To The Honorable Minister of ICT

and

To The Project Manager
Mauritius National Identity Scheme

20 June 2014

Dear Sir,

I am Ish Sookun, systems engineer by profession and a Linux enthusiast. In my free time, I cheer for Open Standards and I create Free Software & Open Source awareness in Mauritius. Recently, I came across some pertinent security issues on the MNIC website. I won't go into details as I hope you have been up to date with media.

This letter is about some more security flaws that once again raise doubts over data security.

Let's talk of Government e-Services first. How will they work? I guess like the current system. A citizen creates an account on the Government Web Portal and he/she can submit applications & relevant documents to various ministries. So, what do I need to create an account on the web portal? A name & an ID number. There is no verification process through phone call or SMS service to confirm if the person is genuinely creating an account. Is this really a flaw? Let's see.

Some time back I did a whistleblow regarding a spreadsheet containing over 9,000 names, addresses, identity card numbers etc, which was available on a government owned website. Do you have a mechanism to identify if someone just went ahead creating 9,000 accounts on the government portal using that spreadsheet? Sadly, you would not identify that.

Let's say an individual having over 9,000 different accounts on the government portal still appears a small problem. I give you another scenario so you may realise the size of this issue. Say the person holding the accounts decide to make an application through a ministry and he/she uploads forged documents to cause prejudice to the owner of that ID. Upon discovery of the same, who will be liable? The person in whose name the account is used isn't even aware of that & yet officials could embark him/her for questioning.

During my observation on the said website something else came persistently in my mind. Why the domain gov-mu.org was used? Is it because gov.mu isn't DNSSEC signed & it was easier to get a .org domain signed. This might have solved the DNSSEC issue but other ethical issues crop up. Several other domain names that come very close to gov-mu.org are available for registration & it's just a matter of time since "scammers" will take advantage of this and create fake websites for data mining, such as getting login credentials. Thinking of how they may tempt people into visiting those websites? Well, we might have a look at another security flaw here.

Currently, mail.gov.mu isn't equiped with SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) which are mechanisms that help in fighting email forgery. To say, someone can easily send out a forged email with @mail.gov.mu extension, the email is delivered to the victim's inbox & the latter is presented a beautifully crafted email talking of "reforms etc". The person is then tempted to click on a colorful download button, asked to log in (page which resides on a similar to gov-mu.org domain) & yes a

PDF is downloaded. Everything looks innocent. Everyone is happy! The poor victim gets a PDF that talks of “reforms” & the attacker gets the victim’s “login credentials”. DNSSEC is important for gov.mu, SPF & DKIM are good practices to fight email forgery and gov-mu.org is very bad for the government’s health.

Since we’re talking of good practices, please consider correcting the DNS settings for gov.mu. It points to nowhere. Only www.gov.mu is configured & that has been the case since years. More on good practices; although the Government servers have been patched against Heartbleed since a month, no email was sent out to alert public of the dangers of Heartbleed & advise them to change their password. I changed mine & advised folks to do the same. Sadly, I was hoping for the authorities of the Cyber Island & would-be Smart Island to do it.

Let’s talk of the MNIS project now. I wish to have my new Identity Card & my folks are waiting for the same but we need answers first. Why are you collecting fingerprints & biometric photo? Initially I learned it was to “prevent” identity theft. I was made aware that the ID Card will suffice to just go to a bank & open an account. I raised doubts over data verification between the bank & the MNIS servers. Then in a recent press conference by the project manager I came to understand that the database containing all biometric data will be offline. So, if someone goes to a bank with a forged ID Card containing a chip with fake elements, there won’t be a real-time mechanism to compare the data against the MNIS database. So much to say that the biometric data will be available only to investigate identity thefts that “surface” rather than fighting identity thefts in real-time. Is it worth it? You can’t fight identity thefts if the data isn’t used in real-time for cross-verification and using that in real-time raises a lot of security doubts. Please keep an Identity Card as an Identity Card and don’t make a one-key-for-all. Several countries have backed down over the security issues surrounding a “centralized” database, which you’re doing with the “Central Population Database”. I won’t go into the various scenarios that can compromise the Central Population Database.

I understand you have put your trust in a country’s “proven” expertise but sadly, those consultants might not be fully aware of our culture. Each country has a distinct set of “habits” when it comes to good practices & malpractices. We have our known. Simply putting a solution that has worked elsewhere doesn’t just “work”. It has to be adapted to the local context.

As I highlighted in previous articles, use of Google Form (cloud service), un-sanitized SQL, poor code quality and non-standard elements on the MNIC website. Then there is the major privacy blunder leaking over 9,000 names & ID Card numbers. We see emails can be forged. I didn’t elaborate on other aspects but you currently have dozens of mis-configured sub-domains on the Sharepoint. Every now & then when I click on a Gov URL and it redirects me to configuration errors I become doubtful of the capacity to safeguard biometric information. So much to say we have a lot of malpractices going around.

I saw several animated characters on the MNIS Facebook page trying to educate people about the “benefits” of the Biometric ID Card. Please stop doing that, it’s irritating. I am tempted to publish more on the security flaws each time you “tempt” the innocent citizens in doing something unethical.

The MNIC website say the following regarding info that will be stored in the NIC chip:

“The only data that will be stored in the chip is strictly that which is specified on the technical data sheet.”

However, there is no link to the “technical data sheet” from the MNIC website. As a citizen whose data is being asked, can I have a look at this sheet?

Moreover, I believe the chip that is mentioned here is an RFID (Radio-frequency Identification) chip that should operate around 13MHz frequency or something similar. Can you assure the population that the information on the chip isn't readable by a DIY antenna (assuming that 13MHz readers aren't sold on the market)?

The MNIC website also states that only the Civil Status will have access to personal data stored on the chip. However, it's being widely publicised that the new ID Card will suffice to open a bank account without carrying additional documents such as proof of address. Are you telling me that the bank official will just look at the card and not read anything from the chip? What about proof of address then?

Our current infrastructure is unhealthy, it's more important to invest in fixing those, rather than doing campaigns for Biometric collection which you say you will use only for identity theft investigation.

I wish I could talk more but sadly, I have to keep this letter short. I'll be glad to discuss more on the security aspects over a cup of coffee as I still have tons of doubts over the need of a biometric ID Card instead of a simple yet modern ID Card.

I am a proud Mauritian, a free citizen of the Republic of Mauritius. No authority can deny me an Identity Card. I want my ID Card before 15 September 2014 but I won't give my fingerprint and biometric photo for just identity theft verification. Those can be done by investigation agencies when an identity fraud is reported. Giving you biometric data to store in a database surrounded by poor security & malpractices at every level is absurd.

Just as the Government is thinking long-term with respect to modernization, I am a citizen who is thinking long-term keeping in mind privacy & security.

Cheers!

…….
Ish Sookun
Proudly, a Mauritian.

This letter has been sent to the Hon. Minister of ICT, to the Project Manager of MNIS and a copy is kept on hacklog.in for the citizens of Mauritius to access.