

Providing Haiti with a Safeguarded Electronic Voting System

A White Paper by Alex St-Gardien Jecrois and Thomas Bronack of JASTGAR

Haiti has a long history of problems and weaknesses when it comes to providing their citizens with a safe and secure voting system, which has resulted in a loss of confidence in elected officials and politicians in general. Additionally, the citizens of Haiti are not receiving the benefits most governments provide to their people through infrastructure, education, and social services.

Most of the problems we have seen fall into either Fraud or Corruption. Fraud being based on an individual voting multiple times and corruption being related to crime at voting stations or against voters to influence who they vote for.

We believe we have a way to protect Haiti against voting fraud and corruption, while also guarantying "One Person – One Vote". Our electronic voting system (*eVOTE*) is based on a Voter ID Smart Card (*eCARD*) that contains the individual's bio-metric signature within its chip, with an original copy maintained in our "Registered Voter Data Base".

The *eCARD* is presented at the voting station and serves as a means of identification that can be verified locally when you insert your *eCARD* into the bio-metric reader and have a bio-metric scan performed (could be finger print, eye scan, facial recognition, etc.). The reader and scan results are compared and if a match is made the voter is cleared to vote, but we also do a remote comparison against the "Eligible Voter List" and the "Voter Activity" data base to insure that this person is allowed to vote and has not already voted in this election.

If the individual does not pass our local and remote tests, the *eCARD* remains in the machine and the local guard notified about the active fraud, so that the individual can be detained for questioning or arrested and the fraudulent *eCARD* taken by the guard. Nipping this crime in the bud and containing the criminal activity in such a visible manner will go a long way to deter crime and bolster trust in the voters that elections are no longer a rigged event.

eVOTE maintains an Audit Trail of all voting activities, and includes pictures snapped when the voter cast their ballot. This information can be used to: identify crimes; drive police activities, produce documentation, and aid in the prosecution of offenders. Our system is flexible, paperless, rapid, and easy to use. We provide the option to have multiple languages to select from, and *eVOTE* is capable of serving the needs of people with disabilities.

We have contacted various Haitian officials, but have not heard any replies as yet. We now believe that we need the support of Haitian citizens to push for a new voting system better

capable of protecting their rights. We do have a request to speak on Haitian radio, but we originally wanted to allow the politicians and officials to respond to us first. Now we believe that the people of Haiti should be told of how a new voting system could safeguard their rights and help place qualified and honest people into political positions. Maybe a strong voice from the people would force the politicians to realize that action must be taken to best protect the citizens of Haiti and give them a true and honest voice in political decisions.

We have design papers, executive presentations, and other White Papers describing our system and its benefits, but let me summarize that information here.

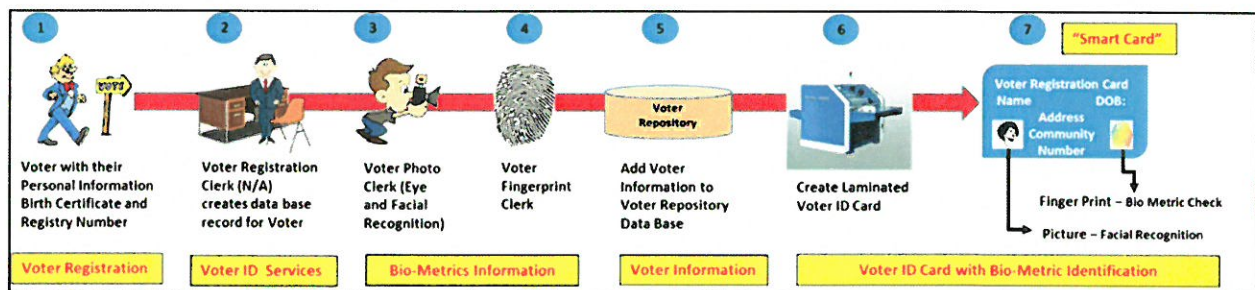
Our system is broken into four basic components and **two major operations**.

- The first operation is identification and validation, while
- The second operation is voting and reporting in near real-time.

The **products** comprising our system include:

1. **eCARD** – a Bio-Metric based Smart ID Card used to verify a person’s identity.
2. **eCARD APPS** – a group of applications (hand held and PC / Server based) that serve the needs of eCARD holders.
3. **eVETTING** – a method for verifying a person’s identity and validating their background through Bio-Metrics and the examination of many data bases from a variety of organizations.
4. **eVOTE** – our electronic voting system

How an eCARD is produced



Although this is a picture for an electronic voting system, it can serve as an example of my concept because it shows the steps necessary to obtain personal bio-metric information and create a Personal Identification Smart Card. The process would include:

1. Individual enters location to obtain a Smart Card Identification for Voting, Driver's License, Passport, VISA, Immigration Services, Alien Identification, Social Security Benefits, Welfare, etc. (the list can go on until all requirements are met).

2. A clerk assists the individual complete the paperwork required to prove they are who they claim to be (background checks can be performed if necessary, but certainly Picture ID, Payroll Statements, Bills Mailed to their address, etc. would be needed to support their claim). This information is used to create a data base record for the individual as a foundation record (Parent) that would be added to as more processes are completed, but as of this point in time we have a documented individual claiming to be someone specific.

3. Stage three would be when Bio-Metric information is obtained from the individual, for example: DNA, Eye Scan, Facial Recognition, Finger Prints, etc. At this point we have the paperwork submitted by the individual and the bio-metric information associated with the individual so a comparison can be made to prove identity.

4. The bio-metric information is checked to insure it has been accurately taken and meets the parameters of the bio-metric equipment being used to scan, read, and process the bio-metric data. Today Smart Cards with chips are inserted into a slot added to the normal charge card scanners. The Smart Card is inserted instead of swiped and must be retained in the machine until the transaction is completed. This is an important issue related to a Smart Card and will allow for apprehension of criminals while in the act of committing a crime, and/or the erasure of information on the chip to eliminate duplication of thefts or criminal acts associated with the Smart Card. Just think about the implications behind that feature, while remembering the size of the equipment needed to read and process the Smart Card (a small investment indeed – think Apple Square).

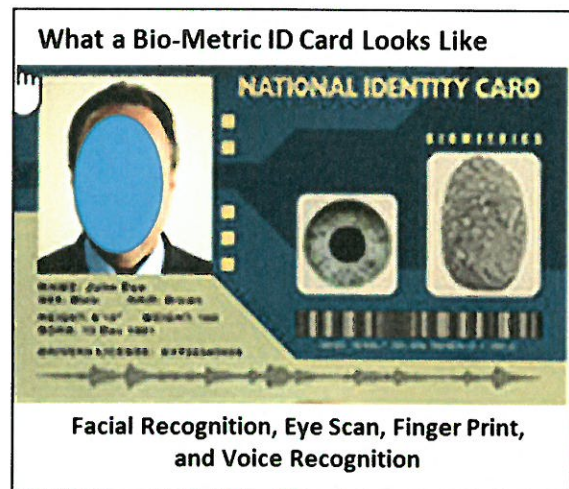
5. The individual's Smart Card Contact information would be used to populate their data base "Parent" record, while the individual's bio-metric information is stored as a Child Record. You could also have Cousin Records that are associated with a Child Record but not a parent (think "Known Associates"). Having a Parent / Child record relationship will allow the addition of information to the individual's identification that could be generated by other government offices and examined without knowing who the information belongs to unless a match is made that would grant legal access through a court order or approved process).

6. Stage four is when the Bio-Metric information has been verified locally and validated through remote systems (like Motor Vehicles Driver License ID System, Criminal Records maintained by the “Department of Defense” (DoD), “Department of Justice” (DoJ), or CIA/FBI, Voting Activity for current election and past archives, or any other system needed to fully Vet an individual). At that time it is safe to generate a Bio-Metric based individual Smart Card Personal ID and store the individual’s bio-metric information on the Smart Card chip. A safeguard associated with this process would be to deny a Voter ID Smart Card to Felons who are not allowed to vote by law. Other warning flags, or restrictions associated with this individual (no-fly list, civil warrant, traffic tickets, etc.) can be accumulated over time and related to the individual as a Child Record, which would be displayed if the card is scanned by law enforcement or within a vetting process.

7. Once the individual is totally vetted, an Identification card will be generated, laminated, and provided to the applicant. On the Haitian *eCARD*, the department the voter’s represent and a color code for the department will be displayed as well. This entire process can take as little as 30 minutes, but will probably take longer in the beginning due to a learning curve and equipment weaknesses.

What an *eCARD* looks like

The *eCARD* contains the individual’s picture, finger print, eye scan, finger print, and voice print – along with any other information your organization deems necessary. The information contained within the *eCARD* chip can be compared against locally read scan information and a actions taken if a match, or non-match, condition arises.



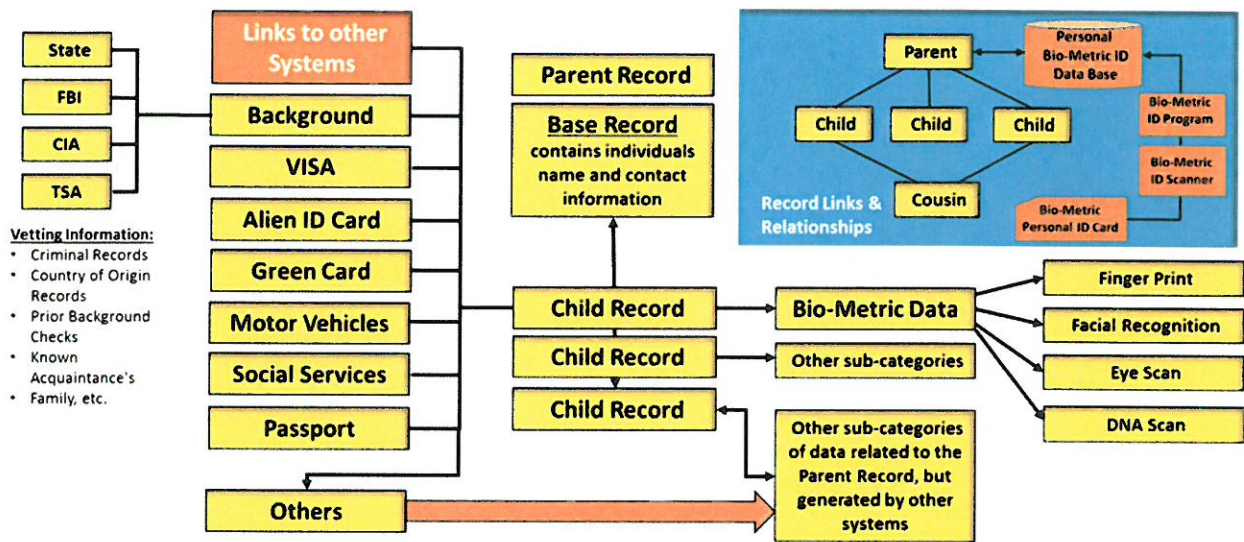
Our Data Base structure

The Data Base Relationship looks like the picture below. As you can see, other systems can link to the Individuals Child Record to scan Bio-Metric information, but not the Parent Record unless a match is made and legal authority granted.

All government and authorized systems can also generate sub-categories of information that can be appended to the Parent Record as Child Records. This is very efficient, because if the individual changes addresses or personal information the change is performed once and all

other systems will have access to the updates so they can use that new information for mailings, emails, and other communication to the person defined in the Parent Record. This one change for many systems approach is most efficient and will result in fewer data entry errors, especially if you have the person represented in the Parent Record perform the update themselves (think Profile maintenance). Changes to an individual's location and status information should also be vetted to insure accuracy and aid in locating the person should they be sought.

The Data Base Relationship



The Cybersecurity Information Sharing Act of 2015 was introduced recently to encourage security information sharing between the government and private sector in order to grow and improve security information availability and better protect private and public sector enterprises. This law could be the foundation for pursuing the recommendations stated within this document.

The Data Base Record structure creates a Parent Record that links Child Records and even Cousin Records into a Relationships (Blue Box Below) showing the Parent, Child, and even a Cousin Record that could be used to identify associates. The Data Base is generated, read, maintained, and deleted through the Bio-Metric ID Program, and remote access to authorized individuals would be via a Bio-Metric Scanner that reads the Bio-Metric Personal ID Card while it is inserted in the Bio-Metric ID Scanner (the card remains in the scanner until the operation is completed, thereby guarantying apprehension of violator or disablement of the Smart Card so it could not be used to commit further crimes or violations).

Now that we have the person's identity and location, along with a range of status information, it will be easier to locate and track individuals should the need arise. This system provides law enforcement with a very strong tool, especially with the aid of GPS information transmitted via the card's chip and the documentation that can be generated to support prosecution.

The identification process would be to insert the Bio-Metric Personal ID Card into a Bio-Metric ID Scanner that is connected to the Bio-Metric Program, which can access the Personal Bio-Metric Data Base (see above picture – upper right blue box diagram). The Bio-Metric ID Program would search the Child Records for anomalies, the Cousin Records for Associates, and eventually the Parent Record for identification should it be warranted. This process would produce an all clear, warning, or arrest command to the Law Enforcement Officer on the spot (total elapsed time is in seconds), so that an apprehension can be made if directed.

An electronic voting process

The card holder will find their new card helpful as well, because the new card and chip can be used for all systems linked to it (i.e. voting, motor vehicles, passport, etc.). The smart card will also be able to support local verification and remote validation of individuals wanting to participate in an on-line caucus or other such electoral activity. They could be verified via home scanner or smart cell phone (think finger print scanner on an iPhone) and allowed to submit their ballot in a caucus. Once submitted the individual would be entered into a "Chat Room" associated with the candidate they submitted their ballot for (say Donald Trump). In the Chat Room, the individual would respond to questions and try to sway others to agree on points they would use to justify their vote for the candidate. After the Chat Room session is completed, people agree on the candidate and supportive information, they submit their vote (everyone's name and contact information is already known from their Voter ID Smart Card without the need of a paper ballot). Their results are added to the results from all Chat Rooms for a candidate, along with their points about why their candidate is the best person to elect. Now is when the caucus starts, because the Chat Room totals and points of justification are submitted to the other side's chat room results and a discussion is conducted electronically until the final voting is completed.

This process would be very easy to accomplish from the comfort of an individual's home, without clogging roads and potentially getting into a car accident. Also, telecommuting has become common place so why not take advantage of it. No problems with running out of ballots, because they are electronically generated. The ballots are completed on-line so they are easily readable. They could even be translated from one language to another (for example from English to Spanish or Chinese).

Once this process has been completed and the final votes submitted, the tally could be calculated in seconds (near real-time) and made public. Of course, checks and balances can be applied to the voting process, but you would never see people rushing into a caucus and submitting recently printed pieces of white paper (instead of blue for example) into a box for counting – no verification needed and so easy to commit fraud / corruption.

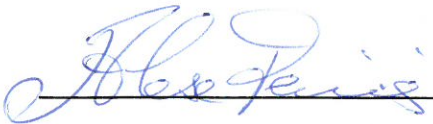
As you can see, my basic premise is that we have the technology today to address these problems and more. As we accumulate safeguarded information we can better detect fraud, corruption, terrorism, criminal activities, and illegal aliens and many more illegal activities – while protecting people better.

If a “Cashless Society” was created, where transactions were performed via Smart Card, it would be so easy to spot fraud and eliminate identity theft that the reluctance from the population for using this technology would be reduced to a point of virtual elimination. The Patriot Act and Dodd Frank would be satisfied easily through this process as well as the Sarbanes Oxley Act (SOX).

Alex and I are strong and loyal supporters of free elections who have accumulated a lot of knowledge throughout our combined 60+ years of experience in Information Technology (IT). We believe this approach could be of value to protect the population and society of Haiti and we are offering our services in any way that could help. JASTGAR would be happy to discuss your needs and we look forward to meeting with you.

We welcome all comments and recommendations for improvement and can be reached via the email addresses listed below our name.

Sincerely,



Alex St-Gardien Jecrois

President & CEO

Email: AJecrois@hotmail.com



Thomas Bronack

EVP & Chief Information Officer

Email: bronackt@gmail.com