

The Italian academic community's electronic voting system

Pierluigi Bonetti, Stefano Ravaoli, Simone Piergallini
{bonetti,ravaoli,piergallini}@cineca.it

CINECA
Inter University Supercomputing Center
Via Magnanelli 6/3 - Casalecchio di Reno – Bologna - Italy

Abstract

A new Italian law regarding the recruitment of university researchers and teaching staff provides for election on a national basis of the members of the selection committees. In order to handle such a process, an electronic voting system has been developed which offers the necessary guarantees in terms of legitimacy, security, anonymity and secrecy both in the voting process and in the scrutiny. The system presented, based on standard cryptographic algorithms, is the one in use by all the Italian university since June 1999.

Keywords

Electronic voting system, Italian universities, cryptography, smartcard

1 Introduction

The Italian law of the 3rd of July 1998 n. 210 modifies the previous recruitment system for tenured university researchers and teaching staff, providing for the creation of an election committee for each post offered. The members of each committee, with the exception of one person designated by the university publishing the competitive public examination, have to be elected from amongst all the teaching staff belonging to the scientific discipline relating to the post offered. Each competitive public examination, therefore, requires a nationally based election. If thousands of competitive public examinations are published by the universities taken as a whole, it becomes necessary to handle thousands of elections contemporaneously, with thousands of ballot-boxes in each polling station.

The scrutiny of the votes is the responsibility of the university which has published the competitive public examination, consequently the votes have to be sent from the polling station to the place where the scrutiny will take place.

The active and passive electorate, that is the set of electors and candidates for each public examination, depend on the academic position of the elector (Researcher, Associate Professor or Full Professor) and his field, the post offered and the field it pertains to, as well as the position of the designated member.

The complexity of the process means a traditional approach based on manual scrutiny and paper ballots is no longer feasible.

2 The electronic voting system

The management of a complex process such as the one resulting from the change in the law entails adopting an electronic system able to improve on the traditional methods previously used to nominate selection committees for candidates, whilst ensuring that these are based on the preferences expressed by the national teaching body with a voting procedure guaranteeing anonymity and secrecy.

The following is a description of the system which has been set up and which is at present being used by all Italian universities.

2.1 General features of the system

The design of the system satisfies the following requirements:

- ✓ it guarantees that it is not possible to trace the vote back to each individual voter, that it is not possible to alter the votes, and that it is not possible to know the results while the polling stations remain open;
- ✓ it enables the voters to vote at their polling station, as well as at any university in Italy;
- ✓ it handles the high number of possible elections (there are 415 disciplines, 3 professional qualifications, and 73 universities);
- ✓ it handles the high number of electors and candidates;
- ✓ it enables the voters to be physically identified by an official present in the polling station at the moment of voting;
- ✓ the lists of electors cannot be modified and can be consulted on the Internet with certification attesting to the source. The proceedings are published with the same guarantees as to their authenticity;
- ✓ the ballot-box can only be opened at the end of the voting process and only by the person responsible for the procedural administration;
- ✓ the system uses a Public Key Infrastructure and cryptographic algorithms conforming to international standards (see Section 5).

2.2 Organizational aspects: preliminary operations

The voting takes place at a polling station, where there is an election committee composed of at least three people, one of whom acts as president.

A few days before the beginning of the voting session, the president of the polling station is given a set of personal “electoral certificates”, one for each voter registered at that polling station. An “electoral certificate” consists of a sealed envelope containing a personal code and an identification key for the voter.

The president of the polling station is also given, a single time, a smartcard for each voting terminal. The smartcard’s functions and characteristics will be described in section 5.3.

2.3 The identification of the voters

Ascertaining the identity of the voters is carried out under the responsibility of the president of the polling station, reference being made to normal identity documents accompanied by a photograph. The identified voter is then given the sealed personal electoral certificate, with which he can access the voting terminal. The certificate is only valid for the voting session for which it has been issued.

The voter who knows beforehand that he will be away during the election period can go to the Electoral Office of his university before the starting date and ask for the electoral certificate, so as to be able to take it with him and use it to vote in a different polling station.

2.4 The voting process

The sequence underlying the voting process is illustrated in Figure 1.

The voter goes to the voting terminal, opens his electoral certificate and types in the identification codes giving him access to the system.

The interface, at this point, presents a list of the elections in which the voter can vote and asks in the case of each one whether the person wishes to vote or not.

If the voter decides to vote, he obtains a list of the candidates and is given the possibility to express his preference. After a request to confirm the choice made, the vote is encrypted and sent to the Central Ballot-Box, which, in turn, acknowledges the receipt. Having been sent, the vote can no longer be modified or revoked.

If the voter has the right to vote in more than one election, he can at this point proceed to the next one.

Even though each vote is sent immediately to the Central Ballot-Box, it is not possible, for security reasons, to interrupt the voting process and come back at a later time.

When the voter has finished, the polling station's printer prints a record indicating the date, time, terminal number, the voter's surname and first name, and the declaration "has voted".

In the case of technical problems, such as a terminal or network crash, it is possible to repeat the process until the vote correctly reaches the Central Ballot-Box.

As in the case of traditional elections, it is possible to vote without expressing a preference by selecting the option "blank ballot".

The functioning of the voting terminal is dependent on the presence of the smartcard in the reader, which is inserted by the president of the polling station at the start of the voting session. Each insertion and removal of the smartcard is indicated on the record produced by the polling station's printer.

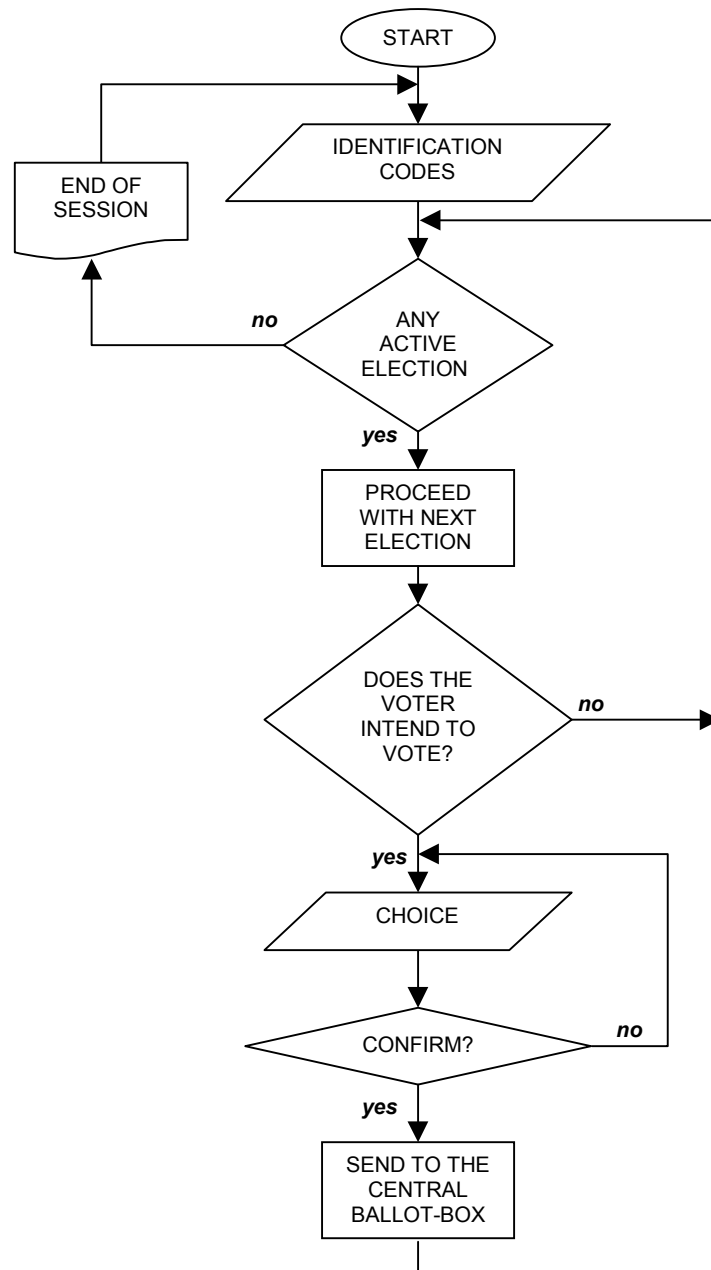


Figure 1: The voting process

2.5 The scrutiny process

The scrutiny of the votes pertaining to an election can only be carried out by the person responsible for the recruiting, nominated by the university which has published the competitive public examination, and can only take place after the closure of the voting procedures.

Each person responsible has a personal smartcard containing a private key to decode the votes which have been encrypted with his public key.

Any of the voting terminals can be used to carry out the scrutiny. The person responsible inserts his own smartcard into the reader and types in the PIN. The terminal acquires the encrypted votes from the Central Ballot-Box after having checked with the Central

Electoral Office that the election has ended. The smartcard decodes the votes and the results are visualised and printed. A copy of the results, signed by a second private key in the smartcard itself, is also sent to the Central Electoral Office for publication.

3 Architecture

The fundamental components of the electronic voting system are:

- ✓ The Public Key Certification Authority (CA);
- ✓ The Central Electoral Office (CEO);
- ✓ The Central Ballot-Box (CBB);
- ✓ The polling stations;
- ✓ The communications network.

One of the features characterizing the architecture is the presence of two central servers, the CEO and the CBB, which are physically separate and run by different administrative bodies, and which enable separating the voter's identity from the votes cast. A similar architecture is also described by [6] and [7]. The version we are presenting introduces some variants making it possible to invalidate any potential collusion between the administrators of the CEO and CBB. What is lost, regarding the algorithms proposed by the above-mentioned authors, is the possibility of an a posteriori check on the part of the voter as to whether his vote has been counted in the result of the scrutiny. The lack of a such a possibility, however, is not contrary to a voter's expectations, seeing that it has never been possible in any traditional type of election.

3.1 The Public Key Certification Authority

The Certification Authority (CA) constitutes the basic infrastructure enabling the identification of two types of entities:

1. the Recruitment Procedure Officers (RPO) at the universities;
2. the voting terminals.

The Ministry for Universities and Scientific and Technological Research, in its role as guarantor of fair play in the electoral procedures and under appointment by the Association of Italian University Rectors, is responsible for producing a smartcard for each of the above entities, containing a pair of 1024 bit RSA keys. The CA's task is to certify the association between the public key and the entity possessing it. The certification takes place by creating a certificate in X.509v3 [1] format, which is signed by the CA and loaded onto the smartcard. The certificate contains the following information:

- ✓ The identifying data of the entity owning the key
- ✓ The public key
- ✓ The identifying data of the CA which signs
- ✓ The period of validity of the certificate
- ✓ The CA's signature

Among the functions of the CA is also the administering of the Certificate Revocation Lists (CRL), so as to be able to annul a certificate before its natural expiry date, should the need arise.

The CA operates in an off-line mode without being connected to a network and intervenes in the electronic voting process only to emit the certificates and to publish the CRLs.

3.2 The Central Electoral Office

The task of the Central Electoral Office (CEO) is that of keeping a record of the elections in progress. In particular, for each election the CEO administers the list of those having the right to vote (active electorate), the candidates (passive electorate) and the situation of each active voter in terms of votes already cast and those still to be cast. It issues the voting authorization and keeps track of their use by consulting the Central Ballot-Box. It also keeps a copy of the X.509 certificates of all the entities involved in the process.

The only information not handled by the CEO is that regarding the contents of the votes cast.

3.3 The Central Ballot-Box

The Central Ballot-Box (CBB) receives the votes cast in all the elections in progress. It has no notion of the identity of the voters, but is able to recognize and accept valid votes checking the voting authorization sent by the CEO. The voting authorization does not contain any reference to the voter who has received it. The votes are received and stored in an encrypted form and the CBB does not have the decoding keys. In the scrutiny phase, the encrypted votes pertaining to a specific election are extracted and sent to the scrutiny terminal, where they are then decoded.

The CBB should function in a separate operating environment from that of the CEO, and should be run by a different administrative body. The only communication between the CBB and CEO is through the protocol application for the transmission of the voting authorization and to notify their use.

3.4 The polling stations

The polling stations distributed over the Country represent the interface with the central services. They are presided over by an electoral committee which has the task of physically identifying the voters. The dedicated clients installed at the Voting Terminals (VT) are linked both to the CEO, from which the voting authorization comes, and the CBB, to which the votes are sent. The VTs do not locally hold any status information and thus totally depend on the central servers, which are accessed using the smartcard. No logging, caching or anything else is carried out by the VTs which might enable any tracking of the votes cast. A printer prints out a record of the polling station's operations in real time, reporting the names of the voters, the significant events (such as the starting up and closing down of the VTs) and periodic summaries of the number of voters.

3.5 The communication network

The Voting Terminals in each polling station and printer are interconnected in a local network via TCP/IP, using private IP addresses. An ISDN BRI (Basic Rate Interface) access is installed in each polling station. Each polling station's LAN is directly connected to the central systems via point-to-point ISDN. The ISDN is configured as a closed user group (CUG), which means no interaction is possible with users external to the defined

group. The ISDN router is configured to dial-on-demand, with the dynamic opening of the second channel “B” in the case of intense traffic. The use of ISDN rather than the public backbone of Internet is due to a question of ensuring reliability and quality in the service, as well as for reasons of security. All the network devices are centrally managed and monitored. In order to guarantee immediate technical support during the voting phases and quickly diagnose any possible malfunctioning, each polling station also has an ISDN telephone enabling communication between the polling station and central technical support.

4 The application protocol

The application protocol specifies the relations between the entities of the electronic voting system and is aimed at guaranteeing the legitimacy, integrity, secrecy and anonymity of the vote.

By *legitimacy* it is meant that only those who have the right to vote can vote and can only vote once.

By *integrity* it is meant that the vote cannot be modified once it has been cast.

By *secrecy* it is meant that the contents of a vote cannot be seen until the scrutiny takes place.

By *anonymity* it is meant that the identity of a voter cannot be traced from the vote cast.

Communication takes place in an encrypted form using the protocol SSLv3 (Secure Socket Layer [2]) with 1024 bit RSA keys. The client and server reciprocally identify themselves by means of X.509v3 certificates.

4.1 The voting phase

The data flows during the voting phase are illustrated in Figure 2.

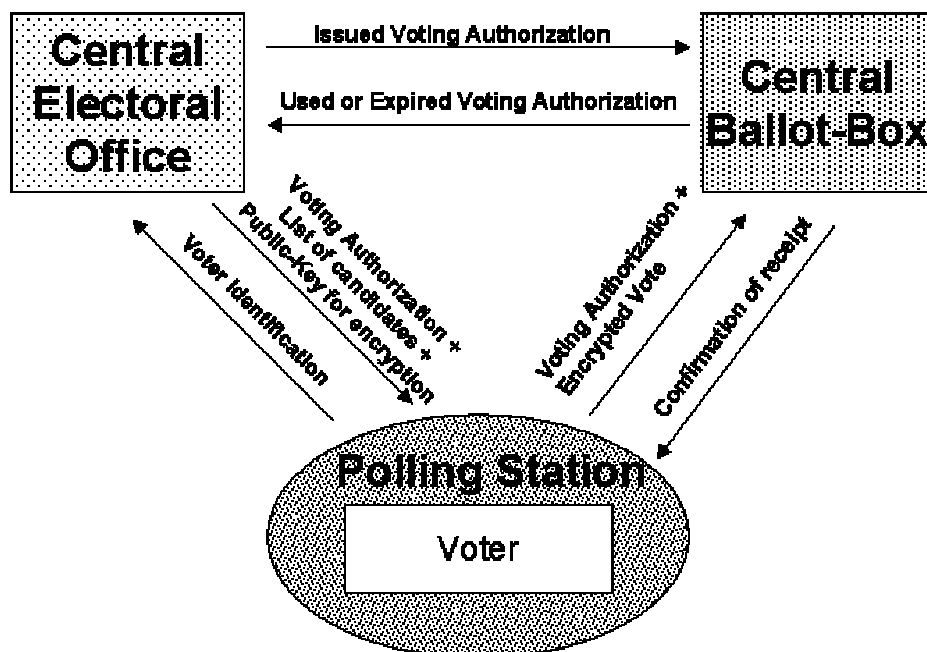


Figure 2: The voting phase

The protocol concerning the voting phase is described in the following Table 1:

Actor	Action	Destination	Voter status
VT	Authenticates itself by means of the VT smartcard	CEO	
VT	Sends the voter's identification codes	CEO	
CEO	Verifies the voter's credentials		Session opened
CEO	Sends list of elections opened to that voter	VT	
VT	Selects an election in which to vote	CEO	
CEO	Gives the voting authorization for the voter and the election		
CEO	Sends passive electorate + voting authorization + public key of the RPO for the election	VT	Voting in progress
CEO	Sends a copy of the voting authorization	CBB	
VT	Encrypts the vote cast by the voter using the RPO's public key and signs it using the private key in the smartcard		
VT	Sends the encrypted and signed vote + voting authorization	CBB	
CBB	Verifies that the voting authorization is amongst those communicated by the CEO and that it has not expired. If valid, the encrypted vote is accepted		
CBB	Communicates the fact that the voting authorization has been used	CEO	
CEO	Records the fact that the voter has voted		Has voted
CBB	Confirms receipt of vote	VT	
CBB	Communicates possible expiry of unused voting authorization	CEO	
CEO	Records the expiry of voting authorization signalled by the CBB		Authorization timed out

Table 1: The application protocol – voting phase

The legitimacy is guaranteed by the CEO, which authorizes the right of each voter to vote only once.

The VT's signature guarantees the integrity of the votes.

The *voting authorization* consists of a random sequence of bits generated on request, having the characteristic of being difficult to guess and having a very low probability of duplication. Used by the CBB to decide whether a vote is valid, it is not kept once it has served its purpose.

The votes stored in the CBB are each encrypted with the public key of the RPO who has organized the election they refer to and are signed with the private key of the VT they come from. The encryption satisfies the need for secrecy and prevents any partial results being known before the end of the voting procedures. Furthermore, it renders, as we shall see further on, any possible data crossover between the CEO and CBB useless, which in any case is prevented by the protocol.

The anonymity is obtained through the combination of encryption, the separation of the CEO from the CBB, the absence of voter identification data in the voting authorization and the fact that this authorization is not stored by the CBB.

4.2 The scrutiny phase

Once the voting procedures have been completed, the CEO authorizes the scrutiny operations, which, in the case of each election, are carried out by the RPO of the university which has held the election. The RPO uses one of the VTs already used in the previous phase.

The sequence of scrutiny operations is illustrated in Figure 3.

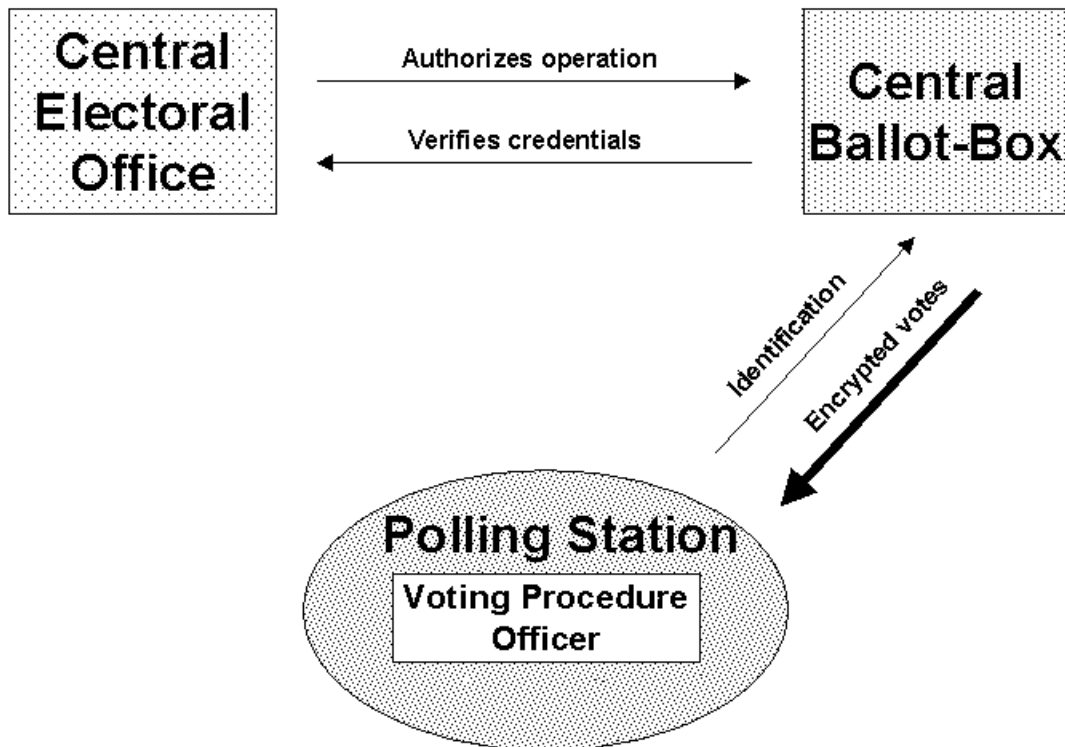


Figure 3: The scrutiny phase

The scrutiny protocol is described in Table 2.

Actor	Action	Destination	Scrutiny status
VT	Authenticates itself by means of the RPO's smartcard	CEO	
CEO	Sends list of elections to be scrutinized	VT	
VT	Requests the encrypted votes for an election	CBB	
CBB	Requests confirmation of the legality of the operation requested by the VT	CEO	
CEO	Authorizes the scrutiny	CBB	In progress
CBB	Sends the encrypted votes for the election as requested	VT	
VT	Decodes the votes using the smartcard, determines the result and signs it with the RPO's private key		
VT	Sends the signed result	CEO	
CEO	Records and publishes the result		Ended

Table 2: The application protocol – scrutiny phase

5 The security infrastructure

The task of the security infrastructure of the system is that of guaranteeing the secrecy, anonymity and integrity of the votes. The secrecy and integrity of the vote must be maintained until the scrutiny, when the votes are counted, while the identity of the voter who has cast the vote must always remain secret.

To satisfy these requirements, wide use is made of cryptographic algorithms in all the phases of the process. We shall start by examining the voting phase.

5.1 The protection of the votes

1. The voting application acquires the preference expressed P_1 from the voter;
2. A random 128 bit key K_1 is generated;
3. The preference P_1 is encrypted by means of the symmetrical algorithm RC4 [8] with the key K_1 , obtaining the encrypted preference P_2 ;
4. A hash HP_2 is calculated on the concatenation of P_2 with the identifying code of the terminal VT and with a random $Rand$, using the algorithms MD5 [4] and SHA-1 [3] in the modality pertaining to SSLv3 [2];
5. HP_2 is signed by means of the RSA [5] of the voting terminal's smartcard, which by using its own private 1024 bit key $PrVT$ generates the signature SVT ;
6. The key K_1 is encrypted RSA using the public key $PuRPO$ belonging to the Recruitment Procedure Officer, obtaining K_2 ;
7. The encrypted preference P_2 , the signature SVT (with VT and $Rand$ elements needed for verification purposes) and the encrypted key K_2 are sent to the Central Ballot-Box via a secure SSL connection with client and server authentication, in accordance with the protocol described in Section 4.

The information relating to paragraph 7 above are stored at the Central Ballot-Box until the scrutiny takes place. The CBB, however, possesses no information which would enable the votes to be decoded, or which would enable a voter who has cast a certain vote to be identified: the only information in its possession being the signature of the terminal from which the vote originates. The function of the signature is that of making it possible to verify that the votes present in the CBB effectively derive from an authorized voting terminal.

Any collusion between the administrators of the CEO and CBB would in any case fail to trace the vote cast back to a specific voter, both because the system does not keep any association between a vote and the voting authorization, and because the vote is encrypted and the decoding key is contained in the smartcard of the RPO responsible for the election to which the vote refers.

5.2 The decoding for the scrutiny

When it is the moment of the scrutiny, the votes are extracted by the CBB and sent to the terminal requesting them, in accordance with the modality pertaining to the application protocol previously described. Communication between the CBB and VT is protected by SSL. The scrutiny procedures at the voting terminal, which we will here call Scrutiny Terminal (ST), are examined in what follows.

1. The scrutiny application at the ST receives the encrypted preference P_2 , the signature SVT , the elements VT and $Rand$ needed to verify it and the encrypted key K_2 ;
2. By means of the VT's public key $PuVT$ the validity of the voting signature SVT is verified. If the signature is not valid, an alarm is given and the entire scrutiny operation is aborted;
3. The RPO's smartcard, using the private key $PrRPO$, carries out the RSA decoding of the key K_2 , obtaining K_1 ;
4. The key K_1 is used by RC4 to carry out the decoding of encrypted preference P_2 , obtaining the explicit preference P_1 .

It should be noted that the CBB's role is merely that of temporarily conserving the encrypted votes, and then sending them when the scrutiny phase starts to the terminal where the RPO of the election to which the votes refer is to be found. The scrutiny is carried out in a polling station which, in general, is not the one where the votes were cast.

5.3 The smartcard

The security infrastructure is based on a smartcard with processing capability implementing RSA. The use of the smartcard is protected by a PIN and the private key stored in the card cannot be extracted. The card blocks after a predefined number of failures to insert the correct PIN.

The VT's smartcards are associated to a particular polling station: the CEO does not accept connections with terminals presenting a smartcard which is not associated with that specific polling station.

5.4 Identification of the VTs

The central servers know the configuration of each polling station and before interacting with the remote terminals they require that:

- ✓ the ISDN connection should originate from the expected caller-id (the presence within the CUG is guaranteed by the telephone company);
- ✓ the router should present the necessary credentials to the authenticating server;
- ✓ the terminal's hardware should be the one expected. Only this hardware will be allowed to carry out the bootstrap;

- ✓ each VT should present a valid X.509 certificate for the polling station where it is to be found. The certificate, contained in the smartcard, permits client authentication with SSL. If the smartcard is extracted or if anything interferes with the regular communication with the VT (such as a switching off or disconnection of the smartcard reader), the application stop working;
- ✓ the polling station should be in opening hours for the operation the VT is about to carry out (voting or scrutiny). The scrutiny operation is only possible if the voting phase has been completed in all the polling stations.

6 System certification

The architecture described and its implementation have been subjected to close examination by a Committee of experts nominated by the Italian Ministry of Universities and Scientific and Technological Research, in its role of guarantor of the correct carrying out of the electoral processes within the Italian academic community. The task of the Committee was to examine the security features of the system and determine whether these were sufficient to guarantee the legitimacy, secrecy, anonymity and integrity of the votes.

The Committee has issued a document certifying that the system satisfies the security requirements and consequently can be used for real elections.

7 The first voting session

The electronic voting system described so far came into service in concomitance with the first voting session for 1999, from the 21st of June to the 9th of July 1999. 71 (out of a total of 73) universities were involved. 79 polling stations were set up with between 2 and 8 terminals per polling station, for a total of 209 VTs.

The number of public competitive examinations published, and, consequently, the number of elections held, were 1,969. 42,494 electors were involved. Each elector was called to vote in a varying number of elections, according to the scientific field he was connected to and his academic position. On average, an elector voted in 6 elections.

In total, there were 26,873 voters, equivalent to 63% of those having the right to vote, and 163,645 votes were cast.

Table 3 gives the data regarding the number of voters in terms of academic position and geographical area.

Italian geographical area	Total			Full Professors			Associate Professors			Researchers		
	Electors	Voters	%	Electors	Voters	%	Electors	Voters	%	Electors	Voters	%
North	18182	11692	64.3	5473	4732	86.5	7324	4516	61.7	5385	2444	45.4
Centre	12439	7579	60.9	3728	3181	85.3	4629	2795	60.4	4082	1603	39.3
South	7737	5128	66.3	1964	1763	89.8	3121	2145	68.7	2652	1220	46.0
Islands	4136	2474	59.8	1002	869	86.7	1716	1037	60.4	1418	568	40.0
TOTAL	42494	26873	63.2	12167	10545	86.7	16790	10493	62.5	13537	5835	43.1

Table 3: Number of voters at the polling stations in the first voting session

Examining the data in the table, what is immediately apparent, among other things, is the link between the percentage of voters and academic position.

The average time taken to vote was around 5 minutes. The time elapsed between the start of the scrutiny operations and the publication of the final results on the web depended on the number of votes which had to be decoded: on average it was about 1 minute.

The first voting session was followed by a supplementary session, provided for in law for those elections where the number of elected people is insufficient to form a complete Committee. The supplementary election was held on the 28th and 29th of September 1999.

8 Conclusions

The system described here came into being as the result of a specific need of the Italian academic community. The fact that its implementation passed the controls of a Ministerial Committee of experts and, above all, the fact that it has been used successfully by tens of thousands of voters leads us to assert that the application protocol and security mechanisms adopted possess a reasonable robustness. The aim of this paper is to submit the system to the international scientific community's judgement in order to obtain useful suggestions with a view to a possible future extension to wider contexts.

9 References

- [1] CCITT. *Recommendation X.509: "The Directory – Authentication Framework"*. 1988.
- [2] A. Frier, P. Karlton, and P. Kocher, *"The SSL 3.0 Protocol"*, Netscape Communications Corp., Nov 18, 1996.
- [3] NIST FIPS PUB 180-1, *"Secure Hash Standard"*, National Institute of Standards and Technology, U.S. Department of Commerce, Work in Progress, May 31, 1994.
- [4] Rivest, R., *"The MD5 Message Digest Algorithm"*, RFC 1321, April 1992.
- [5] R. Rivest, A. Shamir, and L. M. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.
- [6] A. Salomaa, *"Public-Key Cryptography"*, Springer-Verlag, Berlin, 1996, 2nd ed., pp. 200-202.
- [7] B. Schneier, *"Applied Cryptography, second edition"*, John Wiley, New York, 1996, pp. 127-128.
- [8] Thayer, R. and K. Kaukonen, *A Stream Cipher Encryption Algorithm*, Internet Draft, 1999.

10 Vitae

Pierluigi Bonetti was involved with network services management at the Italian National Institute of Nuclear Physics. Since 1995 he works in the Network Services division at CINECA, the Italian most important inter-university supercomputing consortium supported by the Ministry for Universities and Scientific and Technological Research. He focuses on the project and development of value added on-line services and security-critical applications. He is graduated in computer science.

Stefano Ravaoli joined CINECA in 1995 where he was involved in the development and integration of Unix network daemons (HTTP, SMTP, POP3, IMAP, FTP) toward SSL, TLS with particular attention to the support of client authentication and the deployment of smartcard based solutions.

Simone Piergallini received his Laurea degree in Computer Science from the University of Bologna, in Italy, in 1999. Since August 1995 he's employed at CINECA, where he's involved in supporting activities and solutions for the Italian University community. His main interests lie in problems connected with security systems and cryptography applied on internetworking technologies, and in development of user-side software making use of these technologies.