



# The italian Electronic Identity Card: overall architecture and first phase of deployment

**Prof. Enrico Nardelli**

NESTOR Lab. – Univ. Roma “Tor Vergata”

# Goals for Electronic Identity Card (CIE)

A tool for the simplification of administrative processes

In-presence identification

Travel document compliant with ICAO and ISO regulations

Secure Access to network services

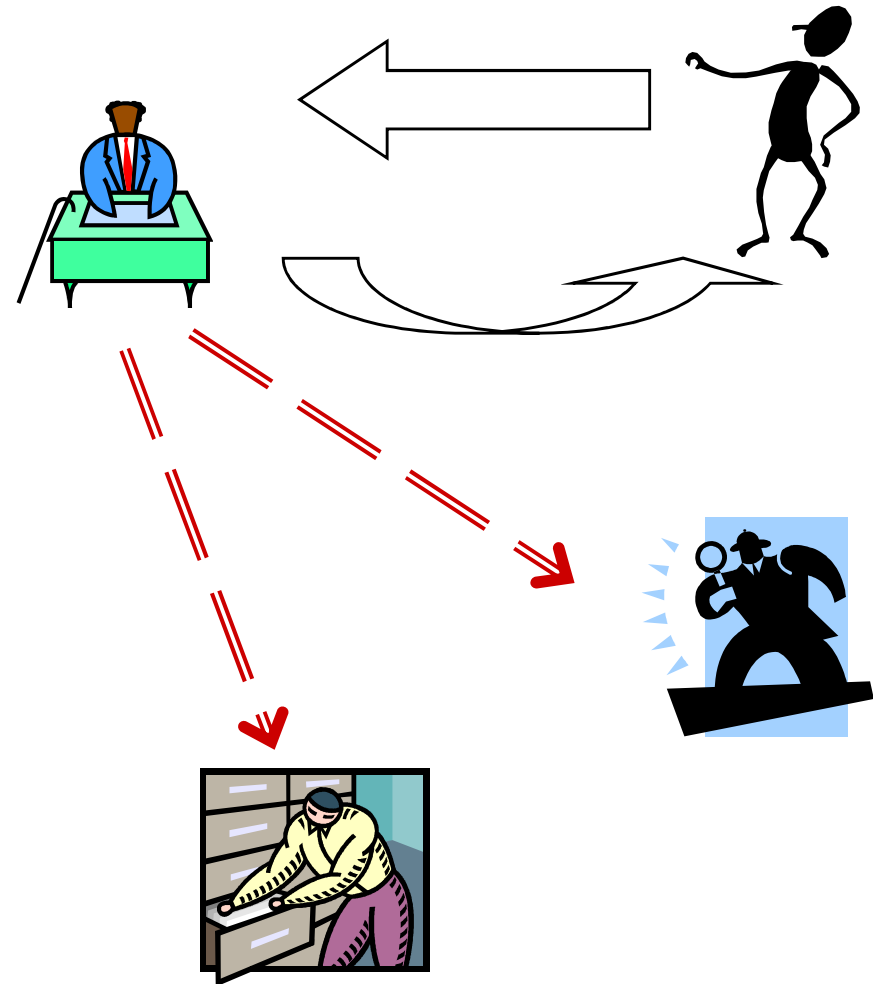
**Citizens Protection**  
**Personal Data Accuracy**  
**Privacy**



# The process of paper-based IC issue

- An older than 15 citizen asks the Identity Card to the Mayor of the residence Municipality, as Government Officer on-site
- The Mayor issues the document, received by State Administration, according to procedures and regulations for security prints
- The Mayor informs local Police Headquarter (*Questura*) of the issued document for Police control activity, by sending a card containing citizen's personal data and photo (plus the fingerprint possibly voluntarily collected)
- The Mayor informs local Ministry of the Interior Office (*Prefettura*), which keeps record of serial numbers of ICs delivered to Municipalities

***The same schema is adopted for electronic IC issue process, with the necessary regulation changes***



# Organizational complexity

- Need of cooperation among all the actors
  - 8102 Municipalities are responsible for at sight issue of both paper-based and electronic identity card
  - 8102 Personal Data Registries interconnected on the Internet
  - 100 Local Ministry of the Interior Offices (*Prefecture* – U.T.G.)
  - 2 Government Commissaries for autonomous Provinces of Bolzano and Trento
  - President of Autonomous Region Valle d'Aosta (acts as the local Ministry of the Interior Officer - *Prefetto*)
  - 103 Local Police Headquarters (*Questure*)
  - 40 millions paper-based IC to be substituted by the electronic ones
- Guarantee the use of EIC as an identification document both at the international and national level
- Guarantee the use of EIC as an international travel document
- Give citizens proper guarantees for the EIC use in accessing network services, also in the perspective of the European Union



# An e-government “grand challenge”

- Transform the traditional process in an electronic one on the Internet, ensuring a smooth transition
- Allow and protect the use of EIC on the Internet
- Open to installation, by national and local bodies, of new e-services for citizens (e.g., electronic signature, identification at the polls, parking payment, ...) without lowering EIC security
- Ensure accuracy and exchange of people personal data among public authorities
- Guarantee security and privacy in people personal data treatment

**Identity theft is the most widespread cybercrime!!**

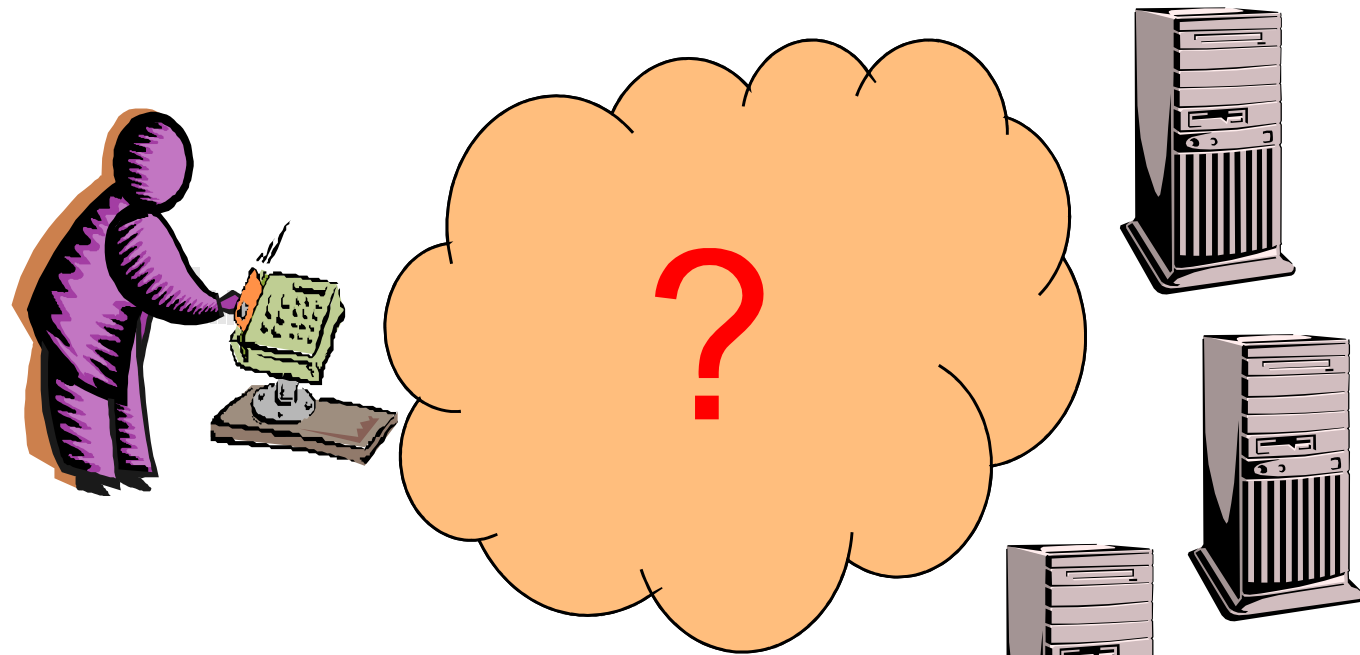


# Leaderships

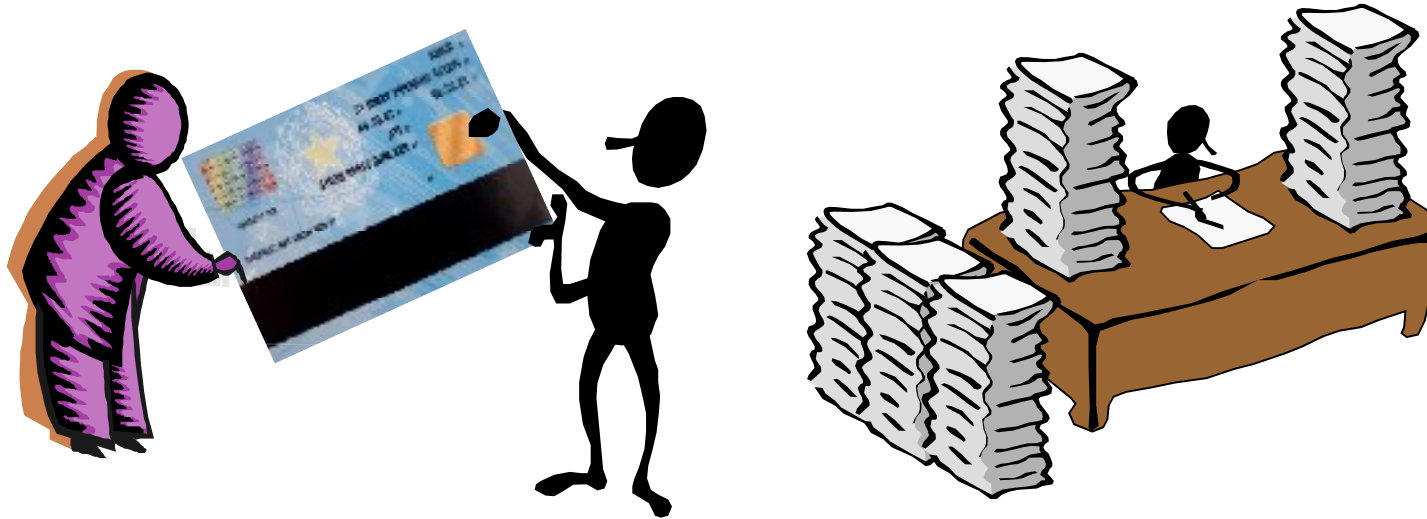
- Overall project coordination and organizational
  - Pref. Mario Ciclosi  
Director Central for Demographic Services of the  
Ministry of Interior
- Scientific and technical
  - Prof. Maurizio Talamo, Univ. Roma “Tor Vergata”



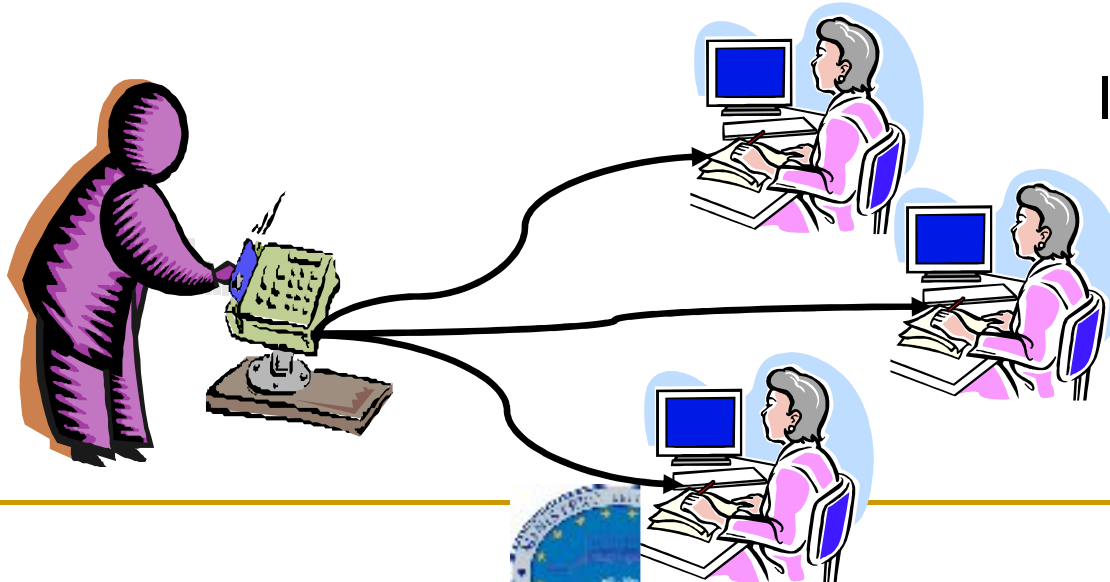
# Which is the technical and organizational complexity to be managed and supported by the IT infrastructure?



# ISSUING: User ↔ Municipality (one to one)



# USAGE: User ↔ Service Providers (one to many)



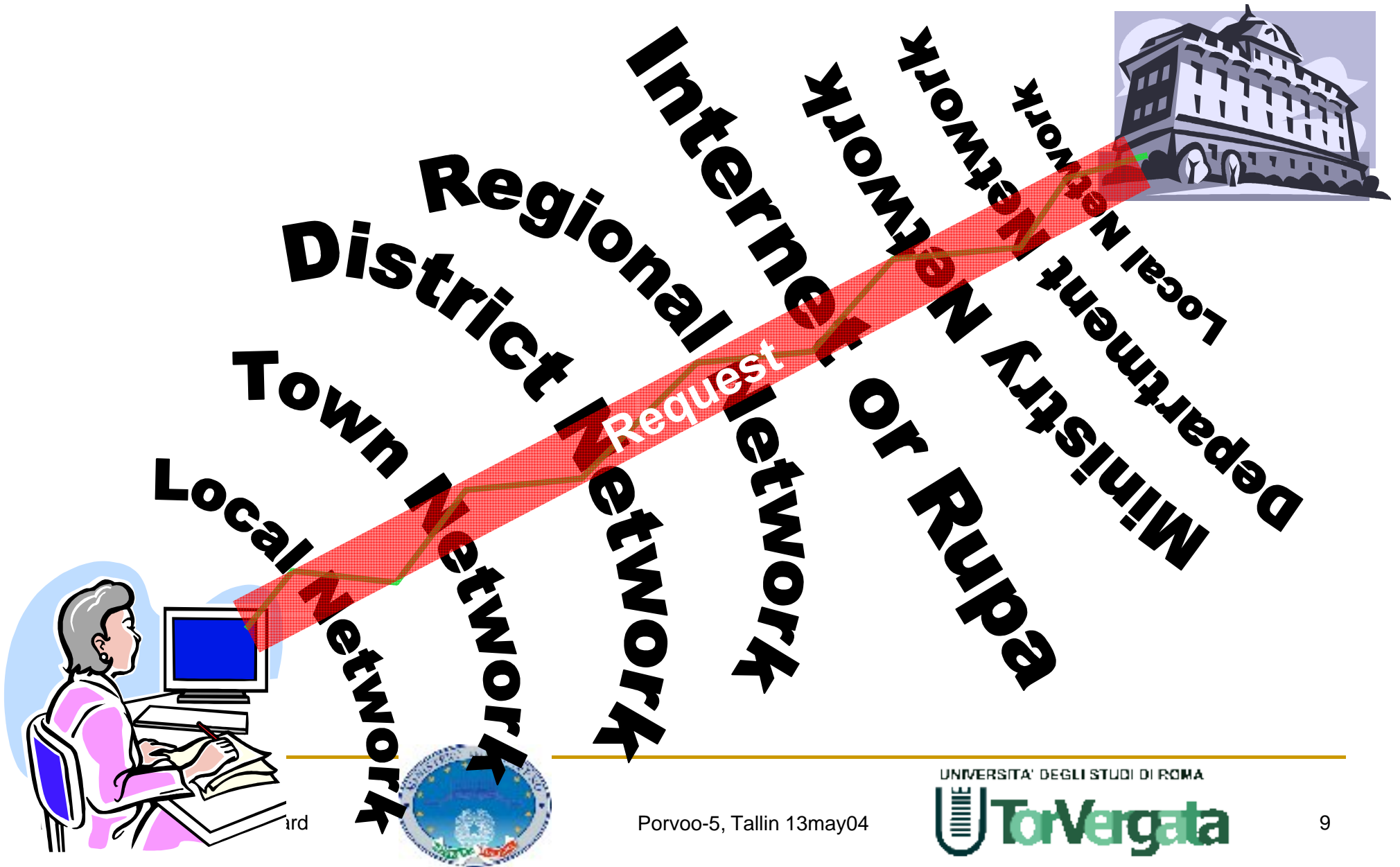
Is the Service Provider reliable?

Are Personal Data still valid?

Has the Card been revoked?



# The REAL path of a *simple* service request



# The core of the problem

- A *simple* service request, before being processed by the service provider:
  - must comply with the security rules of all the organizations along its real communication path
    - Firewalls
    - Intrusion protection software (e.g., antivirus)
    - Proxies
    - Web servers
    - Portals
    - ...
  - even if it has completed its path, must anyhow be checked for compliance with the overall security policy defined for the e-service provision, due to possible “defects” in security all along its real communication path
    - Security policy ill-defined
    - Wrong implementation of the security policy
    - Software bug
    - Trojan
    - Virus
    - Hacker
    - Misconfiguration
    - ...



# Solution ?

- Define a techno-organizational model with the proper combination of organizational structures and technological components
  - Legal, administrative and technical legislations and regulations
  - “Ad hoc” organizational structure (CNSD)
  - Certified Information Technology infrastructure (the **Backbone**)
  - Issue Phase control (SSCE – Security System for the Issue Phase) and validity control (revocation lists)
  - Card Security
    - Cryptographic processor, laser readable optical memory, hologram, typographic details, optically variable inks



# Solution: organizational choices

- Institution of the National Center for Demographic Services (CNSD)
  - Implementation, deployment and management of the IT national infrastructure providing certification and security to network-mediated communication among the actors
  - Deployment in all Municipalities of certified access points to the infrastructure
  - Activation of demographic services
    - National Index to People Personal Data Registries (INA)
    - Personal Data Access and Exchange System
    - Personal Data Registries of Italians living abroad
    - Civil Status Registries



# Solution: organizational choices

- Institution of a National Index to People Personal Data Registries (INA - *Indice Nazionale delle Anagrafi*)
  - “Synthetic” national index containing references to people personal data, updated only by Municipalities through the Backbone, and used as a “junction point” to
    - Distribute updates of personal data coming from Municipalities to all interested Public Bodies
    - Send requests for personal data regarding a specific citizen to the proper Municipality
    - Provide validation of personal data during EIC issue and use



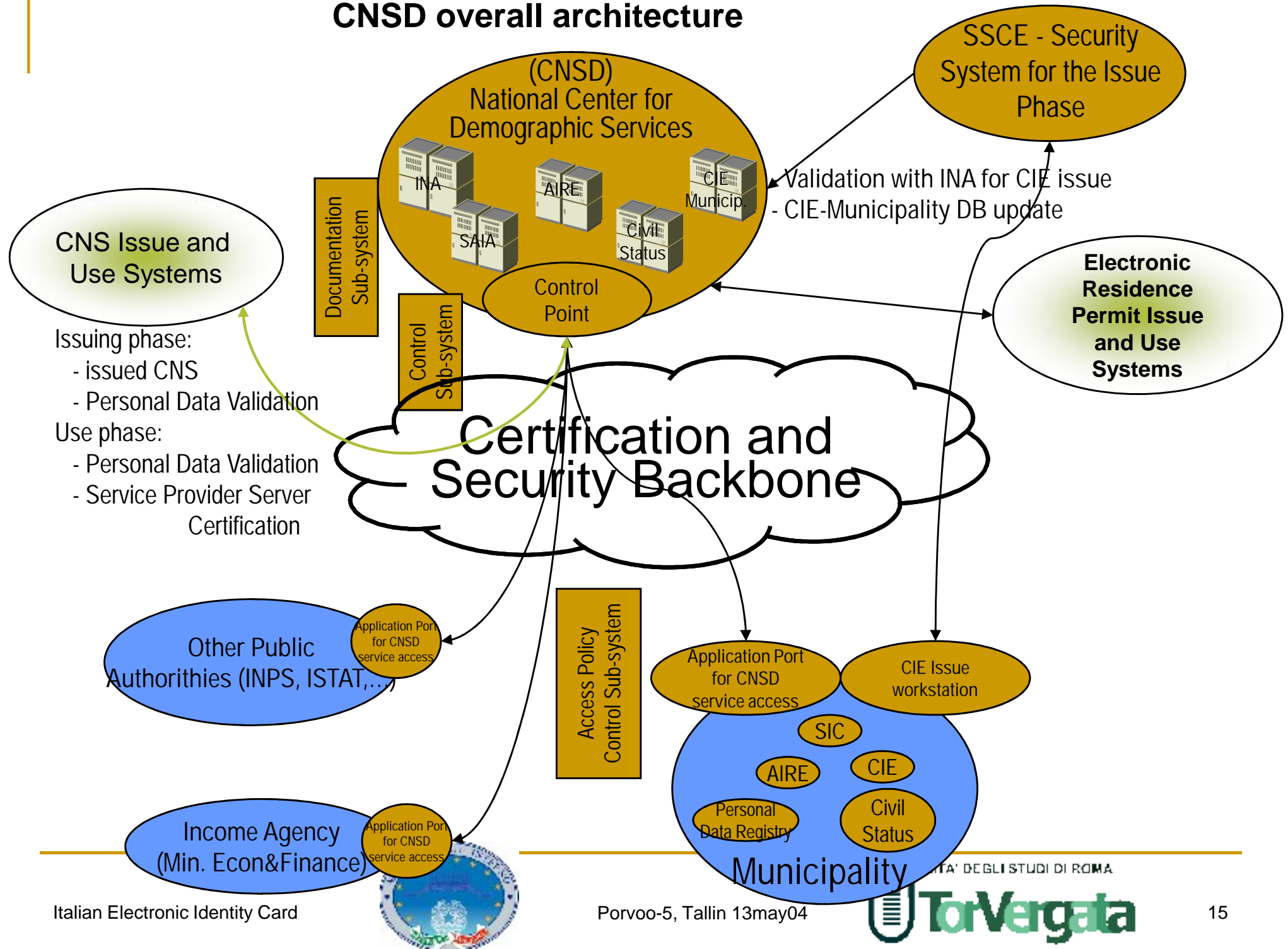
# IT infrastructure: Security and Certification Backbone

***Designed and realized by University of Roma "Tor Vergata"***

- To provide security and quality levels throughout all network systems and devices traversed by communications
- Security and Certification Backbone transparently guarantees as base services:
  - Security of non-intrusion by third parties in communication
  - Impossibility for non authorized machines to access to the service system
- Backbone allows a complete separation between
  - Data needed to identify and authorize users, used by the backbone itself
  - Data needed for a proper access to administrative procedures, used by application software
- PRIVACY is thus fully guaranteed within the service system



# CNSD overall architecture



# Physical support

## Microchip

Secure network authentication

## Optical Memory (Laser Band)

- Large capacity (1,8MB) support provision of many additional services
- Embedded hologram of bearer's photo and personal data supports 'de visu' identification and verification
- Stores unforgeable, permanent and certified traces of all steps and authorizing personnel involved in card issue and updating history

## Physical Aspect

- Bearer's photo and special printing and security features

## ICAO Zone

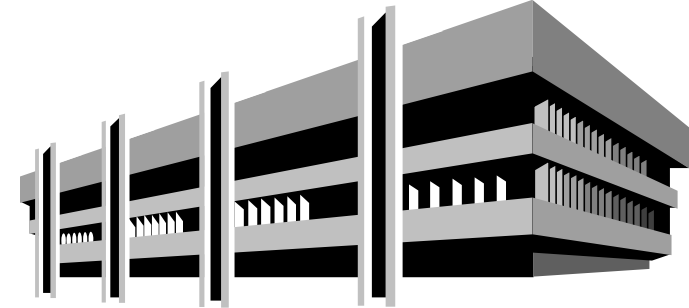
- Allow its use as a travel document



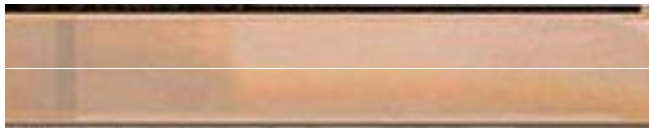
# Physical support production

**Government Printing Office and Mint**  
(IPZS – *Istituto Poligrafico e Zecca dello Stato*)

**Microchip suppliers**



**Optical Memory suppliers**



**Plastic Card Suppliers**



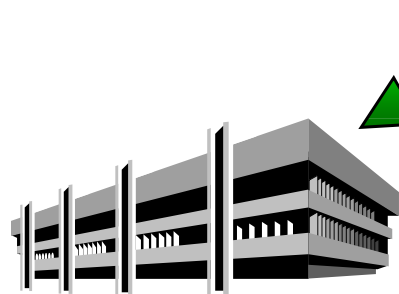
- *Printing of background*
- *Printing of constant elements*



# EIC print and initialization

*Overall electronic control of Ministry of Interior*

Municipality through Ministry of the Interior Local Offices (*Prefettura*) activates EIC print and initialization

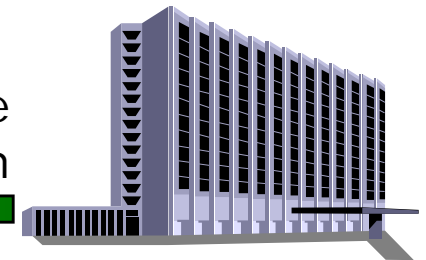


IPZS

- Print name of Municipality and number of the card
- Initialize microchip and optical memory
- Personalization for the exclusive use of Municipality

Request authorization

Release authorization



SSCE

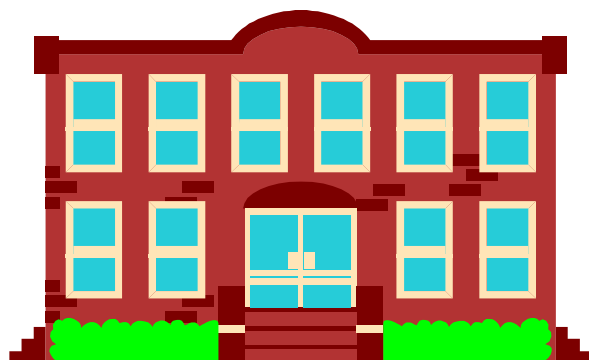


blank initialized CIE

*Delivered to Municipality through Prefettura under the responsibility of Economy and Finance Ministry*



# EIC Issue



**MUNICIPALITY**



- Check citizen identity
- Acquire personal data, photo and fingerprint
- Request card digital certificate
- Write encrypted personal data and certificate on card (microchip and optical memory)
- Complete printing of card
- Update People Personal Data Registry



Encrypted transmission of citizen and card data to SSCE



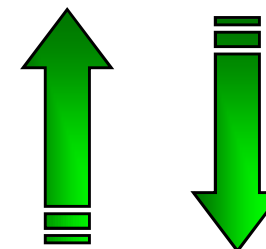
Data and request are validated and card digital certificate is released



Release to citizen  
CIE and PIN



**SSCE**



**CNSD - INA**



# Practical problems for identity document use

- Personal data written on ID documents are static
- People changes
  - City of residence
  - Name
  - Surname
  - Sex ...
- **It is needed to guarantee a continuous process of alignment, update and control of people personal data to ensure a correct use of EIC**



# Solutions: technical choices

- The digital certificate on the EIC, which is used by WEB servers to provide access to network services

## **DOES NOT CONTAIN PERSONAL DATA**

- WEB servers can ask directly to INA, through Backbone validation services, the Fiscal Code associated to a EIC id-number of a citizen, and use it to possibly ask his/her personal data to the competent Registry.

## **Citizen protection**



# Solutions: biometric data choices

- According to current privacy legislation, the citizen's fingerprint *template* (produced using an algorithm provided by the Ministry of the Interior) is stored into EIC only (both in microchip and optical memory) and does not allow fingerprint reconstruction
- Memory space storing the *template* is undeletable and not re-writable
- During police controls or network service access, stored *template* is compared directly to the fingerprint taken on-demand to citizen, whose physical presence is thus necessary. Hence there is no database of fingerprints.
- Such a model is flexible and can be changed if legislation will change

## Citizen protection



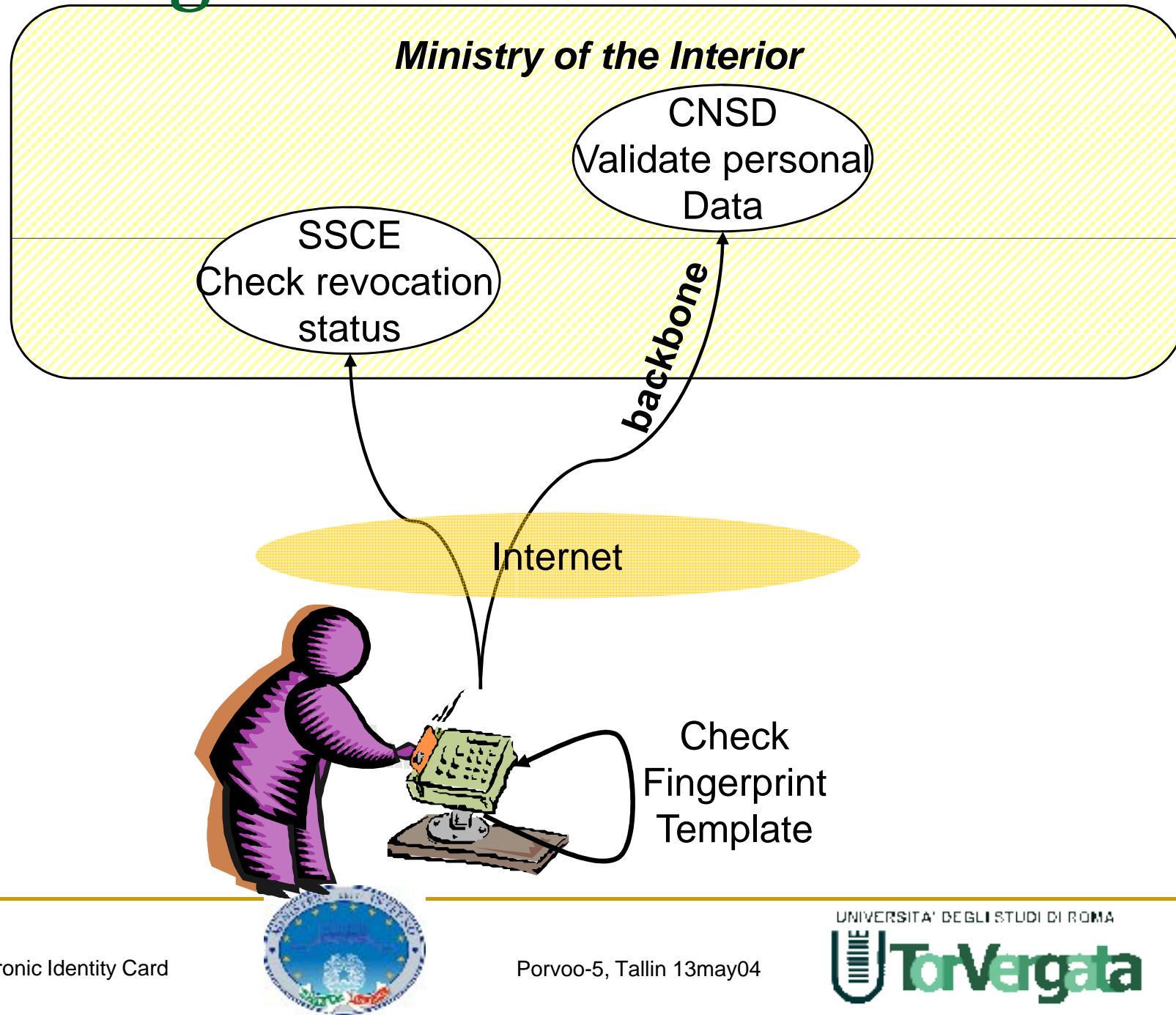
# EIC issue

*The whole process is secured, traced and audited*

- IPZS assembles and initializes the card (ID-number)
- Municipality
  - Receives initialized cards
  - Checks citizen identity
  - Acquires citizen's personal and biometric data
  - Validates personal data with Interior Ministry (CNSD-INA)
  - Activates on-chip generation of public-private keys
  - Receive by Interior Ministry (SSCE) the digital certificate binding public key and card's ID-number
- Citizen receives EIC and the secret PIN



# EIC usage model



# EIC usage to access network service

- Standard mechanism for network identification through a WEB browser
- Reading of digital certificate on the EIC
- Check with SSCE (blacklists) the EIC revocation status
- Ask PIN so as to check for the physical presence of EIC (*challenge*)
- Query the Interior Ministry (CNSD-INA) for citizen Fiscal Code in order to possibly get citizen's personal data from the competent Registry
  
- Possibility of checking biometric data for further securization of the access
- Electronic signature services (additional)



# National Services

## Running

- Check age of person when taking cigarettes at automatic distribution machines
- Person identification at the polls
- Citizen check of his/her fiscal position
- Access to SIM (Mountain Information System)

## In preparation

- Civil complaint filing and status control
- Criminal complaint filing and status control
- Payment of social charges for house servants
- Income tax return payment
- ... Others ...



# Local services

## Running

- Payment of Waste Collection Tax (TARSU)
- Children school enrolment and school fees payment
- City Residence and Street Residence change
- Payment of fines

## In preparation

- Enrolment to local sport centers
- Booking of hospital admissions, medical visits, medical tests
- Welfare requests filing (social support checks, scholarships, ...)
- House Local Tax (ICI) variations and payment
- Economical support to disadvantaged people (elders, orphans, ...)
- ... Others ...



# CNSD service system: state of deployment

- Connected and registered on the Backbone
  - ❑ 7600 Municipalities (out of 8102)
  - ❑ 380 access points in 200 consulates
  - ❑ Income Agency (Ministry of Economy and Finance)
  - ❑ Foreign Affairs Ministry
  - ❑ State Coastal Lands Agency
- AIRE – Public Registries of Italian Citizens living abroad
  - ❑ 7600 Municipalities regularly send data to the central AIRE office
  - ❑ Foreign Affairs Ministry and all 200 first category italian consulates in the world
- INA
  - ❑ 25.000.000 citizens already inserted
  - ❑ The whole population of the 1500 Municipalities has been inserted



# Status of implementation

- First on-the-field trial phase (completed)
  - 83 municipalities involved in the trial
  - 170.000 EICs produced
  - 100.000 EICs released to citizens
  - Design, realization, and validation of information technology infrastructure and security system for the issue phase
- Consolidation and rationalization phase (running in 2004)
  - 56 municipalities involved
  - EIC issue to all citizens older than 15
  - 2.000.000 EICs under production
  - 600.000 EICs already produced and distributed to Municipalities
  - Issue to citizens is an ongoing accelerating process, running in parallel in the 56 Municipalities
  - Access infrastructure for personal data and demographic services already available and working in more than 7500 municipalities
  - Personal data validation services infrastructure already available and working through the Internet
- Third phase
  - EIC issue in all Italian Municipalities (2005-2009)



# More detailed presentations ...

... are available on the site of our laboratory

- <http://www.nestor.uniroma2.it/italianEIC>

Official information is available at

- <http://www.servizidemografici.interno.it>

