## CINECA and university elections in Italy

*CINECA* is an Inter-University Consortium of **36 Italian Universities**.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every 4 month</td>
<td>The Ministry of University and Research nationwide elects the <strong>comparative commissions</strong> that assign places to professors and researchers at University.</td>
</tr>
<tr>
<td>About every 2 years</td>
<td>Universities elect their <strong>administrative organs</strong> (chancellor, academic senate, and so.)</td>
</tr>
<tr>
<td>Several times a year</td>
<td>Universities call <strong>non academic elections</strong> (scientific commissions and so)</td>
</tr>
</tbody>
</table>

Since 1998 up to now, **CINECA uses a poll site e-voting system** for these elections and others:

- **About 60 university and non election events**
- **15,000 – 40,000 voters and 100,000 – 200,000 cast ballots a event**
- **About 100 poll sites in 75 Italian Universities**
in 2005 CINECA e-voting team begun to develop a new voting system release

**u-Vote**

*Designed to support additional voting channels*

Until now, u-Vote has been used for three pilot elections

Designed in compliant with the *Legal, operational and technical standards for e-voting*, adopted by the Council of Europe

Currently it **is being certified** by the Italian Ministry of University and Research

---

**Poll Site Voting Channel**

- Voting equipment
  - placed in a **public environment** called poll site
  - placed in a **physical environment** **supervised** by election officials
  - provided by the voting system supplier
  - its security and integrity are assured by official control procedures
  - connected only to protected networks (VPN channels)

- **Voter’s privacy protection**
- **Protection against software/hardware tampering**

A voter can cast the vote only in the poll site assigned to him or in a poll site of his choice
Kiosk Voting Channel

- Voting equipment not provided by the voting system supplier
- Its security and integrity are not assured by any official control procedure, but they are reasonably protected against malware
- Connected both to protected and unprotected networks – connections to central server are authenticated and secure (VPN channels)

A voter can cast the vote in a kiosk assigned to him or in a kiosk of his choice

Voting machine are usually multi purpose pc - Cheaper and more convenient than poll site voting channel, but less secure

Remote Internet Voting Channel

- Voting equipment not provided by the voting system supplier
- Its security and integrity are not assured by any official control procedure, and it may be unprotected against malwares
- Connected both to protected and unprotected networks – connections to central server are authenticated and secure (SSL channels)

A voter can cast the vote in a place of his choice

A voter can vote from home or office - Cheap and very convenient, but not secure
u-Vote cryptosystem

Voting protocols are usually based on

blind signatures schemes  against not providing universal verifiability
for requiring a simple architecture and few steps to complete the voting phase
homomorphic encryption and verifiable mixes  for providing universal verifiability
for requiring a complex architecture and a lot of steps to complete the voting phase

u-Vote protocol is based on

blind signatures schemes  against one-more forgery if the hash function is poorly implemented
unforgeability

RSA Blind signature scheme with PSS encoding method

Simplified system model

Central Election Office (CEO)  distributes ballots to the eligible voters
signs the voters blinded ballots

Central Ballot Box (CBB)  collects the encrypted ballots
makes ballots available for the counting process

Counter (C)  Decrypts the ballots by a smartcard
Counts the votes

Audit System  Provides recording, monitoring and the ability to cross-check and to verify the correct operations of the e-voting system
**Voter’s authentication**

Authentication with personal smartcard
Available in both poll site, kiosk and remote internet voting channels

Authentication with username and password

Authentication with poll site smartcard
Available only in poll site voting channel

- **Voter 1** Signature 1
- **Voter 2** Signature 2
- ... ...
- **Voter n** Signature n

*Before voting, election official associates the voter’s identity to the poll site smartcard*

*If voter uses a smartcard, CEO collects the voter’s digital signature*

**Voting phase (1)**

1. **Voter**
   - Encrypt the voted ballot with Counter’s public key
   - Apply the blinding function to the encrypted ballot
   - Send the blinded encrypted ballot (and the voter’s signature)

2. **CEO**
   - Sign the blinded encrypted ballot
   - Randomly chose a validation number and associate it to voter’s identity
   - Send the validation number

3. **CBB**
   - Obtain the signed encrypted vote from its blinded form
   - Send the validation number and the signed blinded ballot
   - Store the validation number
Voting phase (2)

CEO
- Sign the blinded encrypted ballot

Voter
- Send the signed encrypted ballot together with the validation number
- Mark the voter corresponding to the validation number has voted

CBB
- Verify the signature on the ballot
- Check if the validation number is in the store and delete it
- Send the validation number
- Collect the encrypted ballot
- Confirm successful voting

Voting phase (3)

CEO
- Voter 1 Signature 1
- Voter 2 Signature 2
- ...
- Voter n Signature n

Audit System
- Validate the voter’s signatures
- Validate the signature on each ballot
- Look for duplicate entries

CBB
- Signed encrypted ballot 1
- Signed encrypted ballot 2
- Signed encrypted ballot n

If CEO and CBB are assumed to not collude, it’s ideally sure that

n eligible voters have voted  n authentic ballots have been cast

CEO and CBB collusion and software/hardware tampering are detectable only through paper audit trails
### Counting phase

- **CBB**
  - Signed encrypted ballot 1
  - Signed encrypted ballot 2
  - ...
  - Signed encrypted ballot n

- **Counter**
  - Verify the signature on each ballot
  - Decrypt each ballot
  - Count each vote
  - Public election results

- **Audit system**
  - Check the votes have been well counted

### Voting channel vulnerabilities

- **Assuming that CBB and CEO don't collude, Poll Site Voting channel is reasonably secure**
- **Remote Internet Voting Channels has unsolvable vulnerabilities**
  - DoS attacks
  - Voter can prove accidentally or deliberately for whom he has voted
  - Voting station tampering

- **Kiosk voting channel helps to mitigate the vulnerabilities by**
  - Control on the physical environment
  - VPN
  - It's not completely secure
  - changes in elections process should be presented as an **evolution and not a revolution**

  technical innovations in internet communication and in operating systems are necessary, before especially remote Internet voting can be widely implemented
Conclusions

What are the contexts in which u-Vote may provide Kiosk and Remote Internet Voting channels, granting an acceptable level of privacy and accuracy?

A voting channel is suitable for a particular election, if it’s invulnerable to any feasible attack. There is at least an attacker that has enough resources and is probably interested in executing it.

The feasibility of an attack depends strictly on the election importance and on the environment in which the voting system is used.

CINECA suggests:
- Poll site voting channel for comparative and administrative elections
- Poll site, kiosk and remote internet voting channel for non-administrative elections