

# A multi-platform tool for digital signature



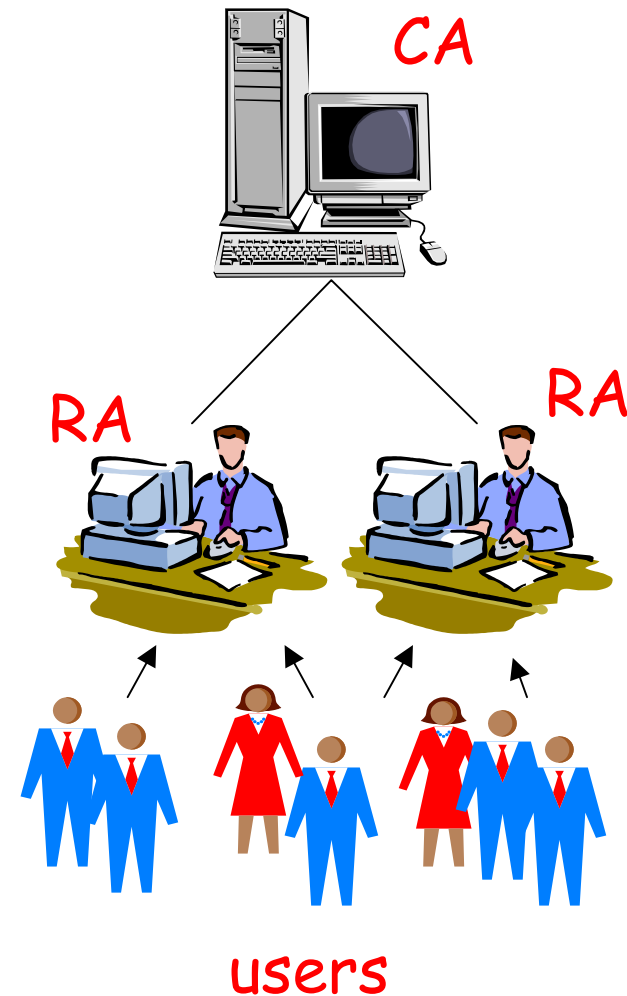
Luca Bechelli

Vincenzo Di Stefano

Davide Fais

# Intro: Public Key Infrastructure (PKI)

- Set of infrastructures, systems and procedures to ensure data integrity and authentication:
  - Certification Authority (CA)
    - PKI key pair generation and self-signed certificate enrolment
    - End-entities Certificates and Certificate Revocation List generation
  - Registration Authority (RA)
    - User recognition and registration
    - User Interaction
  - Certificate Server
    - Certificate and CRL on-line publication



# Digital Signature vs Electronic Signature

## *Electronic Signatures*

•signatures applied to electronic documents with authentication purposes

## *Digital Signatures*

•signatures applied to electronic documents with authentication and **non repudiation purposes**, using technical and procedural constraints, to ensure an high level of security

### *How to apply*

MS Outlook, Netscape Mail, Mozilla and other mail user agent

Mail user agents don't comply with legal constraints for non repudiation

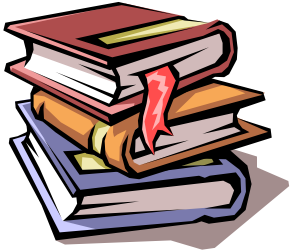
*We need a tool designed at this scope*

# EgoSign

- IIT has developed a tool to allow users to interact with RA and CA services: EgoSign.



- EgoSign is also an API, a software library for the development of encryption-based applications.



- Egosign is an extremely flexible framework right for research environment but also for the distribution as software product

# Design Goals

- Compatibility with many International and Commercial Standards
- Creation and verification of digitally signed documents
- Support for many Hardware Security Modules (HSM)
- Access to certificate server with different protocols
- Use of secure and open source cryptographic software libraries
- Digital signature independence with PKIs
- Platform independence (Windows, Linux, MacOS/X)
- Different PKI integration (OpenCA and some Italian Qualified PKIs)
- Different level of qualification of digital signatures
- Server Side application development

# Features

## Desktop Application

- Hardware Security Modules support

- PKI Interaction (e.g. with **OpenCA**)

- Cryptographic Capabilities

- Operational Protocol Support

- Security Constraints

- Legal and Interoperability constraints

- Digital Signature Standard Support

- I18n Support

## API

- High Level access to client features

- Easy and detailed customization of procedures

- Easy access to smartcard

- API documentation and examples

- Encryption
  - HSM
  - Software

- Low level access to algorithm implementation

- E-voting support

- Attribute Certificate Support

# Egosign-Client in details...

- PKCS#11 interface
- PKCS#12 software credential

- Enrolment Procedure
- URLs, Smartcard File System

- Key Gen
- Verification
- Certificate Validation
- Hash Generation

- LDAP
- HTTP
- HTTPS
- CRL Distribution Point

- Hardware Security Modules support

- PKI Interaction

- Cryptographic Capabilities

- Operational Protocol Support

- Interoperability Constraints

- Security Constraints

- Legal constraints

- Digital Signature Standard Support

- Verification of signed document
- Certificate Validation

- CA Certificate repository
- Validation and Verification

- Enrolment Procedure
- Smartcard Personalization

- PKCS#7
- S/MIME
- CMS
- LDAP
- PKCSs

# Digital Signature Independence & Interoperability

- Independence:
  - users can use many different certificates provided by different CAs
  - different users could use the same application with certificates provided by different CAs
- Interoperability Italian Constraints:
  - all users could verify document signed by others, also if they use different software clients for signature generation
- Interoperability of Egosign:
  - Italian Constraints + Independence

# Different PKI Support

- Web Service based enrolment procedure
- Interoperability support
  - Heuristic to interpret non compatible solutions made by some PKI. Es:
    - Dinamic URL repair and substitution
    - Smartcard facilities
- Easy customization
- CA certificates repository customizable (by users and organizations)
- Support of different PKI and digital signature technologies

# Enrolment Procedure

- Now
  - The client acts as an interpreter of commands to adapt himself at the specified enrolment procedure of the PKI
  - Messages exchanged must be in XML format
  - The client, at the first step, downloads a XML encoded version of Certificate Practice Statement that represents the procedures it has to use to obtain a certificate
- Work in progress:
  - The use of web services will reduce the knowledge base of the client

# Contacts

- For more informations, please contact:

Anna Vaccarelli ([anna.vaccarelli@iit.cnr.it](mailto:anna.vaccarelli@iit.cnr.it))

Institute of Informatics and Telematics  
(IIT- CNR)