Technological Solutions for Electronic Voting and Guarantees of the Integrity of the Electoral Process. A Case Study.

Luis Panizo, Universidad de León (Spain), Mario Torre, GST Caracas (Venezuela)

Abstract— This paper attempts to show, on the basis of a specific example, that a balanced simple and transparent design for the process of identification and in-person electronic voting is essential to safeguard the basic rights of voters.

Mention of in-person electronic voting, a vote cast at a polling station, raises various questions associated with the combination of procedures to be followed in checking the identity of the voter, taking the vote and transmitting results.

According to the level of automation in place, identities can be checked by using lists on paper, through automated biometric procedures, with a coded alphanumeric identifier, or by means of an electronic National Identity Card.

The use of paper listings is the most conventional procedure. Biometric procedures involve the recording of the requisite biometric measurements during the compilation phase of establishing the electoral register. They also require appropriate technology, readers and, generally, connections with sufficient bandwidth at polling stations to allow these measurements to be taken.

However, recording biometric parameters and automating them makes more sense within a framework of a broader strategy for identity management in areas like security, justice, health, education and others. In this case, putting such solutions in place becomes more worthwhile as its economic viability for society is enhanced.

The case to be studied here centres on in-person voting using identification based on biometric parameters. What at first appears an example of well planned and developed design ceases to be so when subjected to more detailed analysis. This is the case of the Sistema de Autenticación del Votante or Voter Authentication System (VAS) implemented by the Consejo Nacional Electoral or National Electoral Board (CNE) of the Republic of Venezuela.

This paper will start by describing the VAS and explaining its sequence of operation. It will then explain the reasons why the system is not efficient and the risks associated with improper use of information from the VAS for individual political purposes. It suggests an alternative structure for the VAS that would lessen these risks and indicates other applications that might be found for the information gathered in the VAS, so as to improve various features of the electoral system, such as the Register of Electors.

Index Terms— Electronic voting, voting systems.

I. Introduction

SINCE the voting related to the Recall Referendum held on 15 August 2004, the Consejo Nacional Electoral or National Electoral Board (CNE) of the Republic of Venezuela has been used a biometry-based system of technology to record and authenticate electronically the fingerprints of all voters. This system is termed the Sistema de Autenticación del Votante or Voter Authentication System (VAS), although it is also commonly called the "fingerprint system".

Ever since the Recall Referendum of 2004, the CNE has used the VAS for all elections, as a part of the technological infrastructure employed by this institution for all electoral processes. In fulfilment of the Ley Orgánica del Poder Electoral, or basic electoral law, prior to each election the CNE must invite the various political organizations to participate in technical review activities (or audits) of the technological provisions at its disposal, of which the VAS is a part. The Grupo de Seguimiento Técnico or Technical Overview Group (GST) has participated in these technical reviews, including those of the VAS. The GST has collected detailed technical information on this system, which has been used as one of the documentary sources for the drawing up of this paper.

The Technical Overview Group (GST) is a group of a purely technical nature, unaffiliated to any political party whatsoever. It is made up of professionals and technicians in the fields of computation, electronics and telecommunications, who voluntarily put time and effort into studying, analysing, evaluating and auditing the automated voting system in Venezuela, without receiving any form of payment. At present, it consists of approximately ten people. It has no access to resources or finance of any kind from state or private bodies.

II. Description of the VAS.

Biometric identification is the checking of a people's identity based on characteristics of their bodies or behaviour. It may use, for example, the shape of their hands, their fingerprints, the iris of their eyes, their voices or their faces through face recognition.

Although biometric studies are not perfect, they are a very

powerful tool for identifying people. Of all the biometric identification systems currently in existence, fingerprints are the only form legally recognized as a reliable proof of identity. They offer a system which is not only effective but easily applied, with authentication being rapidly achieved.

Fingerprint patterns are divided into four principal types, all mathematically describable. This classification is useful when verifying an identification electronically, as the system searches only in the database for the appropriate type group. Figure 1 shows the basic classification for these type groups and Figure 2 the storage procedure.

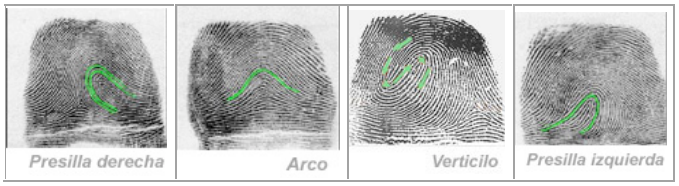

Fig. 1. Classification of Fingerprint Groups: Details ("Minutiae"). (Right Loop, Arch, Whorl, Left Loop).

For this purpose, the position of each characteristic point or "minutia" is represented by a combination of numbers (x and y co-ordinates) on a Cartesian plane. These are used as the basis for creating a set of vectors obtained by linking the minutiae together with straight lines, whose angle and direction yield a unique and unrepeatable configuration. To carry out the reverse process, fingerprint checking, these same vectors are used, not images.

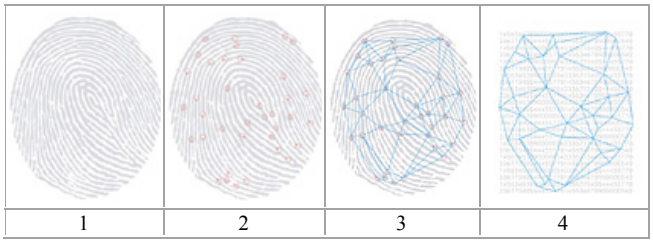

Fig. 2. Procedure for Storing and Identifying Minutiae. (1. The finger is read by the fingerprint reader. 2. The finger is coded by the application. 3. A pattern is generated and digitally compressed. 4. The reader records and recognizes a set of numbers that can be recognized as a unique pattern.)

The Automatic Fingerprint Identification System (AFIS) is a computer system composed of integrated hardware and software that permits reading, consulting and automatic comparison of fingerprints grouped by print files, whether by images, or by minutiae. The print is captured by placing the finger on a transparent pane of glass, with a photograph being taken by a digital camera. This reader terminal is usually called the scanner.

The Voter Authentication System (VAS) is an AFIS implemented by the National Electoral Board (CNE) en Venezuela. It was purchased by this institution from the firm Cogent Systems Inc. (www.cogentsystem.com). The first VAS was obtained in June 2004, but between then and now there have been various extensions and improvements to it.

The prime aim of the VAS is to guarantee "one voter – one vote". The objective that justified the setting up of this system was to ensure that electors can vote just once in any poll, and that if they try to vote again, this will be detected immediately, so that they can be punished for committing this offence.

The VAS consists of a complex system of computers and telecommunications, made up of the following subsystems:

--Identification Points at the Polling Stations.

--Data Centre.

--Satellite Communication Links.

Each Identification Point (also called the "fingerprint checker") consists of:

--A fingerprint scanner.

--A standard portable computer (laptop P.C.), Windows-compatible.

--A mouse.

--A satellite communications terminal.

On a polling day, a given Polling Station may have one or more Identification Points, all sharing a single satellite communications terminal through a Local Area Network (LAN) set up in the Polling Station. These Points are set up at the entrance of the Polling Station, separate from the Automated Voting System, and there are no communication links between the two systems, which must function completely independently.

On entering the Polling Station, voters must go to the Identity Point and identify themselves with their National Identity Card. The operator inputs these identity data and asks voters to place their thumbs on the scanner. The P.C. executes a software application allowing the recording of voters' fingerprints and their transmission, together with the personal data for the voters, to the Data Centre through the satellite communications terminal. Figure 3 shows one of the screens of the human-machine interface of the application executed on the P.C..

It is important to stress that the application executed in the P.C. can operate on line or off line. The on-line application (called on-line VAS) executes only when the satellite link to the Data Centre is operational. The off-line version of the application (called off-line VAS) is used exclusively when there is no satellite link or when this link is not operational.

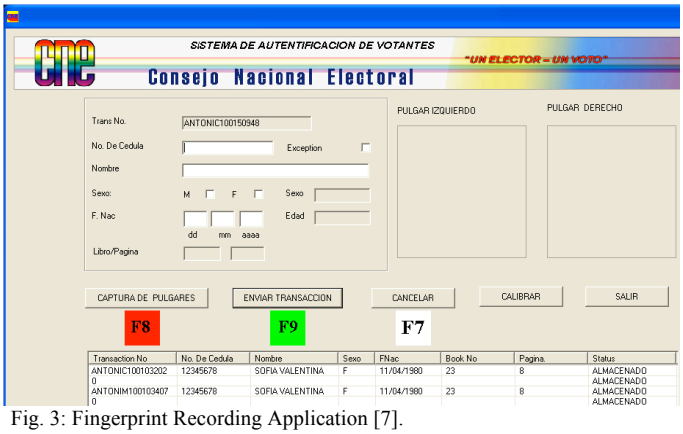

Fig. 3: Fingerprint Recording Application [7].

The functions of the Identification Point do not differ greatly whether it is on or off line.

The operation of capturing the two thumbprints takes between 30 seconds and a minute, depending on the skill of

the operator. However, transmission to the Data Centre (and the related response) may take between 5 and 15 minutes. If the Identification Point is working off line, or if there is a long delay in identifying voters, they are allowed to go on and vote. If voters are doing so for the first time, the system just records their prints and the voters proceed to cast their votes.

The satellite link is via a VSAT satellite terminal, which communicates with the Teleport of the Data Centre through the Skystar 360E Satellite System, via the ANIK-II satellite, using Ku band (11.0 to 14.5 GHz) with a maximum power of 1W. This arrangement uses a VSAT dish, installed on the roof of the Polling Station. For data, the satellite terminal establishes a link using TCP/IP, which is makes transfers to the P.C. via an Ethernet connection.

The Data Centre is a complex Computing System with a distributed processing architecture [1], made up of around 120 high-power computers, sharing a high-speed segmented local area network (LAN). This set of servers executes the Civil AFIS System provided by Cogent Systems. The computer nexus is directly connected to the Satellite Teleport, and forms a private data network with all the Identification Points set up around the country on polling days.

The system receives via satellite all the transactions coming from the Identification Points. On receipt of a search request, the AFIS System initiates comparison of the prints submitted against the database of voters who have been registered as voting up to the moment in question. The results obtained are recorded, the databases are updated and a response message is sent to the relevant Identification Point. Exchanges of packets of data between the AFIS System and the workstations are in enciphered form, as well as requiring due authentication from both the System and each Identification Point.

Starting with the packet received from an Identification Point, the servers perform a search in the database, then instruct other levels (parallel multithreaded architecture, or PMA, processors) to carry out a 1:N search. This search may lead to one of three outcomes:

--"MATCH": There is a coincidence between the print from a voter at one of the Identification Points, and a print from a person recorded as having already voted (with prints being taken) in the same poll.

--"NO MATCH": The system has determined that this print does not coincide with any of those previously collected.

--"GREY AREA": The system has not been able to determine if there is a "MATCH" or "NO MATCH". In this case, the print is passed on to a working party of around 25 fingerprint experts, who determine manually whether the person has already voted (MATCH) or has not yet done so (NO MATCH).

Regional servers instruct the PMAs through communications controlled by Messaging Servers. The comparison order is sent to one of the 40 PMA Servers. These servers perform a 1:N search of all the prints reaching the system. Every PMA holds internally the ENTIRE biometric database for the system and can carry out up to 500,000 searches per second. Information in the form of MATCH / NO MATCH / GREY AREA is returned via the messaging servers to the regional servers, which respond to the fingerprint checker.

Finally, the PMA that carried out the comparison of a given print sends the result of this comparison to the appropriate messaging server, which in its turn sends it back to the Identification Point.

Figure 4 gives a block diagram showing the satellite communication system implemented for the VAS.

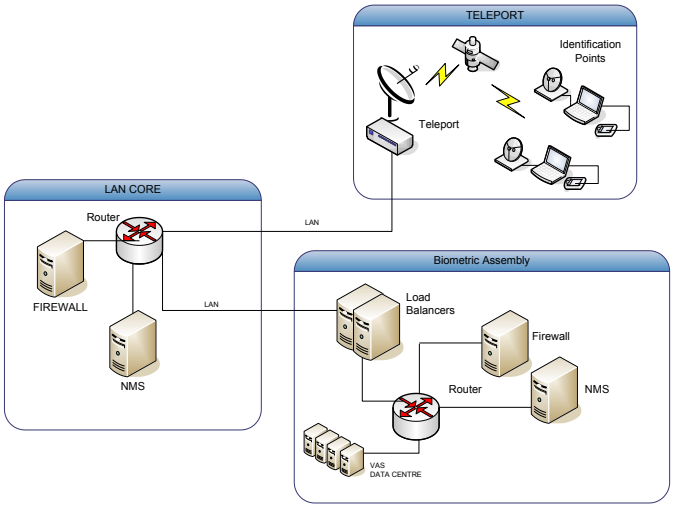

Fig. 4: Block Diagram of the Satellite Communication System.

It is important to emphasize that the database resident in the laptop does not contain the images of the prints of all the electors in the state (nor even in the Polling Station). It contains only the minutiae, which are stored in the vvv_minucia database. However, both the on-line VAS application and its off-line VAS counterpart store the images of the prints of all the voters coming to the given Identification Point. This storage takes the form of .BKP format files on the hard disk of the machine. In the most extreme case, the total size of all the image files stored during one polling session is no greater than 30 MB (Megabytes).

The operating procedure for the VAS on polling day can be summed up as consisting of the following steps:

1) On polling day, voters come to the Identification Point, bringing their National Identity Cards (NIC).

2) The operator keys details of the NIC into the applications software of the Point (whether or not the Point is on line), then pushes the F8 key for "Thumbprint Capture" (see Figure 4). The first step is to investigate whether this elector has already come through this Identification Point, either because the print has already been taken, or because it has simply been checked against the data tables. If either of these has been done, the operator informs the voter there has been a prior registration, so that no further vote can be cast.

3) In the case where there is no record of either of these actions, the application moves on to check the elector's data against the vvv_voter and vvv_voter_vc in the database, determining whether electors are entitled to vote in this state and whether they are registered to vote at this Polling Station.

4) If either of these gives a negative result, electors are told that they cannot vote at the Polling Station in question and informed about the Station where they can cast their votes (only if it is a question of an elector entitled to vote in the state concerned but not in the specific Polling Station).

When both results are positive, the operator proceeds to record the thumbprints for both of the voter's hands.

5) Once the prints and personal details (forename, surname, NIC number, sex, and so forth) for an elector have been taken, the application carries out the following processing:

--It converts the image of the two thumbprints into minutiae.

--It stores the elector's personal details, minutiae and the image of the prints in a file on the hard disk of the P.C..

--It carries out a search for the minutiae of the elector's prints in the table vvv_minucia (1:1 search). The result of the comparison of minutiae is stored on the P.C.'s hard disk. This search will yield one or another of the following results:

--There is no record of the minutiae for this elector (NIC) in the table vvv_minucia (result = NEW VOTER);

--The quality of the minutiae stored in vvv_minucia is not good enough to carry out a valid comparison (result: POOR QUALITY).

--The minutiae for the prints recorded and the minutiae stored in vvv_minucia are not from the same print (result: NO MATCH).

--The minutiae for the prints recorded and the minutiae stored in vvv_minucia coincide (result: MATCH).

6) The result of the comparison is presented to the Identification Point operator. This operator takes the following decisions:

--If the result is NEW VOTER or MATCH, the operator immediately tells the elector to go and cast a vote.

--It the result is POOR QUALITY, the operator tries again to capture a print record. If the error persists, the elector is permitted to cast a vote.

--If the result is NO MATCH, the operator advises the elector that the prints do not correspond to those stored in the database for the National Identity Card number concerned.

It should be noted that in all cases the system immediately informs the operator about searches undertaken locally in the P.C.. It is of importance to point out that at this level irregularities occur only if the prints of the elector do not coincide (NO MATCH) with those previously stored in the table vvv_minucia. In this case, the Identification Point operator requests electors to sign a document indicating that they have been informed of the irregularity, but allows them to go and vote, the sole condition for casting a vote being that the relevant line in the voting ledger must be empty.

Thereafter, the system operator pushes the F9 key "send transaction". When this is done, the following steps are executed:

--A transmission message is created with the personal details for the elector (forename, surname, NIC number) of the voter.

--If the result is NEW VOTER, NO MATCH or POOR QUALITY, the image of the voter's prints is added to the transmission message.

--If the result is MATCH, no print image is sent.

--The transmission message just built up is loaded into a queue of messages waiting for transmission to the Control Centre. This queue has a maximum capacity of four messages.

--The application selects at random one of the messages stored in the transmission queue and sends it.

After a certain lapse of time (which may vary from 5 to 15 minutes), the Data Centre responds with the result of the comparison of the minutiae of the prints of the elector and those of all the prints so far recorded which are stored at the Centre.

If the result of the response coming from the Data Centre is NO MATCH, then indeed it is a question of a person who is voting for the first time in this poll.

If the result of the response from the Data Centre is MATCH, the elector is trying to vote for a second time. However, the delay imposed by the control queue means that the Identification Point operator only learns that the law has been broken some time after the voter has committed this offence and left the Polling Station.

The operator now moves on to processing the next elector in the queue, since it is not feasible to wait for the result from the Data Centre relating to the previous voter.

Table 1 sums up all the possible results from an Identification Point that can await an elector.

Table 1: Possible Outcomes from the Identification Point

Case	Status of Voter	Function of the Identification Point	Interaction with the Data Centre	Result for the Voter
CASE A: THE VOTER IS NOT FROM THIS STATE OR IS NOT ASSIGNED TO THIS POLLING STATION				
A.1	NIC number corresponds to a voter not from the given state.	Operator informs electors that they are not entitled to vote at this Polling Station.	None (NO DATA ARE TRANSMITTED) .	Leaves, as unable to vote in this Polling Station.
A.2	NIC number is from the correct state, but is not assigned to this Polling Station.	Idem. A.1, and indicates at which Polling Station they may vote.	None (NO DATA ARE TRANSMITTED) .	Leaves and goes to the assigned Polling Station.

CASE B: THE ELECTOR IS ASSIGNED TO THIS POLLING STATION				
B.1	The print taken from the elector coincides with the print stored in the P.C., corresponding to the NIC number quoted (MATCH)	Immediate response. The operator tells the voter to proceed to cast a vote. The prints taken are stored on the P.C.'s hard disk.	The Identification Point transmits to the Data Centre only personal details (NIC number, forename, surname, etcetera) of the elector. Transmission to the data centre is not immediate	PERMITTED TO VOTE.
B.2	The print just taken from the elector does not coincide with the print stored in the P.C. corresponding to the given NIC number (NO MATCH)	Immediate response. The operator tells the elector the print does not match the record in the database. The print just taken is stored on the P.C.'s hard disk.	The Identification Point transmits to the Data Centre the personal details of the voter, along with the image of the print taken. Transmission to the data centre is not immediate	PERMITTED TO VOTE. The right to vote cannot be denied. The system operator takes details with a view possible legal action against the elector for voting twice. The elector is requested to sign a document acknowledging this situation.
B.3	No print is stored in the database of the P.C. for the NIC number in question (NEW VOTER)	DELAYED Response. The operator inputs the details for the voter and initiates transmission to the Data Centre. The response to this request may take from 5 to 15 minutes. The print taken is stored on the P.C.'s hard disk.	The Identification Point transmits to the Data Centre the personal details of the voter, along with the image of the print taken. Transmission to the data centre is not immediate	PERMITTED TO VOTE. Owing to the delay in responding, the elector proceeds to cast a vote. The response (MATCH or NO MATCH) from the Data Centre will arrive late (the elector will already have voted).
B.4	The print taken from the voter is not of sufficient quality to allow a search to be made in the P.C.'s database (POOR QUALITY)	DELAYED Response. The operator inputs the details for the voter and initiates transmission to the Data Centre. However, the response to this request may take from 5 to 15 minutes. The print taken is stored on the P.C.'s hard disk.	The Identification Point transmits to the Data Centre the personal details of the voter, along with the image of the print taken. Transmission to the data centre is not immediate	PERMITTED TO VOTE. Owing to the delay in responding, the operator tells the elector to proceed and cast a vote. The response (MATCH or NO MATCH) from the Data Centre may arrive when the elector has already voted and left.

III. Recovery of Identification Point Equipment.

When the polling ends, all the Identification Point machines are collected up by the authorities of the CNE and taken back to the depositories of that institution.

Once they are back at the CNE, the P.C.s are examined. The following information is downloaded from the hard disk of each computer:

--The images of all the prints taken on polling day.

--The list of all the electors recorded by the Identification Point equipment.

--The minutiae from the prints collected.

--The results of comparisons between the minutiae of the prints taken on polling day and the prints previously stored in the table vvv_minucia of the database in the P.C..

This information is used by the CNE essentially to update the prints stored in the Data Centre, using the fingerprints collected during polling, if they are of higher quality.

IV. Costs Associated with the VAS.

As described in this document, the VAS is effectively a complex system of computers and telecommunications, developed, deployed and used with the single aim of ensuring "one voter – one vote".

An investigation has been carried out into the costs involved in a system of this complexity. On the basis of the results obtained from these enquiries [2], [3], [4], the following may be concluded:

The first Voter Authentication System (VAS), installed in June 2004, cost 54 million United States dollars (US$ 54,000,000.00) [2].

The System was updated in October 2004 at an additional cost of 20 million United States dollars (US$ 20,000,000.00) [2].

On 20 June 2005, Cogent Systems received an order from the CNE to the value of 31.7 million United States dollars (US$ 31,700,000.00), for new updates and improvements to the system [3].

On 2 August 2006, Cogent Systems received orders for improvements to the VAS worth some 7 million United States dollars (US$ 7,000,000.00) [4]. On 31 December 2006, profits for Cogent Systems attributable to the CNE orders reached 16.9 million United States dollars (US$ 16,900,000.00) [5].

Moreover, the company Gilat Satellite Networks was chosen by the CNE to supply and install VSAT satellite terminals in the majority of the Polling Stations, as also the Teleport in the Data Centre. Although precise details for this transaction are not known, it is estimated that the costs involved come to around 12 million United States dollars (US$ 12,000,000.00).

The total outlays on the VAS, based on the figures quoted above, must come to around 139.5 million United States dollars (US$ 139,500,000.00). In additional, the cost of using Ku band satellite transmission bandwidth polling days had an estimated cost of 960 thousand United States dollars (US$ 960,000.00). If it is kept in mind that the VAS has been used on four occasions (August 2004, October 2004, December

2005 and December 2006), it can be estimated that the expenditure on satellite transmission amounts to some 3.84 million United States dollars (US$ 3,840,000.00). This adds up to a total of more than 143 million United States dollars (US$ 143,000,000.00), excluding all the sums spent by the CNE on staff, equipment, training, travelling expenses, advertising and publicity, and other items.

V. Other Information of Interest with Regard to the VAS.

Further information is available on the functioning of the VAS, complementary to the description given above. This information includes the following points:

During all the uses made of it since August 2004, the VAS has detected just 56 people who actually voted twice in a single poll. Almost all were detected after casting their second vote and leaving the Polling Station. The CNE has never yet brought charges against any of these people.

The comparison carried out in the Data Centre (once a print arrives from an Identification Point arrives) falls into a "grey area" (in which the system cannot determine whether it is a MATCH or NO MATCH) amounting to 1.5% of all cases. In this situation, the system passes on the thumbprints to a group of 25 fingerprint experts who make the final decision. Obviously, when this happens the associated response time climbs to around 30 minutes.

In November 2006 (prior to the Presidential Election of December 2006), the CNE stated [2], [7] that it had on record the thumbprints and personal details of more than 8 million electors. It is estimated that fresh prints were collected from about 2 million voters during that poll. It is also estimated that around a further million prints were gathered in the elections of 2005, 2006 and 2007, so that it can be stated that the CNE has on record the prints of approximately 10 to 11 million voters. However, this calculation may be optimistic, since it is known that fingerprint capture equipment was mostly installed in those same centres where it had been in use in previous voting.

Here is a good point at which to note that in all the elections in which the VAS System has been used the coverage of the system at a national level has been partial (it has not covered all the national territory). There has never been a time when Identification Point equipment has been set up in ALL the Polling Stations. At best 60% of Polling Stations have been covered. Thus, it is in no way possible to assert that the System is achieving its principal objective of ensuring "one voter– one vote".

VI. Inefficiency of the VAS.

The VAS is incapable of detecting, in real time, that an elector is attempting to vote twice in the same election. Assuming that a person takes on the identity of another elector who has never before passed through the VAS (so there is no prior print for this voter in the local database in the P.C.), as explained in Point B.3 of Table 1, the VAS will be unable to prevent the electoral offence, since it will detect the irregularity 5 to 15 minutes (on average) after the person has gone through the Identification Point. From this it may be concluded that it is useless transmitting the thumbprint of the "dubious voter" from the Identification Point to the Data Centre, for the relevant response from the Centre will never come in time to prevent the alleged irregularity.

The VAS is able to detect an irregularity only if it is the case that a person assumes the identity of another elector whose print has been recorded by the VAS during some previous poll and who is supposed to vote in the state in which the Polling Station is located. In this instance, the print of the elector really entitled to the vote is stored in the local database of the Identification Point, and the detection of a NO MATCH is immediate. It should be stressed that this detection occurs without any necessity for transmitting information to the Data Centre; detection occurs entirely at a local level. Furthermore, it is crucial to clarify that in the case of such an irregularity occurring, the operator of the Identification Point cannot legally prevent the person involved from casting a vote. All that the operator (and the Polling Station authorities) can do is to take a note of the details of the person voting twice with an eye to later legal action.

As described in Point B.1 of Table 1, the Identification Point transmits to the Data Centre all the personal details of the elector (forename, surname, National Identity Card number, and so forth) even when it is determined that the print of the voter in question coincides (MATCH) with the print stored in the local database of the Identification Point. This gives the VAS an additional function going beyond its objective of ensuring "one voter – one vote". There is no technical justification for the transmission of the personal details of electors in the case where the system authenticates them locally.

The passing of electors through the Identification Points, and the occurrence of possible irregularities, are duly recorded on the hard disk of the P.C. of each Identification Point. As has been explained in this document, these computers are recovered and their information is downloaded from the hard disks for further processing. Hence, the System can detect irregularities by electors after the polling is completed, if any have in fact been committed. The system has full information on those people who have committed any offence, and the databases hold the evidence to incriminate them.

In the light of the above, it is easy to see that the data link between the Identification Points and the Data Centre is of NO USE. The VAS system can offer the same functions and fulfil its objective ("one voter – one vote"), without any need for such a data link.

It is striking that, in a presentation given by a representative of Cogent Systems at the "First International Conference on Biometrics of the Argentine Republic", on 23 November, in Buenos Aires, Argentina [7], it was stated that the System carried out on-line updating of the list of numbers of National Identity Cards of those who had already voted, offering real-time statistics. In other words, the VAS as installed is compiling a centralized and nearly real-time (on line, with 5 to

15 minutes' delay) listing of every voter in the nation who goes through an Identification Point connected to the Data Centre.

This function has no relationship whatever with the objective of the VAS System, as it provides private details of which citizens have gone to cast their votes, and roughly at what time they have done so. Such a function IS CLEARLY UNNECESSARY. Any political grouping gaining access to such information on line could use it to make decisions about massive mobilizations of voters or utilize it to threaten specific groups of people.

VII. Proposal for Improvements to the VAS.

It is not the intention of this paper to propose the total elimination of the VAS. Nevertheless, as it is designed and as has been explained above, the system performs functions for which it was not intended, and which might bring clear advantages to one political group as opposed to others. Hence, the proposal is to make changes to the Voter Authentication System such that it will fulfil solely and exclusively the aim for which it was created.

The proposals for modification of the VAS are the following:

--Elimination of satellite or other data links between the Identification Points and the Data Centre. As has already been explained in some detail, such links in no way aid in achieving the main aim of the VAS, but do provide privileged information that could be used to the advantage of one political party as against others.

--Downloading onto the hard disk of the P.C. in the Identification Point of the database of minutiae corresponding to ALL ELECTORS at a national level. As has been explained in this paper, every portable computer has on its hard disk the minutiae for the electors registered in the state where the Polling Station is located. If the table vvv_minucia is loaded with the minutiae of ALL the voters listed on the Electoral Roll (ER), the hard disk space required by the P.C. is of the order of 18 Gigabytes. Such a capacity is easily attainable with hardware technology currently in existence.

According to this proposal, Identification Points would be set up in Polling Stations, as in previous elections, but no satellite link would be established between these Points and the Data Centre of the VAS. In fact, the Data Centre would be of no practical use on the polling day itself.

The principle on which the new VAS System would work after the changes put forward here would be as follows:

1) An elector would come to the Identification Point (which would have no communication link with any other equipment).

2) The Identification Point would take the elector's thumbprints.

3) After searching for and comparing 1:1 the elector's prints with those previously stored in the table vvv_minucia and with the elector's National Identity Card number:

--If the prints coincided (MATCH), the voter would have been authenticated and could vote.

--If the prints did not coincide (NO MATCH), the voter would not have been authenticated, and could vote, but would have personal details taken for possible legal investigations.

--If no previously stored print were available in vvv_minucia for this NIC number (potential NEW VOTER), the Identification Point would carry out a 1:N search for the elector's prints among the prints from the whole nation stored in vvv_minucia.

4) If there were a coincidence (MATCH), this person would be identified with a different NIC number and name, not corresponding to the NIC presented. Although such people could vote, their details would be taken by the authorities in the Polling Station.

5) If there were no coincidence (NO MATCH), the person could be a potential NEW VOTER. However, in this case, personal details, minutiae and prints would be stored on the hard disk for later checking once the Polling Stations closed and the Identification Point equipment recovered.

In the case of a 1:N search as described above, more computer power might be needed than is available from a conventional P.C.. Nevertheless, if equipment with cutting-edge technology were used (Dual Core, 2.0GHz or better), with sufficient RAM memory capacity (2GB), and a high-speed hard disk (5,400 r.p.m.), it is estimated that such a search could be carried out in 30 to 60 seconds. In any case, this processing could be performed as a background task and would not delay voters, who should never have to wait for any result before going to cast their votes.

In all of the circumstances mentioned above (even in the case of a MATCH), the new prints from the voter would be captured, along with personal details. At the end of polling, each Identification Point would have an additional table (called, say, vvv_asistentes) in its database, with the information corresponding to all the electors who in fact had passed through that Identification Point (together with their minutiae and thumbprints).

When all the work stations were collected up and recovered, all the vvv_asistentes tables from each of them would be downloaded at the Data Centre. With this information, the following tasks would be performed:

--A cross-check of each vvv_asistentes table would be made with the database of prints stored at the Data Centre. This would verify that those taking part in the poll were indeed people already registered in the system. In this way it would be possible to detect irregularities (for example, individuals voting just once, but under a different name). Any people who were genuinely new voters could be added to the database held at the Data Centre.

--A comparison of the vvv_asistentes table from each Identification Point would be made with the vvv_asistentes tables from all the other Points. This would be the real guarantee of "one voter – one vote". Any irregularities detected here would be subject to legal action under the laws currently in force, to the fullest extent.

In this way, the CNE would be able to carry out the voter

authentication procedure off line, in peace and quiet, days after polling. There is no need for such a sophisticated on-line computing infrastructure as the current VAS. Besides this, the CNE (and consequently the nation) would save around one million United States dollars (US$ 1,000,000.00) at each poll by not requiring payment to be made for the satellite transmission bandwidth, not to mention the costs of operating the Data Centre on the day of polling.

However, the most important point is that the VAS System could no longer be used as a control and real-time follow-up mechanism to check on who had gone to cast a vote on polling days.

Additionally, the objective of the VAS, "one voter – one vote" should be reinforced by a much simpler and more practical procedure: the use of indelible ink. If all voters who had already cast a vote had to dip one of their little fingers in indelible ink, it would be very difficult for them to vote a second time, even if they had a false second identity.

The database of the VAS would hold information about voters' participation in each poll that would be much more accurate than the details provided by voting ledgers. The VAS would record with precision how many and which electors voted at each of the Polling Stations during the voting process.

To conclude, the information stored in the VAS would have a great deal more usefulness than merely the intended objective of ensuring "one voter – one vote". It could be used for the following purposes:

--As a tool for correcting the ER.

--As a source of information for auditing the number of voters per Polling Station.

VIII. The VAS and Correction of the ER.

The most useful feature of the information stored by the VAS since 2004 would be in allowing correction of the ER. Cross-checking of the VAS database against the ER could contribute to obtaining information such as these details:

--Electors who have died, but whose details still appear in the ER, as they would not be registered by the VAS.

--Errors in the ER, caused by duplication of entries, mistakes in National Identity Card numbers, and the like.

Additionally, the VAS database could have incorporated into it the biometric information for new electors. These, at the point at which they were entered on the Electoral Roll or when their details were updated in the ER, would have their prints taken and recorded (in fact, this sort of action already occurs). These prints could be directly uploaded into the VAS database.

IX. The VAS and Audits of Voters.

One of the main risks of the Automated Voting System is the "spontaneous" generation of votes from electors who do not come to the Polling Station, in fact cast by members or observers from a given political party in Polling Stations where observers from other parties are not present. In such cases, unscrupulous people could add votes in the voting machine, falsifying signatures and thumbprints in the relevant voting ledger.

The VAS database would be a useful tool for detecting such irregularities. After polling, when the laptops from the fingerprint capture equipment had been recovered, it would be possible to do the following:

Determine precisely the number of voters who actually came to the respective Polling Stations. This could be compared to the number of votes (including spoilt ballots) cast at each Polling Station, with any discrepancies being detected.

In later auditing, carry out a comparison between the thumbprints made on the voting ledgers and the prints taken by the VAS. This could be done by selecting a random sample and using fingerprinting specialists.

Nevertheless, it is important to stress that this operation might sometimes be inaccurate. This is because quite often for various reasons certain voters do not go through the fingerprint capture equipment installed in their Polling Station. Despite this, the information collected could yield interesting statistical indications.

X. Conclusions.

The Voter Authentication System (VAS) constitutes a complex computer and telecommunications system whose principal objective is to guarantee the authenticity of voters before they cast their votes, and thus fulfil its watchword of "one voter – one vote". In seeking to attain this objective, the National Electoral Board has invested a great deal in both human and material resources.

Despite this, the VAS, as it is designed at the present moment, performs the tasks for which it was set up in an incomplete and inefficient fashion. In additional, it provides privileged and confidential information about the attendance of electors at Polling Stations during the voting period. This risks being used as a political weapon to gain advantages for the political party in power by controlling and frightening the population of electors.

Nonetheless, it is not proposed that the VAS should be eliminated, but rather that it should be restructured, so that it will fully achieve the aims for which it was developed, at a lower operating cost and without the dangers currently present. This paper has outlined an efficient alternative architecture, eliminating any risk of the system providing real-time identification of individuals in the flow of voters.

Finally, the paper has shown that the information collected by the VAS since 2004 down to the present could be used for various activities and corrections of other parts that go to make up the Electoral System.

References

[1] GST, Reports on the technical audits of the Voter Authentication System carried out in November 2006 and November 2007.

[2] Cogent Systems, "Cogent Systems Announces Record Third Quarter Results", 1 November, 2004. Available: http://investor.cogentsystems.com/releasedetail.cfm?ReleaseID=147036(URL).

[3] Cogent Systems, "Cogent Systems Receives Letter of Intent for $31.75 Million Follow-on Order from the Venezuelan National Electoral

Council", 20 June, 2005. Available: http://investor.cogentsystems.com/releasedetail.cfm?ReleaseID=166523(URL).

[4] Cogent Systems, "Cogent Systems Announces Second Quarter Results", 2 August 2006, Available: http://investor.cogentsystems.com/releasedetail.cfm?ReleaseID=206124(URL).

[5] Cogent Systems, "SEC Annual Report (Form-10k), 1 March, 2007. Available: http://investor.cogentsystems.com/secfiling.cfm?filingID=1193125-07-44364(URL).

[6] Gilat Satellite Networks, "President of Venezuelan National Elections Board, Jorge Rodriguez, announces that Gilat is among the companies chosen to take part in project for the transmission of data via satellite during upcoming Presidential referendum in August 2004", June 2004, Available: http://www.gilat.com/Content.aspx?Page=news&NewsId=1359(URL) .

[7] Valdés Muñoz, Sergio (Cogent Systems). Presentation: "Sistema de Autenticación de Votantes. Un elector – un voto", Primer Congreso Internacional de Biometría / First International Conference on Biometrics of the Argentine Republic, 22 to 24 November 2006, Buenos Aires, Argentina. Available: http://www.biometria.gov.ar/ppt/Valdes_venezuela.pps(URL).