St. Vincent and the Grenadines

E-Government System Development Planning and Consultancy Services

St. Vincent and the Grenadines e-Government Network Services Strategy Plan (V1.01)

17 May, 2012

Prepared By

International Integrated Systems, Inc., Taiwan

iisi International Integrated Systems Inc.

Supervised by Taiwan International Cooperation and Development Fund (ICDF)

TAIWAN ICDF

Revision Log

Version	Date	Revision	Author
V0.90	9 May, 2012	Initial release	SJ Tu Jerry Wang
V1.00	12 May, 2012	1st Distribution for Client	SJ Tu Jerry Wang
V1.01	17 May, 2012	Modified by ICDF's comments	SJ Tu Jerry Wang

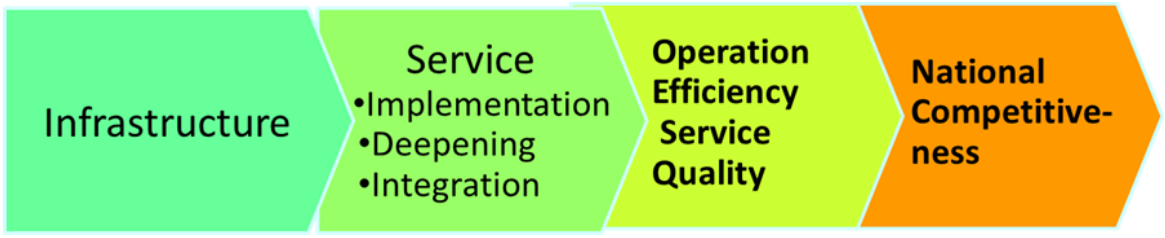
Table of Content

1. Foreword

'This report is an extension of the "St. Vincent and the Grenadines E-Government Development Strategy Plan Report" (e-Gov Service Strategy Report for short) and focuses on the network infrastructure and services. The reader is suggested to view the "St. Vincent and the Grenadines E-Government Development Strategy Plan" in advance to have an overview and understand the connection of these two reports.'

In the e-Gov Strategy Report, we had the definition of E-Government as "utilizing the internet and the world-wide-web for delivering government information and services to citizens". *(From the Benchmarking E-government: A Global Perspective, United Nations – DPEPA, 2002)* The implied meaning of "e" is "on-line" or any other ICT technologies and these technologies help government to offer information and services through Internet or other channels. It also means citizens can acquire government information, submit government service application or pay government fees on-line. In order to offer on-line services to citizen, government has to ensure the network readiness is well for e-Government services delivering.

Referring to the e-Government development history of advanced countries; all of countries start e-Government development from the network infrastructure construction as the basis. The network infrastructure is not only network construction, Internet access but also includes the identification and information security issues.



In the "e-Gov Service Strategy Report", the global e-Government development trends now are identified as the follows.

- Online Service Delivery
- Online Service Integration & Citizen-Centric Design
- e-Participation
- Public Sector Interoperability
- Multichannel Service Delivery
- Bridging Digital Gap

In order to realize these e-Government global trends, it is necessary for SVG government to build a robust network and network services. The purpose of this report is to recommend the network services which should be developed in SVG in the future.

2. The essence of e-Government Network Services

2.1 E-Government Development Framework

According to the five e-Government development levels defined by United Nation, we can divide e-Government development into five layers as the following.

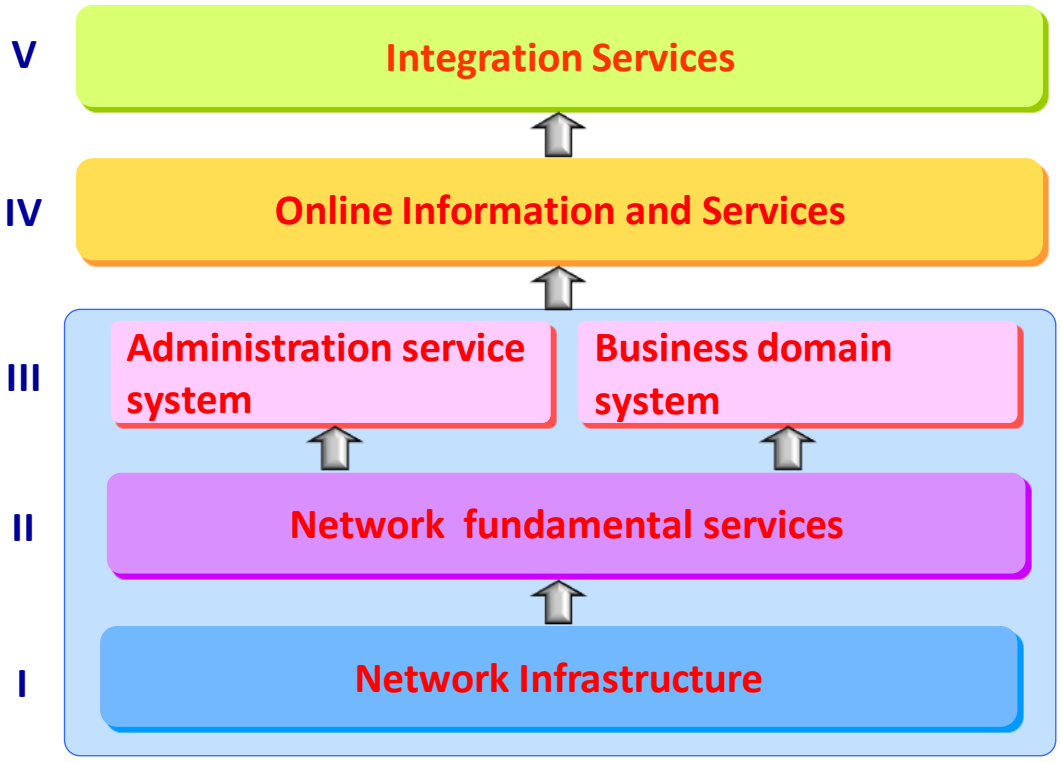
(1) Network infrastructure.

(2) Network fundamental services

(3) Application system, include: administration service system and business domain system

(4) Online information and services

(5) Integration services



The meaning of item I to item V is to develop the network infrastructure and network fundamental services first. Based on the network infrastructure and services, government can develop different application systems and transform the system functions to on-line services. Finally, government can integrate related individual services to be an integrated service for the citizens and other users. The descriptions of the e-Government services are summarized in the “e-Government Service Strategy Plan” report and we will focus on the Network infrastructure and Network fundamental services in this Network Service report.

2.2 SVG e-Government Shared Infrastructure

In the SVG Information and Communication Technology Strategy and Action Plan 2010- 2015 report, it mentioned *"The e-Government Programme aims to provide a shared technology infrastructure that is stable and secure and which embraces a set of policies and standards for the connection to and use of this shared infrastructure*" The e-Government development is expected to provide the services such as:

- Domain management
- Security and intrusion protection
- Virtual private networks
- Firewalls
- Physical connectivity between government locations.

The shared infrastructure will enable the provision and management of shared services such as email, Internet, Intranet, Voice over IP, collocation of servers, application hosting and SAN facilities. The challenge will be for the government of SVG to re-organize itself to take advantage of the enabling technology to improve its business processes and its service delivery model to its businesses and citizens.

In order to make the suitable suggestions on infrastructure for SVG Government, Consultant will provide related suggestion in this report based on the definition of SVG Government's plan and expectation.

2.3 Network Services Framework

E-Government network services should be a supporting mechanism for e-Government development and e-Government system operation. Government has to utilize the network services to fulfill e-Government services delivery. The essential of e-Government network services will include:

(1) Network:

Government has to provide physical connectivity between government agencies.

(2) Access:

Government employee can access to the government network, include fix line and wireless access.

(3) Data center:

Government should establish a data center to locate e-Government system servers and data.

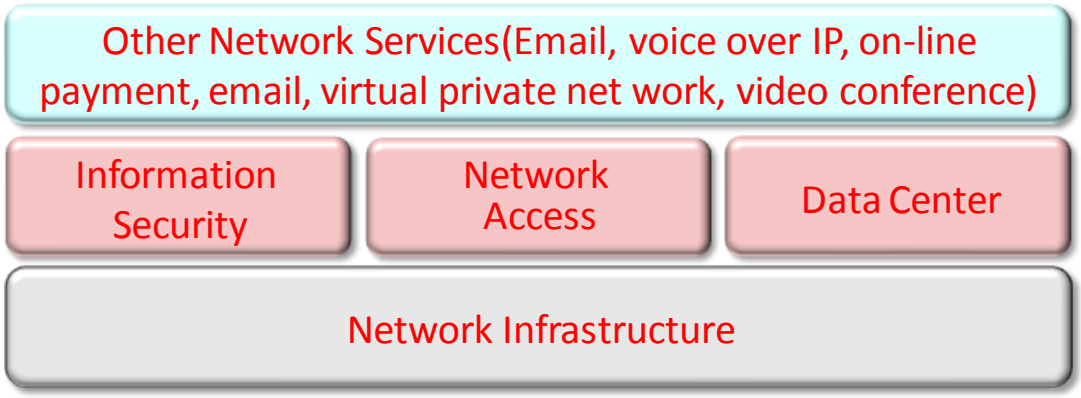
(4) Information security:

In order to ensure the integrity, confidentiality, accountability, non-repudiation, e-Government has to establish information security mechanism for on-line services and on-line transaction.

(5) Other network services

Email, voice over IP, on-line payment, email, virtual private network, video conference… etc.

The framework of network services is as the following figure.



3. SVG network services strategies

3.1 Current State of SVG Network Services

According to the essence of network services, Consultant reviewed and summarized the current state of SVG network services as follows:

(1) Physical connectivity between of government agencies:

SVG has already built government fiber network to connect each government agency. Almost all government buildings in Kingstown are connected with fiber and connectivity scope is continuously extended. For example, to extend fiber network connectivity to airport, school etc. The government network infrastructure is almost completed in SVG.

(2) Network access of government employee:

In current network infrastructure, government employees can access to the government network in their office. The government network to internet outbound is “Old Telecom Building”. All internet access has to pass through the “Old Telecom building”. There is no government outdoor wireless access solution in SVG.

(3) Data center:

SVG has already built the data center in Information Technology Service Department (ITSD). SVG national portal and most of government systems are co-located in ITSD. In November 2010, an ICT cooperation agreement was signed by the governments of SVG and the Republic of China (Taiwan). Taiwan government will provide assistance with the establishment of state-of-the-art ICT centre. This centre will be the e-Government centre of SVG and will work with ITSD data centre. All the systems which are developed in this ICT cooperation project will be located in this ICT centre.

(4) Information security:

Currently, there is no enough information security mechanism for on-line services and on-line transaction in SVG. The EGRIP now start to discuss the PKI in the regional meeting. However, the plan and the implementation of government PKI are not defined yet.

(5) Other network services

For some other network services’ current situation are as follows.

- Email: SVG has already built government email system.
- Voice over IP: ITSD has built up VOIP system. Most of user use softphone system.

- On-line payment: SVG doesn't have on-line payment system yet.
- Virtual private network: Government agencies are connected with fiber. That means all government agencies are in government intranet. Government agencies don't need to connect other one through internet. All government agencies are in government private network.
- Video conference: SVG doesn't have video conference system for government internal use now. There are some equipments for regional meetings only.

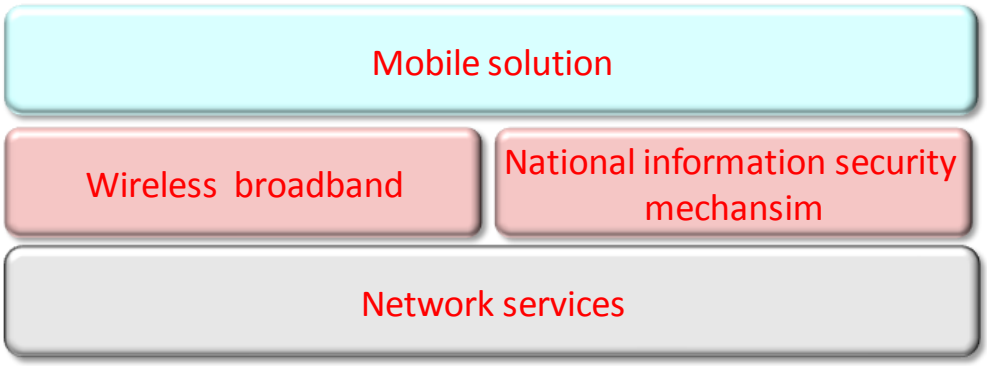
The summary of network services assessment is as following table:

Item	Assessment	Suggestion
Network	・Connectivity between government is ready, ・Continuously extend to other agencies	Use fiber or wireless solution to extend to other agencies
Network access	・Access in office is ready	Implement outdoor wireless access solution
Data center	・It's ready	Need to build disaster recovery center
Information security	・It's not ready	Implement PKI mechanism

3.2 Network Services Development Strategies

Base on the current state assessment summary in the last section, there are three (3) strategies for network service development in the future.

1. Use state-of-the-art wireless broadband technology to extent government network connectivity and government network access.
2. Build SVG national information security mechanism to ensure the safety of on-line services and on-line transaction.
3. Implement mobile solution in e-Government services based on the wireless network connections



According to the strategies above, Consultant identified the five (5) initiatives of network infrastructure and service as follows.

- WiMax Network Initiative
- Disaster Recovery Center Initiative
- Public Key Infrastructure (PKI) Initiative
- ISMS Consultancy Initiative
- Mobile Initiative (Mobile solutions for VOIP, police force, disaster mitigation etc.)

4. Network Services Initiative

4.1 WiMax Network Initiative

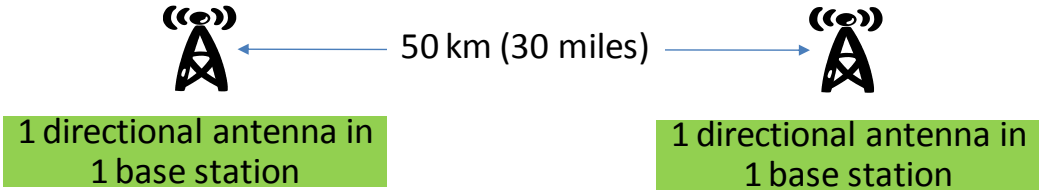
4.1.1 WiMax Features

WiMax is one of the 4th Generation (4G) communication technologies and it's widely used in the worldwide. The features in terms of bandwidth, coverage, subscribe users of WiMax are as following description.

1. WiMax bandwidth: 70 Mbps. (10 times of 3G communication)
2. Coverage: there are two kinds of access models and the corresponding coverage is as follows.

(1) Peer to Peer Connection: 50km (about 30 miles)

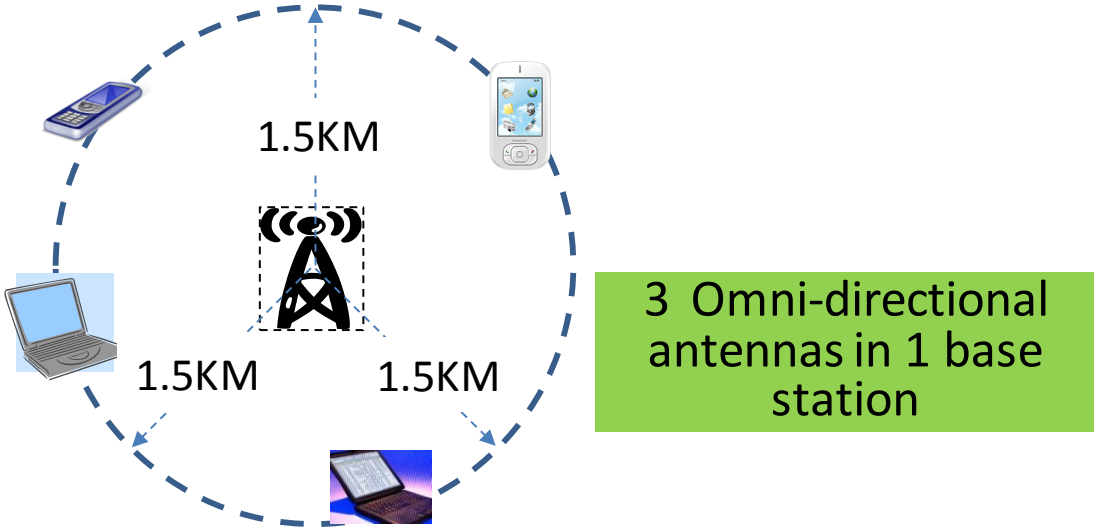
- It's to use WiMax as a backbone network. The coverage between 2 WiMax base stations is 50 km (about 30 miles)
- In peer to peer scenario, if one site wants to connect to another site with WiMax, it is necessary to build at least 2 base stations for connectivity.
- One base station needs to install one directional antenna to connect to another one.



(2) Access Service:

It means to use WiMax as a wireless access point for mobile terminals, the coverage (service area) around one base station is as follows.

- Urban: the radius is about 1 km ~ 1.5 km (0.625 mile ~ 0.938 mile)
- Suburban: the radius is about 1.5 km(0.938 mile)
- In access service scenario, if government wants to provide wireless service to government employees, it is necessary to build at least 1 base station. This base station has to connect to government network and link to internet.
- The base station needs to install three omni-directional antennas to fully cover the scope and provide access service.



3. Maximum subscribe users for access service for one base station

(1)Bandwidth of 1 base station: 70Mbps

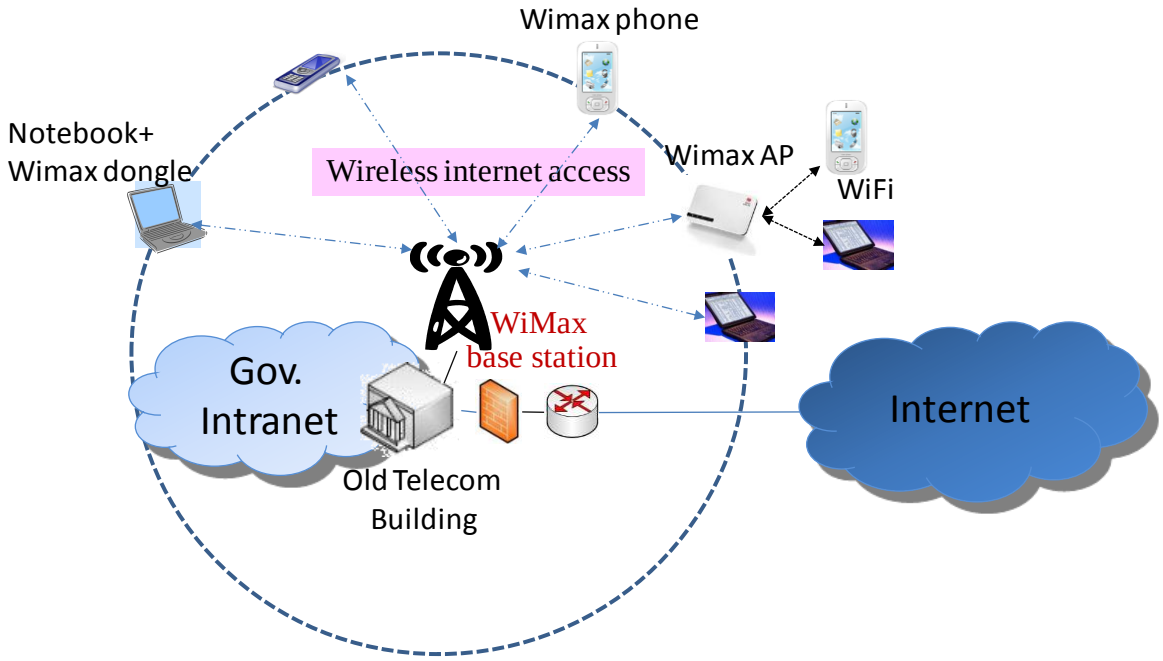
(2)Assumption and estimation:

- Maximum allocate bandwidth of 1 user: 1 Mbps
- Maximum concurrent users:
  70 Mbps/ 1 Mbps-per user = 70 users
- Total subscribe users of 1 base station in operation are estimated as follows.
  70*20=1,400 users (20 is the experience parameter of subscribe user calculation)

It means in access service scenario, the maximum subscribe user in one base station service area is 1,400. If the subscription users in this area are over 1,400, it needs to establish another base station for better access quality.

4.1.2 WiMax Construction for Government Internet Access Service

According to the WiMax access service feature which is described in section 4.1.1. We can use WiMax to provide wireless internet/intranet access services in Kingstown. The WiMax infrastructure for wireless internet/intranet services is as following figure.



(1) Establish one WiMax access service base station in Kingstown. The location of this base station should be near by the internet outbound. (ITSD/ Old Telecom building)

(2) The base station will connect to SVG government network.

(3) Users can use WiMax access devices (notebook + WiMax dongle, WiMax phone or WiMax access point box) to access WiMax signal and connect to SVG government network.

(4) If users want access intranet service, the access will be routed to SVG intranet. If users want access internet service, the access will follow current internet outbound routing to access internet service.

(5) Users can also use WiMax access point box to access to SVG government network. The signal between WiMax access point box and the WiMax base station is WiMax but the box transfers the signal between the box to terminal devices (notebook, smart phone etc.) to Wi-Fi. That means the users can use the current Wi-Fi devices without buying new one.

(6) In the first step, it's suggested to establish one access service base station. It can provide 1,400 subscribe users. That will be around 30% of government employee in Kingstown. In the second step, SVG government can establish another access service base station. They can provide 2,800 subscribe users. That will be around 60% of government employees in Kingstown. Finally, SVG government can evaluate the usage and loading to decide if it's necessary to establish other access service base stations.

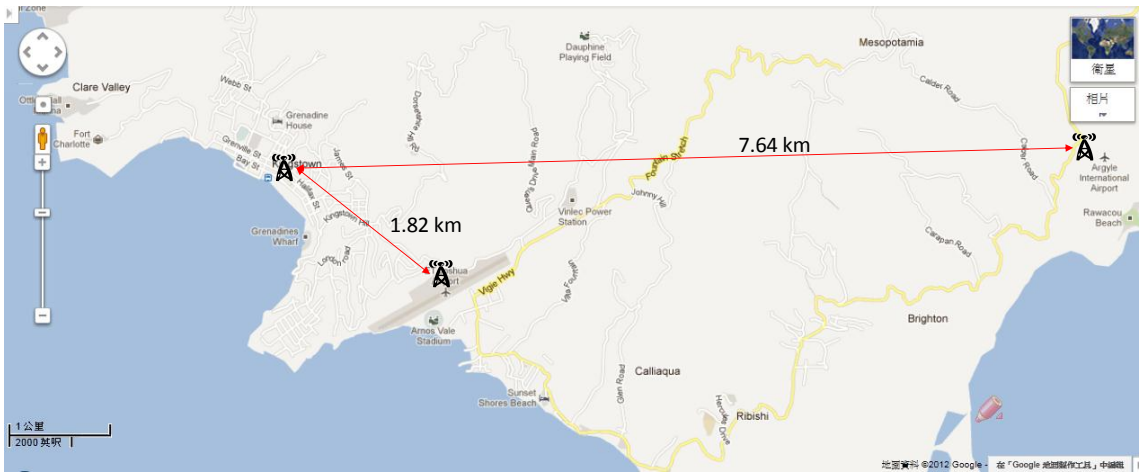
(7) The estimated access service coverage of WiMax in Kingstown is as following figure.

4.1.3 WiMax Construction for Government Agencies Connectivity

(1) Connect to other agencies in St. Vincent

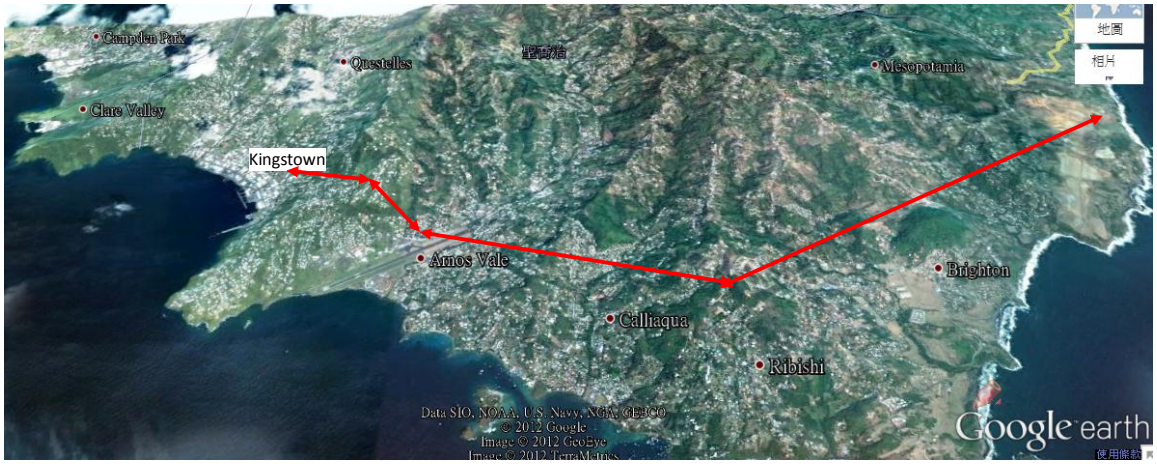
SVG government network is planning to connect to ET Joshua Airport and to Argyle international Airport (the new airport). The peer to peer WiMax backbone can be establish for connectivity.

The linear distance between Kingstown and ET Joshua Airport is around 1.82 km; between Kingstown and Argyle international Airport is around 7.64 km. Both of them are within the coverage of WiMax peer to peer base station.



Due the mountain between will block WiMax signal. It is necessary to establish some transit stations between 2 base stations. The accurate location of base stations, transit stations will be decided after real site survey.

We can use the sample approach to use WiMax to connect to other city in St. Vincent.



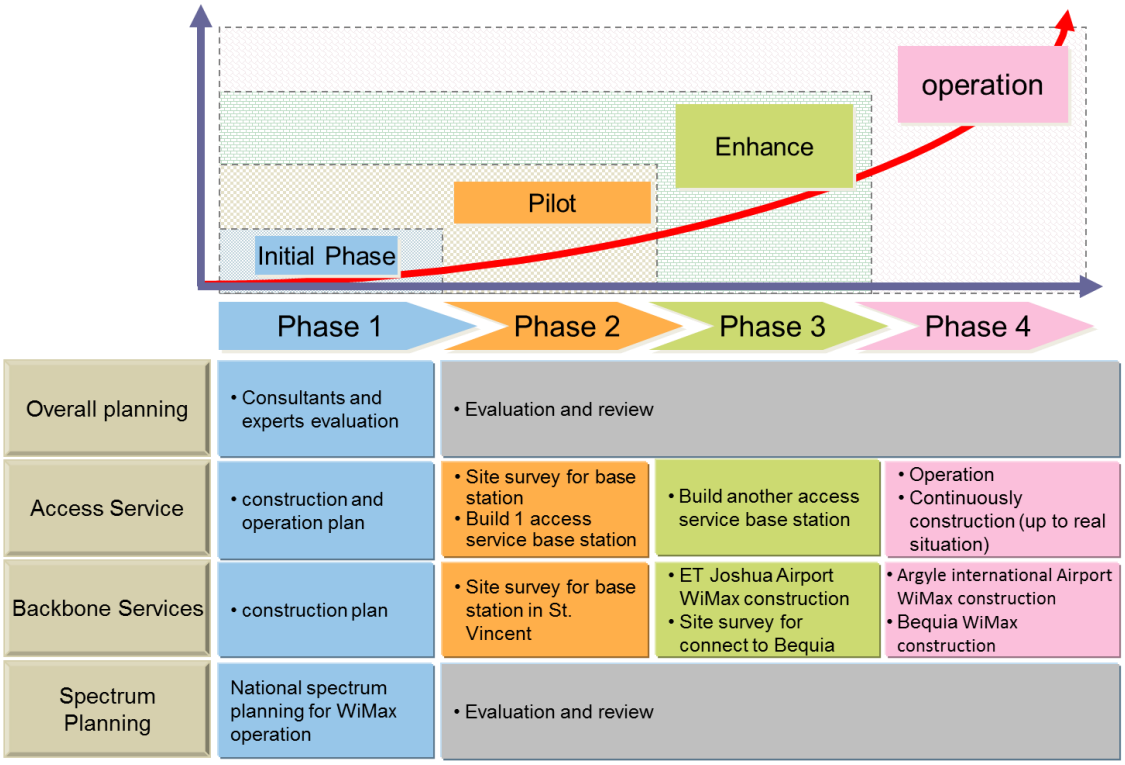
(2) Connect to the Grenadines

The WiMax solution also can be used to connect to The Grenadine. (For example, Bequia Island) There is a government agency building - Bequia Revenue Office in In Bequia Island, and Customs & port, Post office, Inland Revenue, Immigration, Registry, Treasury are locate in the same building. The linear distance between St. Vincent and Bequia Island is around 14 km. It is also within the coverage between 2 WiMax base stations. The WiMax base station can be established to connect 2 islands.

Of course, the accurate location of base stations, transit stations (if necessary) will be decided after real site survey.

4.1.4 Schedule of WiMax construction project

As we mentioned in the previous sections, WiMax construction includes two kinds of scenarios - one is access services and the other is backbone connection. These two scenarios should be considered together and the overall planning and real site survey are necessary for WiMax construction. The proposed implement schedule and tasks for each phase are as follows.



4.2 Disaster Recovery Center Initiative

Disaster recovery means to restart or recover the system, data, software configurations and hardware to continue the business or service providing after a natural or human-induced disaster. The disaster recovery plan is the process, policies and procedures to prepare the disaster recovery and disaster recovery center is one of the most important components in the plan. In another words, disaster recovery is one of key components of e-Government services continuity. Based on the different levels of backup and recovery time, the disaster recovery center is usually identified as the following types.

Hot Sites

A hot site is a duplicate of the original site, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites is used to completely mirror the data environment of the original site through

WAN or fiber. When a disaster happens, the hot site can quickly start with minimal losses to normal operations. The capacity of the hot site can be same as the capacity of the original site or not depending on the organization's requirements. Hot backup sites have a virtual mirror image of the original data center and can often be brought up to full production in no more than a few hours. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies and e-Commerce providers.

Cold Sites

A cold site does not include backed up data and information from the original site or the set up hardware. The lack of hardware results to the minimal costs of the cold site, but requires additional time after the disaster to have the operation running at a capacity close to the original one. A cold backup site is little more than an appropriately configured space in a building and it’s the most inexpensive type of disaster recovery center to operate.

Warm Sites

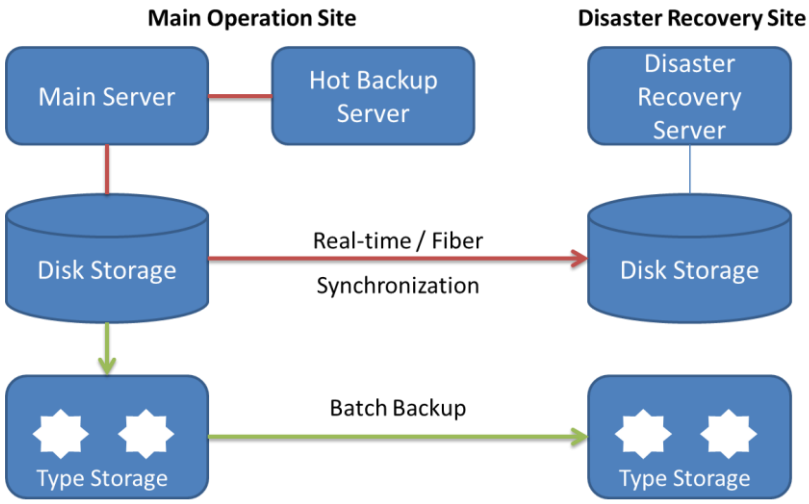
A warm site is the compromise between hot site and cold site.

These sites will be allocated hardware and connectivity, with the smaller scale as the original site. Warm sites have backup data, but they may not be complete and may be several days and a week old. An example would be backup tapes sent to the warm site by courier. To restore service, the last backups from storage facility must be restored before the real recovery of the service

Due to ITSD and e-Government center are both IDC center. These two sites can be the disaster center to each other and a remote recovery center outside of Kingstown is also expected in the future.

Because the e-Government center will be established on Aug. 2012, the schedule of disaster recovery center will be proposed to start to plan on 2013 and establish on 2014.

For the disaster recovery center, the site selection, system coverage, expected recovery time, backup architecture are all the issues to be planned. It’s suggested SVG government to start the plan in the future. One of the examples of the disaster recovery site architecture is as follows.



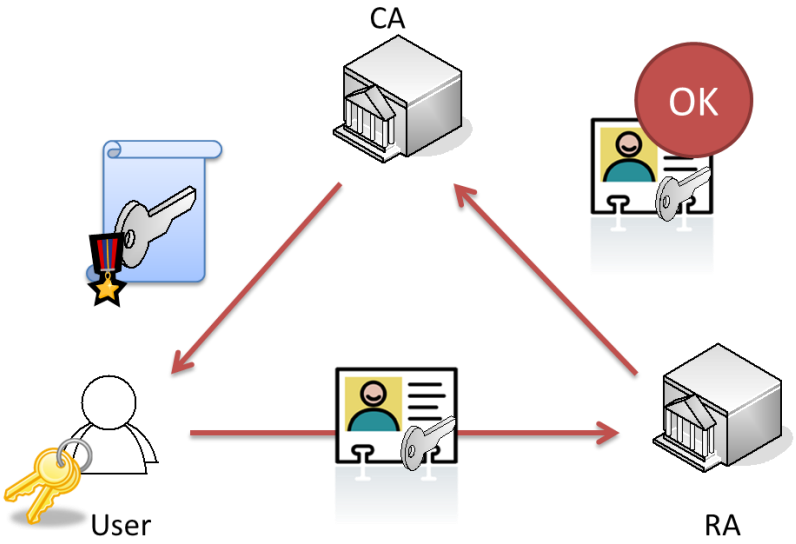
Besides the disaster recovery, there are some suggestions for the e-Government Center. As the SVG government agencies are mostly located in Kingstown and the distributions are not separated far away from the e-Government Center, the e-Government Center is suitable to act as the shared data center in government field. Hence, it's also suggested the e-Government Center can extend the services with cloud technologies as a G-Cloud Data Center. For the cloud services, one popular example in the market is the cloud storage such as the "Dropbox" or "Google Drive" services. If this kind online storage service is deployed in the e-Government Center, it can support government employees to storage, share and manage their data in the cloud instead of using the traditional flash-disk which usually cause the security issues because of losing the device. It can also support different devices to access the data and increase the work efficiency in government field.

4.3 National Public Key Infrastructure Initiative

4.3.1 PKI Promotion

A public-key infrastructure (PKI) is a set of hardware, software, roles, policies, and procedures to create, manage, distribute, use, store, and revoke digital certificates. The government field PKI is usually called GPKI.

The two major roles in PKI are Certificate Authority (CA) and Registration Authority (RA). The CA binds the person and his/her public keys and the user identity must be unique within each CA domain. The binding is established through the registration and issuance process. The role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation. The scenario is following figure.



In order to promote e-Government online application and online services, the government has to provide the mechanisms to ensure the information on-line are secure and to identify the users. The essential of information security includes:

1. Confidentiality: Only authorized person can encryption information
2. Integrity: Ensure accuracy of information
3. Accountability: Ensure the activity of entity is traceable.
4. Non-repudiation: Can't deny the fact of happened activity.
5. Authentication: To avoid someone disguise your identity
6. Access control: Only authorized person can access system

PKI mechanism can meet the above requirements of information security.

Government should establish national PKI mechanism and form a task force to promote government e-certificate. The task will include:

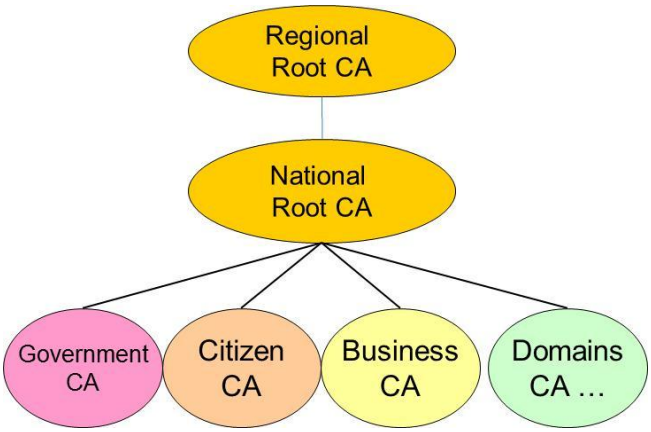
1. GPKI overall planning
   (1)Formulate government e-certificate policy and operation standard.
   (2)Formulate government e-certificate technical standard
   (3)Formulate the structure of government e-certificate system
2. Establish government certificate center
   (1)H/W installation
   (2)PKI solution evaluation (source review and inspection)

(3)Certificate standardization

(4)System establishment

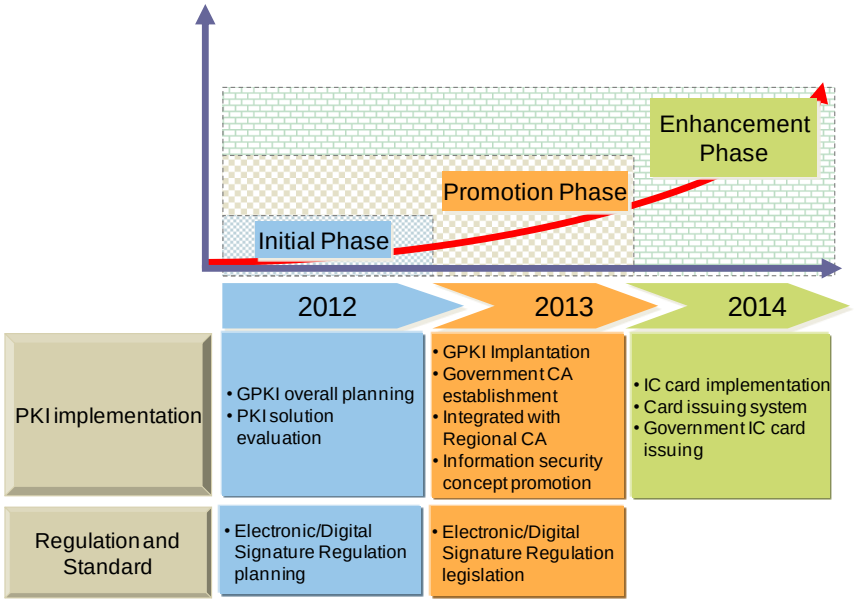
(5)Certificate issuing and application

For PKI promotion, the regional organization is stating the meetings to discuss the PKI development. As a member of the regional organization, the regional strategies and standards must be followed but the national GPKI structure could be designed by SVG's environment and requirements.



4.3.2 Schedule of PKI

WiMax construction should include 2 scenarios: access services and backbone. Overall planning and real site survey are necessary for WiMax construction. The implement task for each year is as following:



4.4 ISMS Consultancy Initiative

In order to provide a secure IT environment and services, SVG government should invite the consultants or the expert team to develop the Information Security Management System (ISMS for short), including the consultancy initiative and the implementation initiative. In the ISMS consultancy initiative, the main task is planning the information security management system with eleven domains, including

(1) Security Policy

(2) Organization of Information Security

(3) Asset Management

(4) Human Resources Security

(5) Physical and Environmental Security

(6) Communications and Operations Management

(7) Access Control

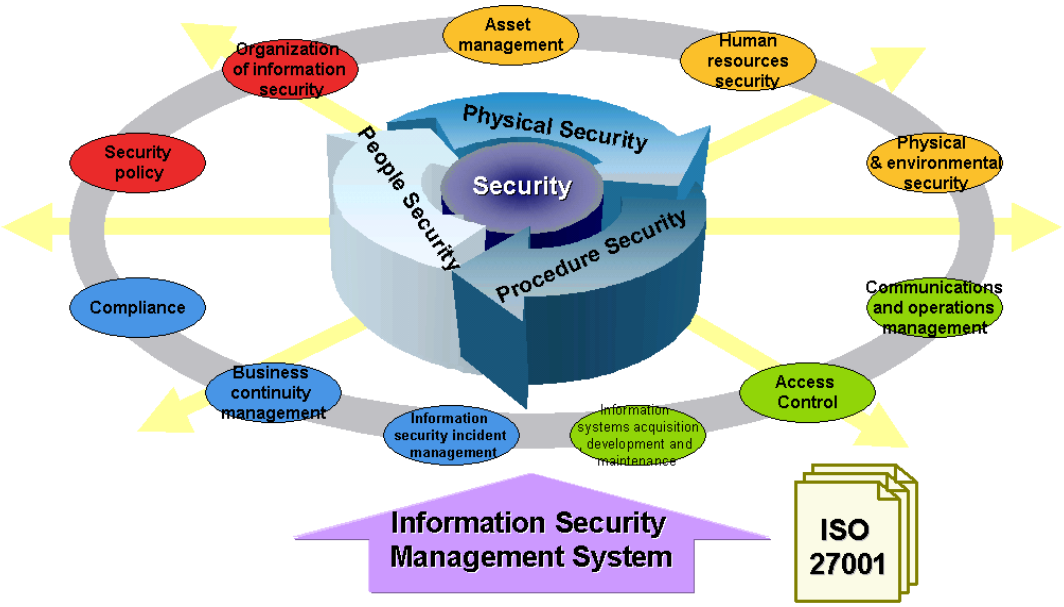
(8) Information Systems Acquisition, Development and Maintenance

(9) Information Security Incident Management

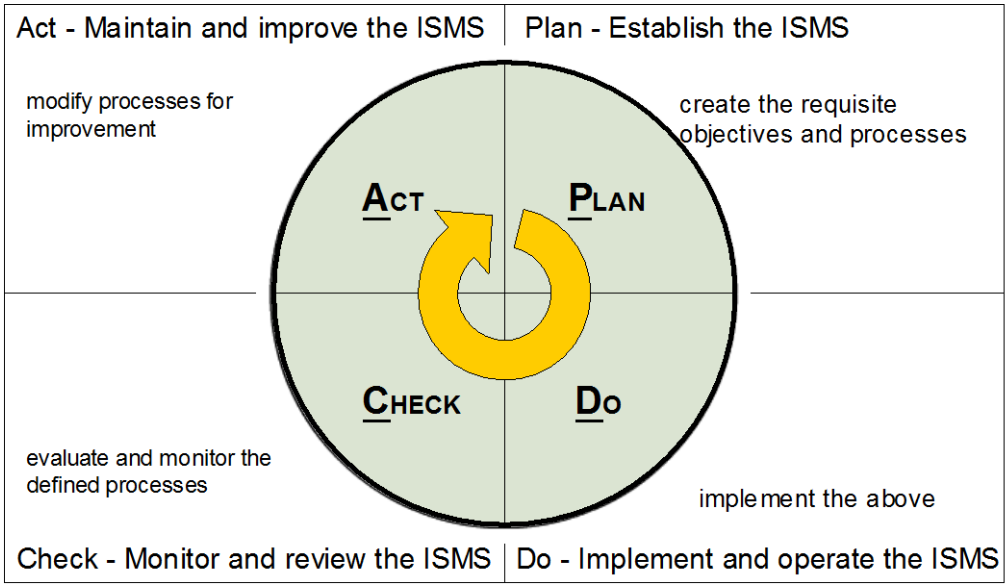
(10) Business Continuity Management

(11) Compliance

Furthermore, those eleven domains should be considered as an integral whole and implement simultaneously. Since the methodology to apply ISMS is defined in ISO 27001 as an international standard.



In the long term, ISMS must adapt to the changes from internal or external environment effectively and efficiently. Therefore, the approach to apply ISO 27001 is a PDCA lifecycle in practice shown as below. These four phases represent “establish the ISMS”, “Implement and operate the ISMS”, “Monitor and review the ISMS” and “Maintain and improve the ISMS” and approach to continuous improvement.



[Schedule]

The ISMS Consultancy project is recommended to start on 2013.

4.5 Mobile Solution and Services Initiative

Mobile solution is highly related with WiMax construction project. SVG will be a wireless broadband country when WiMax construction is completed. Then, it is able to use wireless environment to provide mobile services in SVG, such as the following applications.

Mobile VOIP

Use WiMax smart phone or other WiMax mobile devices to communicate to others with VOIP. It can save a lot of expense for government.

Mobile-Police

In the past, the police cannot easily get information when they are on duty outside. With the WiMax environment, the police can use the WiMax mobile devices

(notebook, PDA, smart phone etc.) to access the backend database anywhere and anytime to check the criminal data, lost car information etc. It can help the police to increase the efficiency and effectiveness and also help to enhance the public safety. Of course, the backend system has to be modified for mobile access. The scenario of the Mobile Police can be imaged as following figure.

Disaster mitigation

The SVG government can use the WiMax network to setup the real-time surveillance camera for disaster data collecting, such as the river water level, rainfall information monitoring, and send those data to the backend system. The collected information can be displayed with the GIS system for easily identifying the situation remotely and send the rescue resource on time. For example, the government officers can remotely watch the real-time image of George Town and make commands in Kingstown. The example of the disaster mitigation application is as following figure.

[Schedule]

WiMax can provide a wireless broadband environment for mobile services development. Due to the mobile services are domain related it needs to develop domain system and then can provide its mobile services. The schedule will depend on the progress of domain system development and would not be described in this report.

5. Conclusion

Network infrastructure is the fundamental of e-Government development. In accordance with the global trend of e-Government development, no matter what kinds of online service are provided, all of them need a robust network infrastructure. For the multichannel service delivery, the mobile devices are also an important channel to access e-government services. It is necessary to build a broadband wireless environment for future development.

Besides the network issue, successful implementation of e-government also depends on the confidence of the public. E-government services must protect the information which is transferred and processed on-line, and ensure the individual privacy. It's also necessary to protect national security. The government must define uniform privacy protection practices and establish information security mechanism. It also must adopt a data encryption/decryption and digital signature standard for sensitive information and on-line transaction.

The purpose of network services initiatives is to support e-Government services development under a well-structure network environment. In the e-government development progress, network services and e-Government domain services are both important for e-Government development. Therefore, the initiatives in this report should be considered together with the initiatives in "St. Vincent and the Grenadines e-Government Development Strategy Plan" and to be the SVG e-Government development master plan in the future.