Ministry of Information,
Communications and Technology

Feel safe online

NATIONAL CYBERSECURITY STRATEGY

2014

Government of Kenya
Ministry of Information Communications
and Technology
Telposta Towers, 10th Floor,
Kenyatta Avenue
Nairobi, Kenya

CONTENT

Message from the Principal Secretary

Global information and communication technology (ICT) growth has transformed how individuals, businesses, and governments produce and receive information. Adoption of ICT into everyday life is widespread in Kenya. The Government of Kenya is proud of this development and is actively encouraging its continued growth through national initiatives such as Kenya's Vision 2030, ICT Master Plan, and the recent deployment of nationwide fiber-optic network infrastructure. Such efforts provide a dramatic increase in interconnectivity among businesses and individuals throughout Kenya. Kenyan public and private sector organizations are now using this increased bandwidth and ICT capabilities to efficiently deliver services, conduct business transactions, and share information across organizational, social, and geographic boundaries.

As Kenya matures into an information society the nation faces an increasingly evolving cyber threat landscape. Nation states, criminal organizations, and hacktivists from all over the world are—and will continue—to exploit ICT vulnerabilities in Kenya. This is simply a reality that every nation with robust ICT infrastructure faces. While these actors seek to illicitly access, alter, disrupt, or destroy sensitive personal, business, and government information, we are working diligently to evolve our means of protecting information in order to counter today's threats as well as those coming from over the horizon.

In response to these threats, and in direct support of the national priorities and ICT goals defined in Vision 2030, Kenya's ICT Ministry developed a National Cybersecurity Strategy. The Strategy defines Kenya's cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures.

The Government of Kenya is committed to the safety, security, and prosperity of our nation and its partners. We see cybersecurity as a key component in that commitment, providing organizations and individuals with increased confidence in online and mobile transactions, encouraging greater foreign investment, and opening a broader set of trade opportunities within the global marketplace. Successful implementation of the strategy will further enable Kenya to achieve its economic and societal goals through a secure online environment for citizens, industry, and foreign partners to conduct business.

Cybersecurity is a shared responsibility. The Government of Kenya will continue to partner with government, private sector, academia, and other non-government entities to implement our Strategy in the most efficient and effective way possible. We have every confidence that we will meet these challenges together and increase recognition of Kenya as a trusted partner and cybersecurity leader in the East African Community (EAC), Africa, and the world.

Joseph Tiampati Ole Musuni

Digitally signed by Joseph Tiampati Ole Musuni
DN: c=KE, o=ICTA, ou=Telposta, cn=Joseph Tiampati Ole Musuni
Date: 2014.06.19 15:09:36 +03'00'

Mr. Joseph Tiampati ole Musuni
Principal Secretary
Ministry of ICT

INTRODUCTION

The Importance of Cyberspace

Cyberspace is more than just the Internet and information and communications technology (ICT). It is a domain similar to the domains of land, air, sea, and space, but with its own distinct characteristics and challenges. The cyber domain is characterized by the digital storage, modification, and exchange of data via networked systems and supported by critical information infrastructures. It has national and international dimensions that include industry, commerce, intellectual property, security, technology, culture, policy, and diplomacy. As such, cyberspace plays a critical role in the global economy.

Similar to other nations with a robust ICT infrastructure, Kenya's conducts its social, economic and national security activities in this digital, interconnected environment. For example, the Government of Kenya relies on common infrastructure, information technology (IT) platforms, and new technologies to increase the efficiency and effectiveness of government services. One of the main priorities of the Government of Kenya towards the realization of national development goals and objectives for wealth and employment creation, as stipulated in the Kenya Vision 2030, is to achieve an e-Government capability. At the same time, the development, implementation, and adoption of technologies such as mobile computing, mobile banking, and broadband communications enables Kenyans to connect with a speed and ease—unthinkable only five years ago.

However, these same technologies can present new risks that can cause widespread damage to national security, economic growth, and critical infrastructures. Moreover, the reach and impact of cyberspace is accelerating across the national and international boundaries, making it a complex challenge for any government to address alone. For this reason, the Government of Kenya considers securing its national cyberspace a national priority to continue to facilitate economic growth for the country and its citizens.

Government of Kenya Cybersecurity Implementation Hierarchy

ICT growth is particularly prevalent in Africa, where technological advancement and innovation are driving progress in key sectors (e.g., agriculture, education, financial services, government, and health). In 2009, the regional fiber-optic underwater cable increased ICT mobilization and interconnectedness across Kenya and much of East Africa.

With the rapid growth of technology, the Kenyan people have quickly become accustomed to and dependent on the services provided to them through government and business websites, banking connectivity with central banks and other individuals, and ease of communications. These advances continue to bring new and exciting opportunities to businesses and individuals across Kenya.

According to statistics released by The Communications Authority of Kenya (CAK), Kenya had an estimated 11.6 million Internet users and 31.3 million mobile network subscribers as of the second quarter of fiscal year 2013/2014

(source:http://cck.go.ke/resc/downloads/Sector_Statistics_Report_Q1_201314.pdf)

THE CYBERSECURITY CHALLENGE

The Evolving Threat Landscape

Aggressively supporting the technological advancements in Kenya has resulted in a more open, interconnected nation which can offer adversaries avenues for exploiting computer networks. Cyber attacks are continuously evolving—to a great extent faster than cyber defences—resulting in an ever-increasing frequency of attacks and the probability of success over time. *Figure 1* provides a snapshot of the sophistication of cyber-attacks from 1980-2014. These cyber attacks may come from hacktivists seeking to publicize political views, from criminal organizations seeking financial gain, from terrorist groups seeking to inflict economic or political damage, or from state-sponsored intelligence and security organizations advancing their own economic or national security aims. Many attacks involve extremely sophisticated technological and social engineering techniques; however, low-technology penetrations—such as insider threats—remain a danger.

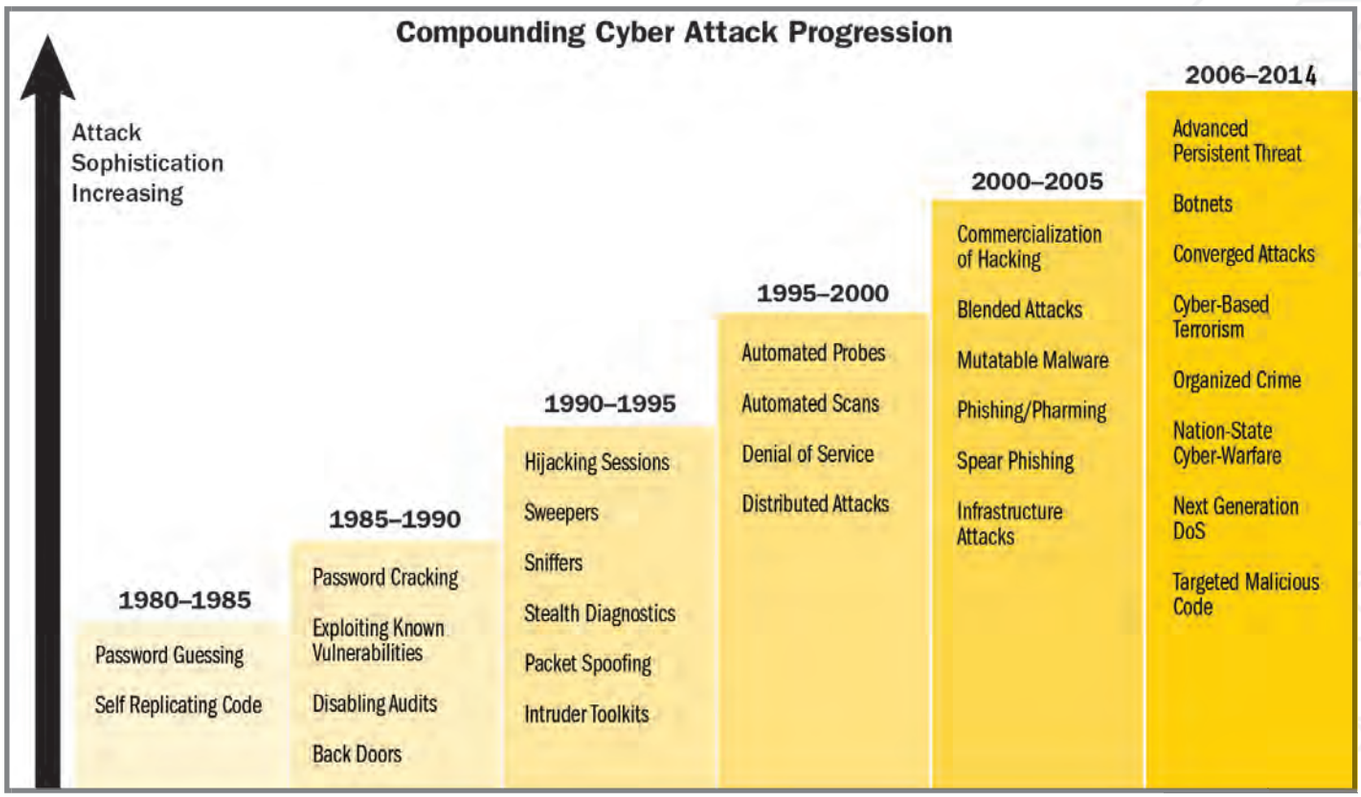


Figure 1 provides a snapshot of the sophistication of cyber-attacks from 1980-2014.

Cybersecurity—a National Priority

The expansive and dynamic nature of ICT creates a wide and deep range of challenges. The Government of Kenya is addressing these challenges to provide for cybersecurity at the national level, enabling economic growth and protecting the interests of the Kenyan people. In evaluating the potential paths forward, the Government of Kenya identified several key challenges resulting directly from emerging risk areas inside Kenya, the East Africa Community (EAC), and internationally. By addressing these risks and understanding the impact of Kenya's cybersecurity efforts, technology growth and economic development will be significantly enabled by cybersecurity implementation.

Risks and challenges can manifest from various sources—even from those areas where technology is enabling significant growth and prosperity. For example—by providing people with the ability to access and exchange information, they become dependent on that information to socialized with family and friends, conduct business, and feel connected in our modern world. The National Cyber Security Master Plan addresses emerging cyber risks and the challenges that the ICT may face in the future.

Recognizing this and understanding the critical role ICT plays in Kenya's economy, the Government of Kenya developed the National Cybersecurity Strategy (Strategy). The Strategy supports the three pillars of the Vision 2030 and supports other national initiatives such as the National ICT Master Plan[1] (see *Figure 2*). The purpose of the Strategy is to clearly define Kenya's cybersecurity vision, goals, and objectives to secure the nation's cyberspace, while continuing to promote the use of ICT to enable Kenya's economic growth.

Both financial and non-financial institutions need high awareness of the need for secure online systems. This will ensure a secure online environment for conducting business and other economic activities. Encourage the use of security standards while designing, building and deploying IT systems.

(source: http://www.ict.go.ke/docs/MasterPlan2017.pdf)

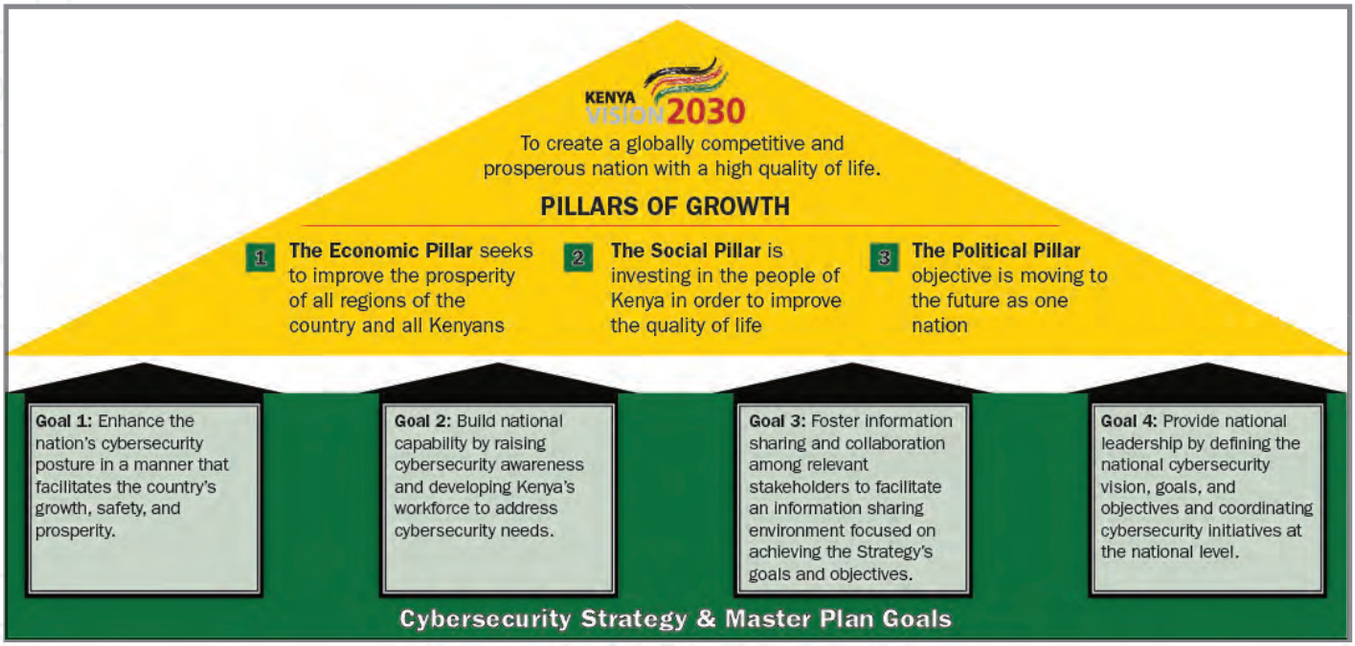


Figure 1: Cybersecurity Strategy Benefits

The National ICT Master Plan strategic goals are: (1) every citizen connected; (2) Kenya is Africa's ICT hub; (3) public service for all; and (4) a society built on knowledge.

Recognizing the need to improve its cybersecurity posture, GoK has taken steps to promote improved cybersecurity including the Kenya Information and Communications ACT, CAP 411A as amended by The Kenya Information and Communication (Amendment) ACT, 2014 , the formation of the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), and the establishment of the National Certification Authority Framework, which provides a foundation for public key infrastructure implementation and partnership with regional and international cybersecurity bodies and forums including the International Telecommunications Union (ITU) and the East Africa Communications Organization (EACO). While these activities and initiatives will help GoK evolve its cybersecurity posture, overall, GoK's cybersecurity posture is still relatively immature in the face of the growing complexity and sophistication of cyber threats. The GoK National Cybersecurity Strategy will help mature GoK's posture by providing a strategic cybersecurity direction for GoK with accompanying implementation actions to secure the nation's critical cyber infrastructure against existing and emerging threats.

A robust cybersecurity policy, legal, and regulatory framework that provides direction, roles, responsibilities, goals, resources, and governance plans in the creation of a strong cybersecurity doctrine is essential to translating strategic cybersecurity intent into a viable operating model. The GoK Regulatory, Policy, and Legal Framework provide essential inputs to GoK National Cybersecurity Strategy by:

- Analyzing GoK's baseline cybersecurity governance model;
- Analyzing GoK's baseline cybersecurity governance model;
- Evaluating GoK's cybersecurity maturity;
- Highlighting national cybersecurity master plan considerations from other nations; and,
- Providing recommendations for a GoK Regulatory, Policy, and Legal Framework that:
- Identify needed laws, regulations, and policies;
- Define governance roles and responsibilities;
- Prescribe measures to secure critical cyber infrastructure in the public and private sectors;
- Involve the private sector in policy development;
- Facilitate international cooperation;
- Define and protects against cybercrime;
- Balance information security and privacy considerations; and,
- Promote secure online transactions through trusted identities.

Developing the GoK Regulatory, Policy, and Legal Framework involves a three step process, as depicted in Figure 2.

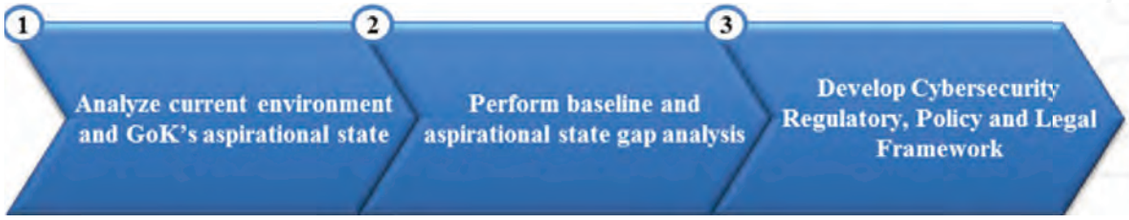


Figure 3 GoK Regulatory, Policy, and Legal Framework Approach

GoK Cybersecurity Governance Maturity Analysis

The Governance maturity analysis examines GoK's national-level cybersecurity organizations and their roles and responsibilities for both steady-state and incident response. GoK has taken initial steps at developing a cybersecurity governance framework by imbuing the Communications Authority of Kenya (CAK) with regulatory responsibilities and standing up National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), which provides an important first step for national-level incident response. GoK will continue to refine its cybersecurity governance model, define steady state and incident response roles and responsibilities, and expand KE-CIRT's information relationships across GoK, with private sector partners within Kenya, and with regional and international partners to promote coordinated situational awareness and incident response.

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
Organizational Structures and Policies - General: clear goals and objectives; clear responsibility for cyber security at all levels of government: institutional level, policy level and issue level; public and transparent commitment to cyber security; private sector involvement and partnership; government authorities in place; special agencies; consumer protection; homeland security; national defense; security; appropriate regulations and refrain from imposing regulatory restrictions that are not strictly necessary for cybersecurity; a technology neutral approach fosters broad competition	Initials	• Adopt national policy that includes action items for attainment of cyber security goal. • Establish formal regional and multi-stakeholder partnerships and agreements • Provide regulators with effective legal power and funding to execute their responsibilities • Enable regulators assume lead role in cybersecurity policy-making • Ensure cybersecurity frameworks allow for technological innovation • Provide GoK agencies/ministries with specific, codified information security roles, responsibilities, and requirements
Emergency Requirements/National Security and Emergency Preparedness	Progressing	• Implement capabilities to detect, investigate, analyze and respond to cyber-related incidents • Develop crisis communications plans • Consolidate responsibilities and resources for emergency responses • Prepare and implement periodic cyber security risk assessments, audits and reviews on national and sector basis • Conduct cyber security exercises to test readiness and responsiveness • Expand KE CIRT's incident monitoring facilities and capabilities • Participate in global and regional cybersecurity incident monitoring initiatives and forums (e.g., FIRST)

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
Operating Requirements (Targeted): network operators, service providers, hardware/software suppliers, end-users	Initials	• Establish and enforce regulations for service providers • Use and/or coordinate public-private sector efforts to develop cyber-security standards, procedures, codes of conduct, etc.
National Strategy & Frameworks: roadmap design and evolution; national policy framework; creation of a national strategy and policy; legal foundations; involvement of stakeholders; program evaluation, optimization	Initials	• Provide training to key government personnel on cyber security standards and regulatory frameworks • Establish inter-agency information sharing relationships • Empower regulatory body to report on most effective and efficient means of ensuring cybersecurity for commercial networks and consider consumer education and outreach programs
National Organizations: adapt organizational structures based on availability of resources, PPPs, and ICT development; define specific roles, functions and resources; establish central organizational entity to support the national cyber security policy and facilitate regional and global cooperation	Initials	• Identify key Ministries to oversee cybersecurity strategy (e.g., MICT) and serve as regulator (e.g., CAK) • Ensure adequate personnel with cyber security skills form working groups for collaboration among stakeholders; Attorney General's Office and/or Director of Public Prosecution Office to review Cyber laws
Regional and Global Frameworks & Organizations: cooperation and collaboration on misuse of cyberspace; ensure cross border coordination	Initials	• Lead the development of mechanisms for regional cooperation to solve and prosecute cybercrimes • Develop bilateral agreements with key countries to promote cybersecurity and cybercrime prosecution including Legal Mutual Assistance Programs.

Cybersecurity Governance Maturity Analysis

NATIONAL CYBERSECURITY STRATEGY

To promote the Government's commitment to cybersecurity, the Strategy includes four strategic goals:

1. Enhance the nation's cybersecurity posture in a manner that facilitates the country's growth, safety, and prosperity.

2. Build national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs.

3. Foster information sharing and collaboration among relevant stakeholders to facilitate an information sharing environment focused on achieving the Strategy's goals and objectives.

4. Provide national leadership by defining the national cybersecurity vision, goals, and objectives and coordinating cybersecurity initiatives at the national level.

The subsequent sections outline specific objectives for each goal.

Goal 1: Enhance the Nation's Cybersecurity Posture

Objective: *Protect Critical Information Infrastructure*

The Government of Kenya is promoting ICT usage to both the government and the Kenyan public through an undersea and terrestrial cable and network installations, increased availability of mobile/wireless technology, and a movement towards e-government services. However, the increased use of and reliance on ICT exposes Kenya to increased cyber risks. Threat actors can exploit ICT vulnerabilities to perpetrate crimes against the Government of Kenya and Kenya's citizens who rely on ICT to perform electronic transactions or obtain key critical government services. Also, natural disaster may pose a threat by causing potential damage critical information infrastructure and disrupting communications. As such, it is imperative that as the Government of Kenya protect critical information infrastructure. Its cybersecurity activities should also be flexible enough to counter and mitigate the increasingly complex threats and vulnerabilities to ICT infrastructures.

The Government of Kenya is taking steps to increase the security and resilience of its critical information infrastructure to protect its government, citizens and residents, and corporations from cyber threats and to reap the social and economic benefits of cyberspace. The government is doing this through a coordinated effort with other countries

to increase the security of global cyberspace as a whole. This includes securing critical infrastructures, applications, and services. Additionally, the Government of Kenya is working with relevant stakeholders to build cybersecurity capabilities focused on operations, infrastructure and mission assurance. Within the National Cybersecurity Master Plan the Government has identified a governance and capability structure (Figure 3) which will support scalable growth of cybersecurity within the public and private sectors.

Goal 2: Build National Capability

Objective: *Awareness and Training: Inform and educate the Kenyan public and workforce to secure the national cyberspace*

As part of building national capability goal, the Government of Kenya is informing and educating the public and workforce on how to secure the national cyberspace. This includes partnering with other government organizations, the private sector, and academia to ensure that people with cybersecurity responsibilities possess the appropriate level of cyber qualifications and competencies. This effort incorporates human capital management, leadership development, education and training, and strategic communication and change management to develop a nation-wide workforce for the future. Additionally, the Government of Kenya is:

- Working with academia to develop cybersecurity curriculums for higher education and specialized training programs to ensure competency building for cybersecurity professionals; and
- Developing, promoting, and implementing incentive programs to increase the appeal of cybersecurity career paths to attract and retain Kenyans into this critical field.

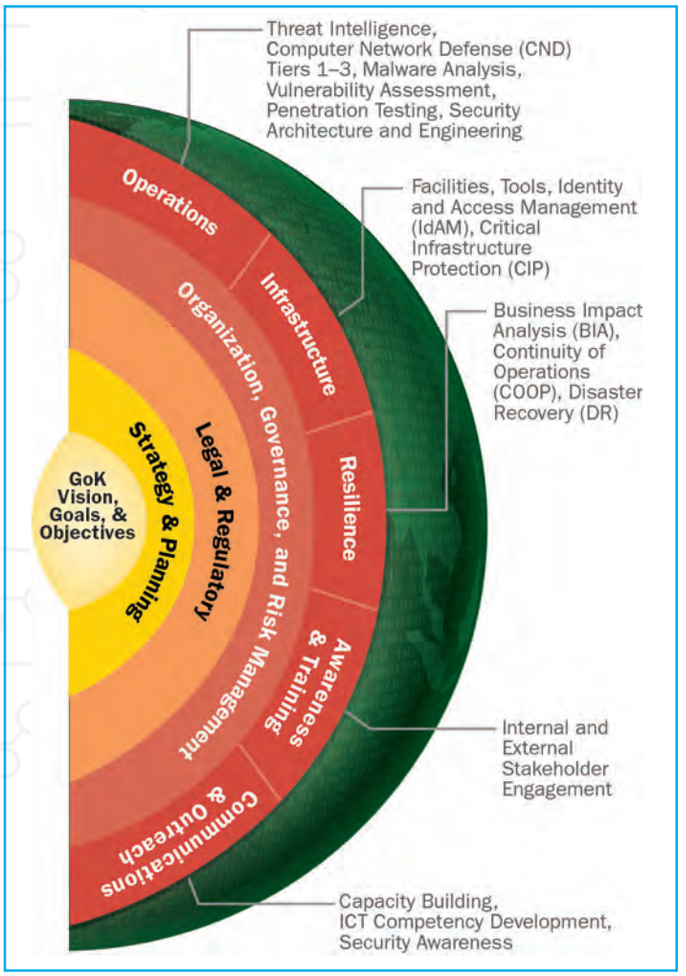


Figure 4: Kenya cybersecurity Goals and Objectives

Objective: *Communications and Outreach: Elevate cybersecurity awareness for government, private sector, and the Kenyan public*

The Government of Kenya is developing, launching, and promoting targeted awareness programs to inform the general public and workforce of common cybersecurity threats and counter measures. Through targeted communications and outreach activities, the Government of Kenya is:

- Increasing the understanding of cyber threats and empower the Kenyan public to be safer and more secure online; and
- Communicating approaches and strategies for the public to keep themselves and their families and communities safer online.

Goal 3: Foster Information Sharing and Collaboration

Objective: *Develop a comprehensive governance framework to leverage resources, reduce conflict and duplication of effort, and work toward Kenya's long-term cybersecurity goals*

Cybersecurity is a complex, multidisciplinary challenge that requires coordination across a wide array of stakeholders. Therefore, implementing the Strategy requires developing a comprehensive governance model that includes meaningful participation by relevant stakeholders, working together toward the common goal of securing Kenya's cyberspace. Through this governance framework, the Government of Kenya intends to:

- Develop the required laws, regulations and policies required to secure the nation's cyberspace;
- Solicits stakeholder input and feedback, as appropriate; and
- Balance information security, privacy considerations and economic priorities.

Cultivate a culture of information sharing that facilitates the real time exchange of cybersecurity information

Successful implementation of the Strategy requires the sharing of cybersecurity information (cross- organizational and cross-sector) in a trusted and structured manner. The Government of Kenya will develop and manage a secure information-sharing capability to promote knowledge and lessons learned among relevant stakeholders.

Goal 4: Provide National Leadership

Objective: *Develop and Coordinate Implementation of the National Cybersecurity Strategy and Master Plan*

Enhancing Kenya's cybersecurity posture is a top priority for the Government of Kenya. As such, the Government of Kenya will continue to provide a single, unified agenda that will guide all relevant national stakeholders. Specifically, the ICT Ministry will:

- Continue to refresh the Strategy (vision, goals, and objectives), as required and establish a tactical roadmap for achieving national cybersecurity objectives; and
- Use the Strategy, and complementary Cyber Security Master Plan to identify and implement relevant cybersecurity initiatives, in conjunction and in collaboration with relevant stakeholders.

Development Impact

Secure communication, the technology that facilitates the safe and secure processing, transfer and exchange of information in an economy, delivers positive impacts over time to an economy. Secure communication has changed business operations and the way people communicate. It has introduced new efficiencies for existing services and created new services altogether. The Figure below emphasizes that the growth of an economy depends upon a secure communications infrastructure, the use of applications that ride over that infrastructure and also on communications-related human capacity:

- Capacity by both government and private sector to provide and maintain the infrastructure at an affordable price and on a sustained basis
- Capacity of entrepreneurs to create and make available useful content
- Capacity by users to understand and use the applications.

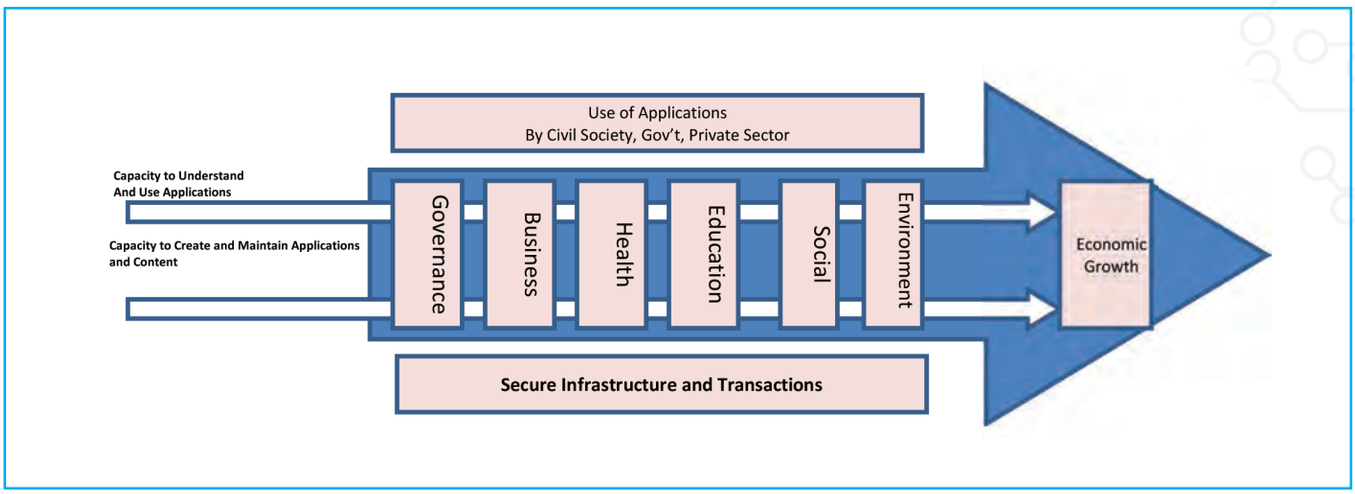


Figure 5
Source: "ICT In Developing Countries," Alexander Osterwalder

KEY BENEFITS

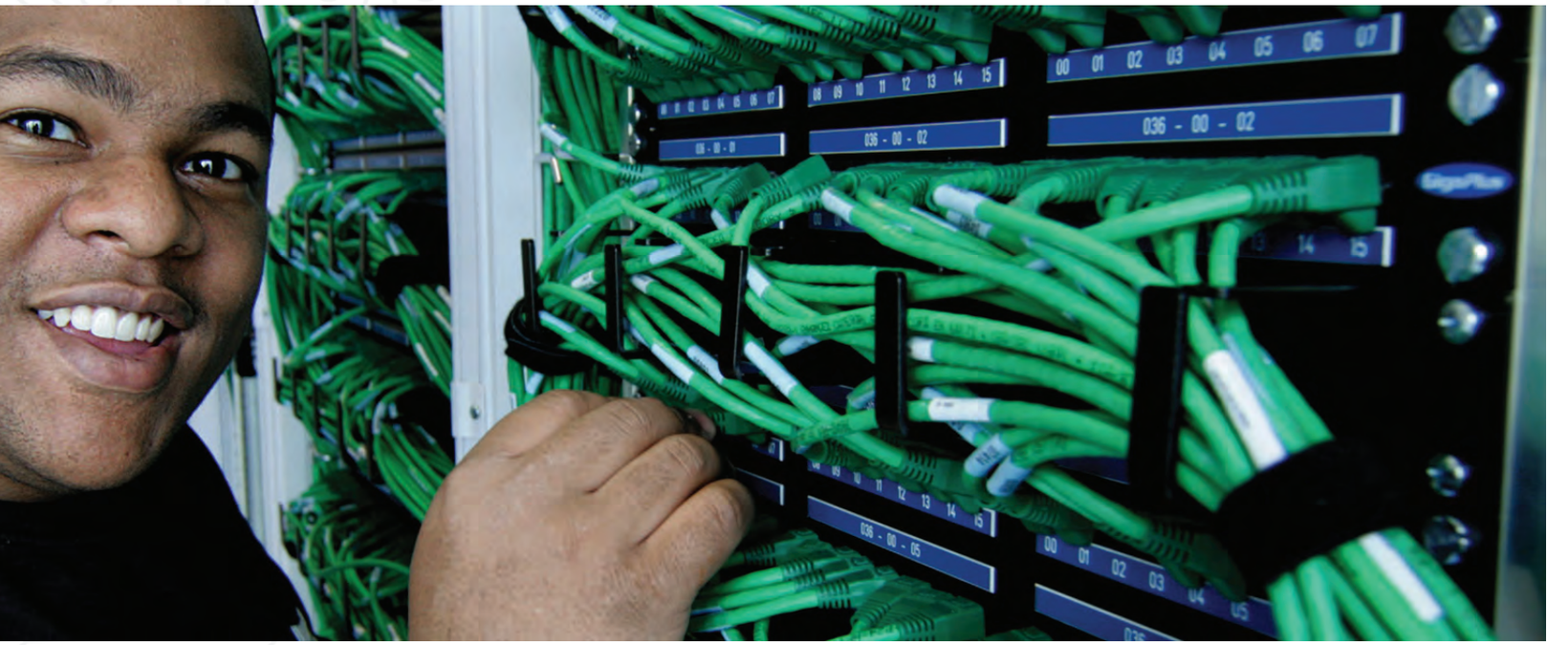
The Government of Kenya expects to see considerable benefit from the development of a holistic national cybersecurity strategy. These benefits will be realized, not only within ICT circles, but across social and economic areas by all Kenyans.

These benefits clearly impact and improve the Pillars of Growth established by Kenya Vision 2030: The Economic Pillar, The Social Pillar, and The Political Pillar by directly supporting the goals of increasing prosperity, improving the quality of life, and moving to the future as one nation.

Benefit Area	Details of Benefits Resulting from Improved Cybersecurity
Private Sector Growth	■ Added e-commerce applications due to a more secure environment ■ Growth in the quantity of e-commerce transactions ■ Lower business risk and uncertainty ■ More competition among firms as secure e-commerce grows ■ Financial sector growth as the number of financial transactions grow ■ More sustainable economic growth through sustained security and increased confidence in e-commerce ■ Through e-markets, suppliers are able to interact and transact directly with buyers, thereby eliminating the costs related to intermediaries and distributors. Businesses can increase revenues and margins
Greater Cooperation with Relevant International Organizations	■ Increased incentives to participate in the formation of international rules, including intellectual property rights, contract law, electronic signatures and authentication, consumer protection, jurisdiction and others; secure electronic commerce issues are addressed in international for a such as WIPO (World Intellectual Property Organization), UNCITRAL (United Nations Commission on International Trade Law), the Hague Conference on Private International Laws, ISO (International Standard Organization) including COPOLCO (Consumer Policy Committee), OECD and others

Details of Benefits Resulting from Improved Cybersecurity

Benefit Area	Details of Benefits Resulting from Improved Cybersecurity
Improved Organizational Performance and Reduced Transactions Cost	■ Lower costs due to improved efficiency of transactions ■ Lower cost leads to an increase in the number of firms in the market ■ Provides avenues for firms to enter into the business-to-business and business-to-government global supply chains ■ Easier marketing of agricultural products and local sourced goods in the global market ■ Reduction of search costs as buyers and sellers are together in a single online trading community ■ Reduction in the costs of processing transactions (e.g., invoices, purchase orders and payment schemes), with the automation of transaction processes ■ Efficiency in trading processes and transactions as sales can be processed through online auctions ■ Online processing improves inventory management and logistics
Promote Anti-Corruption in Government and Industry	■ Increase in price transparency as the gathering of a large number of buyers and sellers in a single e-market reveals market price information and transaction processing to participants; the publication of information on a single purchase or transaction makes the information readily accessible and available to all members of the e-market ■ Increased price transparency can exert downward pressure on price differentials in the market; buyers are provided much more time to compare prices and make better buying decisions ■ Expansion of borders for dynamic and negotiated pricing wherein multiple buyers and sellers collectively participate in price-setting and two-way auctions; prices can be set through automatic matching of bids and offers; the requirements of both buyers and sellers can be more easily aggregated to reach equilibrium price levels, which are lower than those resulting from individual actions
A More Competitive Business Environment	■ Trade liberalization as cross-border transactions costs decline ■ Resolution of patent issues: international programs will contribute to achieving harmonized patent protection for progress and developments in secure transactions ■ Enhanced public welfare through improved access to online goods and services ■ Greater social cohesion as wage and income disparities lessen due to improved communication and information sharing, i.e., a better functioning labor market ■ More options for consumer transactions (more, reliable distribution channels) ■ Lower transactions costs ■ Lower prices in longer term
Transparency and Efficiency in Government	■ Expedited government financial transactions enabling greater efficiency and expediency in resource allocation ■ Improved communications



CONCLUSION

As Kenya's remarkable ICT growth continues, ensuring the confidentiality, integrity, and availability of public and private sector information across Kenya's ICT infrastructure is of significant importance. Kenya's National Cybersecurity Strategy serves to demonstrate the government's commitment to improving Kenya's cybersecurity posture and share overarching vision, goals, and objectives. Implementation of the strategy is supported by an evolving national Cybersecurity Master Plan, which has been developed to define (and ultimately govern) a prioritized roadmap of discreet cybersecurity projects.

Both the strategy and master plan are critical to securing the online environment for citizens, industry, and foreign partners; increasing the Kenyan people's confidence in online transactions, data security, fraud protection, and privacy; encouraging greater foreign investment and enhancing trade opportunities; and enabling Kenya's broader economic and societal goals.

Glossary

Term	Definition
Broadband	A type of high-capacity telecommunications especially as used for access to the Internet.
Computer Incident Response Team	The personnel responsible for coordinating the response to computer security incidents within an organization
Critical Infrastructure	A term used to describe assets that are essential for the functioning of a society and economy. (e.g., electrical grid, telecommunications, water supply)
Cybersecurity	The processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction
Cyberspace	The notional environment in which communication over computer networks occurs
e-Government	Short for electronic government, it is digital interactions between a government and citizens, government and businesses, government and employees, and also between two governments
Globalization	Growth to a global or world-wide scale
Governance	Consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility
Insider Threat	A malicious individual who is also an employee or officer of a business, institution, or government
Social Engineering	A non-technical kind of intrusion (or “hack”) that relies heavily on human interaction and often involves tricking other people to break normal security procedures
Digital Certificate	A digital certificate is an electronic “passport” that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).
GoK	Government of Kenya
PKI	Public Key Infrastructure

Annex 1: Legal/Regulatory Maturity Analysis

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
Critical Information Infrastructure Protection: principles for protecting CI, e.g., G8, UN; adequate and reliable supporting infrastructures, e.g., power supply	Initials	• Define GoK critical cyber infrastructure • Identify GoK critical cyber infrastructure protection requirements • Develop national cybersecurity policies and implementation plans • Develop consumer protection plan(s)/ policies
Criminal Law: illegal access, acquisition of data and interception; data and system interference; content: pornography, racism, religious offenses, libel, defamation, spam; illegal gambling; misuse of devises, forgery, theft, fraud; terrorism, cyber warfare ; Privacy and Human Rights: balancing security and freedom; judicial review of intrusions into PII; independent oversight of investigations; limiting access to PII	Progressing	• Develop specific cybercrime penal code • Draft technology neutral cybercrime legislation • Provide digital forensics/cybersecurity training (including deep packet inspection) to facilitate law enforcement's prosecution ability • Adopt investigative protocols that balance security and freedom • Provide basis for: intellectual property rights law, e-commerce law, freedom of access to information, e-security/ data protection/ privacy laws
Procedural Law: internet investigation, preservation and disclosure of stored data; data retention; search/seizure; data content and collection; regulation of encryption technology	Progressing	• Craft legislation to provide regulatory body with powers of investigation and enforcement, e.g., use and abuse of ICT networks, physical damages, spyware, spam • Develop and adopt ICT laws that facilitate e-commerce and are comprehensive (security, electronic signatures, PKI, DRM, cybercrime, et. al.) • Ensure all laws are technology neutral • Provide a regulatory body with sufficient funding to provide oversight of cybersecurity law implementation
Digital Evidence: the ability to use specific data-related investigation tools to present digital evidence in court; Law Enforcement, Investigation, Prosecution: victim awareness; reporting of crime; locating the evidence; encryption challenges; patrolling; Liability of Internet Providers: access providers; caching; hosting; obligation to monitor; hyperlinks; search engines	Progressing	• Develop/adopt a diverse set of tools to allow for alternative approaches in providing evidence • Ensure liability of all involved parties is clear, documented, understood, and enforced

Annex 2: Capacity Building Maturity Analysis

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
Building Awareness: awareness campaigns, dedicated websites, use of PKIs and digital certificates; training programs; use of the media; government, commercial and consumer understanding of cybersecurity threats	Progressing	• Implement awareness campaigns to educate users, law enforcement, and policy makers implemented • Deploy PKI systems for secure transactions • Provide affected GoK staff with communications and PR training • Ensure public is aware of ways personal data is shared with third parties • Partner with private sector for cybersecurity awareness
Building Capacity at National Level: promote security of products and services; well-documented products; easily understood security measures; integration of security early in product life-cycle; e-government applications and services; address risk prevention and risk management; preparation of a security plan by government; outreach to civil society to raise citizens' awareness; enhance S&T and R&D activities	Initials	• Ensure public and industry possess knowledge of internet and basic cybersecurity practices • Promote adoption of cybersecurity standards across government agencies/departments • Partner with professional industry associations committed to promote cybersecurity standards adoption • Provide technical training to legislators, prosecutors, the judiciary and law enforcement of ICT related technical aspects of cybercrime
Private Sector (Individual/Civil Society): individual without protection present the greatest source of vulnerability	Initials	• Target organizations (civil society groups) for cybersecurity training and awareness and solicit cybersecurity input from consumer groups
Private Sector (Business/Industry): the role of the PS is indispensable as the infrastructure is owned and operated by the PS and the PS is first to adopt technology changes	Initials	• Promote industry adoption of adequate technical solutions such as norms, standards, modes of conduct through regulation as necessary • Promote the formation of industry groups to provide input to regulatory body on technology development, costs, benefits, etc. • Promote the adoption of secure business practices with priority given to those economic sectors with higher levels of risk/ negative consequences such as banking and financial • Encourage industry and regulators to jointly develop and agree on industry-specific cybersecurity standards and regulations

Annex 3: Harmonization Maturity Analysis

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
National Coordination: information sharing; collection of evidence; coordination with criminal justice systems	Initials	• Develop and enact national regulations via legislation
Regional and Global Coordination: identification of applicable instrument for international cooperation: international agreements, protocols and conventions; procedures regulated by bilateral agreements; international reciprocity; Strategies for Integration: mutual legal assistance and extradition; transfer of prisoners; transfer of proceedings in criminal matters; asset recovery	Initials	• •Ensure national laws are developed within international cooperation principles • •Build partnerships and among stakeholders, government, private sector and academia • •Participate in binding conventions and protocols, e.g. ITU, OECD, APEC TEL, Forum of Incident Response and Security Teams (FIRST), Inter American Telecommunications
Private sector/Industry/Academia: PPPs; scientific and independent approaches	Initials	• Develop and enact national regulations via legislation • Partner with private sector for cybersecurity awareness campaigns

Annex 4: Financial Maturity Analysis

Evaluation Area	Current GOK Maturity	Recommended Maturity Actions
Policy: means by which to provide funding or effective regulation	Initials	• Allocate part of government annual budget to cybersecurity • Review regional and global options for funding (NEPAD, ADB, MDGs, ITU's WSIS, , DSF, WB, UNECA, UNDP, UNCSTD, UNESCO, etc.) • Establish regulatory oversight for investments leading to new services, etc. • Set up PPPs to coordinate efforts of private sector with government in pursuing investment opportunities through government subsidies or co-financing arrangements • Balance cybersecurity requirements with incentives for ISPs et. al. to increase revenues through market expansion, penetration, etc.
Government Sources: stimulus funds, PPPs, loan guarantees, grants; facilitation of non-traditional investors in ICT such as banks, electric companies, et. al.	Initials	• Make information on criteria and access publicly available • Where/when possible, provide cybersecurity loans and grants to promote cybersecurity across Kenya

Other	Initials	• Consider incentives to lower the costs of cybersecurity measures • Adopt regulatory measures to promote new technologies and innovation in cybersecurity

Annex 5: Near Term Actions

Action	Description
National-Level Cybersecurity Strategy: Create an overarching GoK cybersecurity policy that outlines roles, responsibilities, and authorities	The policy would: • Detail which GoK ministries provide cybersecurity oversight for standards development and adoption, regulatory responsibilities, research and development, incident response, international relations, etc. • Detail GoK-specific roles and responsibilities for GoK cybersecurity efforts across GoK and within each GoK ministry for government systems and networks [e.g., GoK Chief Information Officer (CIO) roles and responsibilities, information security roles and responsibilities within each ministry (e.g, ministry-specific CIOs, CISOs, etc.)] • The policy will serve as the foundation of GoK's cybersecurity framework
Critical Cyber Infrastructure Protection: Establish a cybersecurity regulatory body within GoK to define cybersecurity regulations with input and consensus from the private sector	• The entity will be responsible for development of specific regulations, oversight of cybersecurity implementation and compliance across the public and private sectors • Through open comment periods, private sector owners and operators would have the ability to inform regulations prior to finalization **The regulating authority will:** • Oversee cybersecurity critical infrastructure protection efforts • Monitor public and private sector cybersecurity compliance reporting • Assist in developing a cybercrime penal code
Define and identify cyber : Define and identify cyber critical infrastructure across the public and private sectors	• Develop criteria for what constitutes critical cyber infrastructure in the private sector and within GoK. • For example: critical cyber infrastructure consists of physical assets and virtual systems and networks that enable key capabilities and services in both the public and private sectors • Develop a law/regulation requiring GoK ministries and private sector companies to identify their critical cyber infrastructures and report their inventory to GoK

Action	Description
With industry representatives, establish sector-specific baseline cybersecurity protection criteria and requirements	• Regulator will work with industry consortia to establish mutually agreeable cybersecurity standards and practices for critical cyber infrastructure in each industry; for example: • SCADA security standards • Health information security/privacy standards • Identity and Access Management and Authentication standards (e.g., for financial transactions) • Other standards as appropriate for each industry sector
Document GoK standards and guidelines for GoK systems and electronic transactions	• Establish security controls and standards to be adopted for all GoK information systems and networks (e.g., NIST-like function) • Includes standards for GoK information handling/ privacy, identity management, continuous monitoring, incident detection/response, etc. (Government-specific) • Develop GoK national-level cyber incident response plan
Require public and private sector cybersecurity compliance reporting to regulator(s)	• Promotes consistent cybersecurity across the public and private sector and accountability
Cybercrime: Develop specific cybercrime penal code	• Draft technology neutral cybercrime legislation • Augment existing legislation to provide regulatory body with powers of investigation and enforcement, e.g., use and abuse of ICT networks, physical damages, spyware, spam; • Ensure laws that facilitate e-commerce and are comprehensive (security, electronic signatures, PKI, DRM, cybercrime, et. al.);
Digital Certificate	• A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).
GoK	Government of Kenya
PKI	Public Key Infrastructure

Produced by

Ministry of Information Communications and Technology
Designed and Published by ICT Authority

Feel safe online

Ministry of Information,
Communications and Technology
Tel: +254 (0) 204920000
Email: info@information.go.ke
P.O Box 30025 - 00100,
Nairobi, Kenya
www.information.go.ke