points.
120	Can assure up to 20 points.
130	Can assure up to 25 points.
140	Can assure up to 30 points.
150	Can assure up to 35 points. This is the maximum amount one keeps.
200	Special situations, needs approval from CAcert Board of Directors.

What products ship with CAcert.org root certificates?

- CentOS, the Community ENTerprise Operating System
- Debian GNU/Linux®
- FreeBSD®
- Gentoo Linux®
- Knoppix Linux® Live CD
- Nokia® 770 Internet Tablet

Soon in Mozilla®, grml, Fedora and more!

Statistics

- More than 43000 users
- More than 4000 assurers worldwide
- More than 57000 email addresses secured
- More than 26000 domains secured
- More than 86000 certificates issued

CAcert Incorporated

- Founded in 2003
- Non-Profit Association
- Legally established in NSW, Australia
- Directed by an elected Board of Directors

?

Evaldo Gardenali
evaldo@gardenali.biz

Made with LaTeX2$_\epsilon$