UITS Journal Volume: 4 Issue: 1
ISSN : 2226-3128

Role of PKI : Realizing Digital Bangladesh

Prosun Mozumder[1] Joya Das[2]

Abstract: ***Public Key Infrastructure around the world has had mixed success over the past ten years. Some jurisdictions (like Australia and the USA) have been left largely disillusioned by the hype, while others (like China and Korea) see PKI as indispensable infrastructure for e-business. The typical situation around Asia is that PKI is highly desirable but difficult and/or costly to implement. Through this article we have tried to prove that PKI is the key ingredient for e-government. Without PKI full digitalization of a country is simply impossible. We have also tried to identify the field where & how we can implement PKI service to add a stone on our dream wall of Digital Bangladesh within 2021.***

Keywords — **public key infrastructure, e-business, authentication, security, digital certificates, smartcards, e-governance, digital signature.**

INTRODUCTION

Public key infrastructure, commonly referred to as PKI, is an Information Communication Technology (ICT) infrastructure. PKI is a term used to describe the laws, policies, procedures, standards and software that regulate and control secure operations of information exchange, based on public and private keys cryptography. The term PKI is used in this article to refer to the comprehensive set of measures needed to enable the verification and authentication of the validity of each party involved in an electronic transaction [5].

One of the main preconditions for the spread of e-government in Bangladesh is that the public have as much confidence in the digital handling of affairs as the traditional method. One should be able to rely on the security, privacy and stability of transactions, regardless of the method used.

Digital signatures based on public key infrastructure will be an important factor in building up such confidence. A new Digital Signatures Act, No. 28/2001, and the prospective review of the Public Administration Act, lay the foundation for e-government parallel to traditional methods. It can be deduced that, over the coming years, all citizens can obtain certificates and other equipment for fully valid digital signatures and encryption at an acceptable cost.[2]

[1] Experienced Advanced Engineer, CD Radio Access Network, LM Ericsson Bangladesh Limited, Dhaka, Bangladesh prosun.mozumder@gmail.com

[2] Lecturer, Dept of CSE & IT, University of Information Technology & Science, Dhaka, Bangladesh joya.cse.sust@gmail.com

Role of PKI : Realizing Digital Bangladesh

The development of technical solutions for digital signatures and equipment to support public key infrastructure is very rapid accompanied by intensive marketing activity. In light of the rapid development of the technology, and the fact that the spread among the public will take some time,. It seems more attractive to take up simpler solutions in the short-term that can ensure the adequate security of many aspects of digital public services. The same or parallel solutions could be used in various fields of e-commerce.[3]

MOTIVATION

Information and Communication Technologies (ICTs) were recognized by the world leaders as a key development enabler in World Summit on Information Society (WSIS) in Geneva in 2003 and in Tunis in 2005 (Tunis Commitment). In the Poverty Reduction Strategy of the country called National Strategy for Accelerated Poverty Reduction (NSAPR) 2009, ICTs were similarly identified and given due importance. The current government's Digital Bangladesh by 2021 vision proposes to mainstream ICTs as a pro-poor tool to eradicate poverty, establish good governance, ensure social equity through quality education, healthcare and law enforcement for all, and prepare the people for climate change. One of the main preconditions for the spread of e-government in Bangladesh is that the public have as much confidence in the digital handling of affairs as the traditional method. One should be able to rely on the security, privacy and stability of transactions, regardless of the method used. So PKI is the main key concern for any country to full fill its digitized dream.

ROLE OF PKI IN DEVELOPING DIGITAL BANGLADESH

Information and communication technologies (ICT) has evolved into a key enabling infrastructure across the world while proving to be a powerful driver of enhanced living conditions and opportunities around the globe. ICT has changed the world dramatically and it is bound to continue to do so in the future. Most of the countries are now heading to implement E-Government & some pioneer countries have already implemented it to some extent.

Progress in online service delivery continues in most countries around the world. The United Nations E-Government Survey 2012 [1] finds that many have put in place e-government initiatives and information and communication technologies applications for the people to further enhance public sector efficiencies and streamline governance systems to support sustainable development. Among the e-government leaders, innovative technology solutions have gained special recognition as the means to revitalize lagging economic and social sectors. The overall conclusion that emerges from the 2012 Survey in today's recessionary world climate is that while it is important to continue with service delivery, governments must increasingly begin to rethink in terms of e-government – and e-governance – placing greater emphasis on institutional linkages between and among the tiered government structures in a bid to create synergy for inclusive sustainable development. An important aspect of this approach is to widen the scope of e-government for a transformative role of the government towards

cohesive, coordinated, and integrated processes and institutions through which such sustainable development takes place.

E–Government Development Index - Top 20 Countries	
Country	*Index*
Republic of Korea	0.9283
Netherlands	0.9125
UK and Northern Ireland	0.8960
Denmark	0.8889
United States	0.8687
France	0.8635
Sweden	0.8599
Norway	0.8593
Finland	0.8505
Singapore	0.8474
Canada	0.8430
Australia	0.8390
New Zealand	0.8381
Liechtenstein	0.8264
Switzerland	0.8134
Israel	0.8100
Germany	0.8079
Japan	0.8019
Luxembourg	0.8014
Estonia	0.7987

E–Participation Index Top 20 Countries	
Country	*Index*
Netherlands	1.0000
Republic of Korea	1.0000
Kazakhstan	0.9474
Singapore	0.9474
UK and Northern Ireland	0.9211
United States	0.9211
Israel	0.8947
Australia	0.7632
Estonia	0.7632
Germany	0.7632
Colombia	0.7368
Finland	0.7368
Japan	0.7368
United Arab Emirates	0.7368
Egypt	0.6842
Canada	0.6842
Norway	0.6842
Sweden	0.6842
Chile	0.6579
Russian Federation	0.6579

Fig 1. E-Government Development Index

All countries of Southern Asia fall in the lower half of the e-ready countries with approximately an equal number of them above and below the regional average. A low GDP per capita, a still evolving infrastructure and lower levels of functional literacy translate into low service provision and user uptake for the majority of the populations of India, Bangladesh, Bhutan, Pakistan and Nepal, with e-government development levels ranging from 0.2664 to 0.3829[1].

	E-gov. development index		World e-gov. development ranking	
Country	2012	2010	2012	2010
Maldives	0.4994	0.4392	95	92
Iran (Islamic Republic of)	0.4876	0.4234	100	102
Sri Lanka	0.4357	0.3995	115	111
India	0.3829	0.3567	125	119
Bangladesh	0.2991	0.3028	150	134
Bhutan	0.2942	0.2598	152	152
Pakistan	0.2823	0.2755	156	146
Nepal	0.2664	0.2568	164	153
Afghanistan	0.1701	0.2098	184	168
Sub Regional Average	**0.3464**	**0.3248**		
World Average	**0.4882**	**0.4406**		

Fig 2. E-Government Development in Southern Asia

From figure 2, we have found that Bangladesh has significant downgrade in world rank from 134 to 150 within two years span. There are several critical factors which become barriers in the implementation of e-government in all level of Bangladesh.

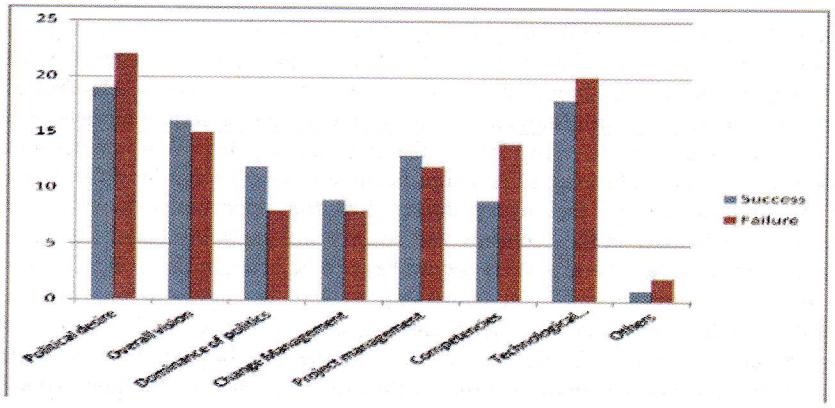

Fig 3. Parameters for E-Government of Bangladesh

The Constitution of the People's Republic of Bangladesh, particularly the Articles concerning people's rights and provision, and Vision 2021 form the cornerstone of this Perspective Plan [2]. The strategic document has been formulated in consultation at the national, divisional, district levels with people from different walks of life including kishan-kishanis, labourers, ethnic people and other marginalized and disadvantaged sections of the population, civil society members, administrators and policy makers, public and private enterprises, NGOs, and other interest groups, thereby making the document a participatory one. This all level of participation can only be applicable if E-government based on ICT & tuned by PKI is introduced in Bangladesh. Figure 3 reflects the parameters for e-government of Bangladesh.

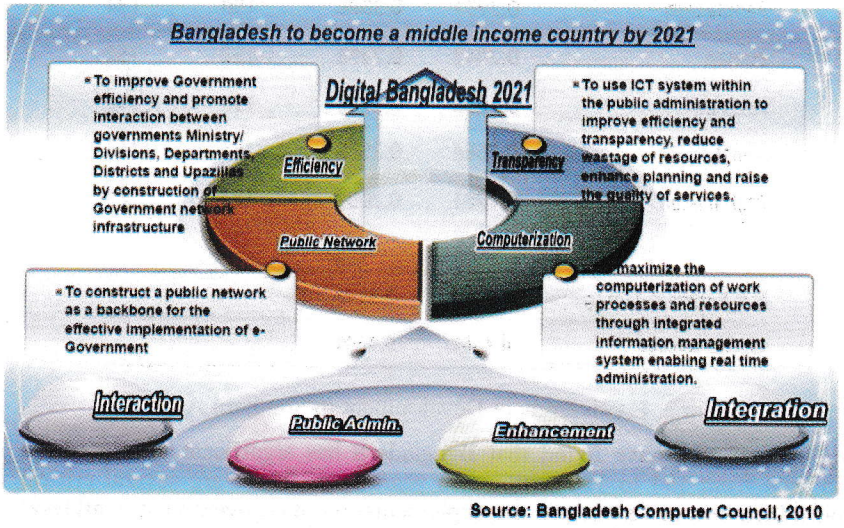

Fig 4. Digital Bangladesh Framework 2021

Given that emerging realities of globalization are changing the pattern of global economic relations, this Plan aims at turning the unfolding scenario into national advantages towards building a sustainable future which is based on ICT. Indeed, the resolve is to transform Bangladesh into a middle income in real terms as well as a high HDI country by 2021, the Golden Jubilee Year of national independence. For achieving such a significant status, much harder effort would be required to ensure that every citizen has the opportunity to fully and positively contribute in the economy and society and equitably benefit from the results achieved. Levels of poverty would have to be brought down significantly by increasing income and asset ownership as well as higher access to food, nutrition, education services, healthcare, gender equality, and creation of opportunities. Social discrimination, environmental degradation, physical insecurity, and socio-economic-cultural vulnerability must go. The framework is shown in figure 4.

ICT enabled connected governance contributes both internally & externally over traditional Government.

Internal contributions are [3]:

- Avoidance of duplication.
- Reducing transaction cost.
- Simplifying bureaucratic procedures.
- Greater efficiency.
- Greater coordination and communication.
- Enhanced transparency.
- Information sharing between agencies.
- Security of information management.

External contributions are:

- Faster service delivery.
- Greater efficacy.
- Increased flexibility of service use.
- Innovation in service delivery.
- Greater participation.
- Greater citizen empowerment.
- Citizen participation.

ICT applications can support sustainable development in the fields of public administration, business, education and training, health, employment, environment, agriculture and science within the framework of national strategies [3]. In a nutshell, the applications of ICT in interactions between

- Government and Citizens
- Government and Business
- Government and Employees
- Government and Government

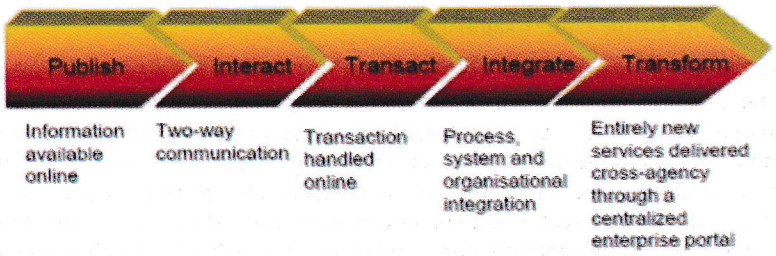

Fig 5. The Application of ICT

To make ICT becomes an indispensible part for Government system we should find out the constraint of implementing ICT. In table 1 we have shown some

common constraints concerning Digital Bangladesh & some recommendations to overcome those constraints.

Table 1. Constraints & Recommendations to overcome those

Constraints	Recommendations
▪ Inadequate Access to ICT ▪ Public Awareness about ICTs ▪ Lack of integrated approach ▪ Lack of regulatory/legal framework ▪ Absence of processes and systems	▪ Create one-stop government portal ▪ Prioritization of Services ▪ Improve ICT access by citizens ▪ Emphasize Bangla interface for citizen services ▪ Need training and leadership from the government ▪ Awareness for the use of Open Source ▪ Payment Gateway

PRIVACY & SECURITY IN E-GOVERNANCE

One of the main preconditions for the spread of e-government in Bangladesh is that the masses have as much confidence in the digital handling of affairs as the traditional method. One should be able to rely on the security, privacy and stability of transactions, regardless of the method used. As per the decision on Expert Group Meeting on Regional Cooperation towards Building an Information Society in Asia and the Pacific, 2009 for building confidence & security in the use of ICT the following steps are taken [3]

- Network Security Policy
- Cyber Laws: Formulated
- Digital Signature: Law Formulated
- Privacy Law Approved
- Intellectual Copyright: Approved
- Anti Piracy Law: Approved
- Cyber Crime Unit: Established

The e-Governance application needs to build the trust of citizens in the system [6]. It needs to ensure that the data and transactions of the citizen are secure. The information shared by the citizens should also remain safe and the privacy of the citizen needs to be protected. Whenever a citizen gets into any transaction with a Government agency, he shells out lot of personal information, which can be misused by the private sector and anti-social elements. Thus, the citizen should be ensured that the information flow would pass through reliable channels and seamless network. Secured ways of transactions for the Government services are another issue of concern. The identity of citizens requesting services needs to be verified before they access or use the services. Here digital signature will play an important role in delivery of such services. But the infrastructure needed to

support them is very expensive and requires constant maintenance. Hence a pertinent need still survives, compelling the authorities to ensure the authenticity in their transactions thereby gaining absolute trust and confidence of the citizen.

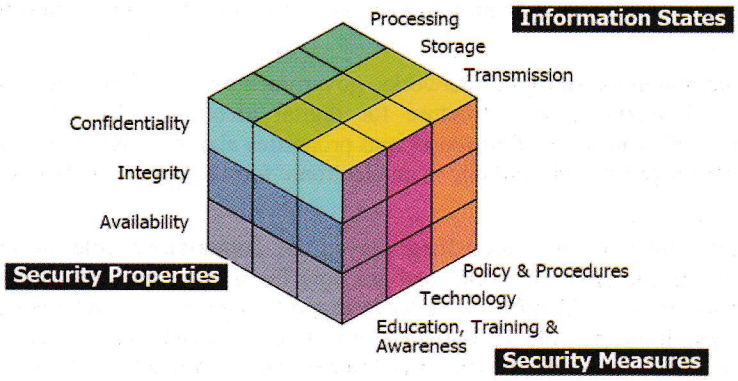

Fig 6. Measures of Information Security

The various security concerns that may be there for an e-Government System are listed as under [3]:

- Virus Attacks
- Outside and Inside Attacks
- User Frauds
- False identity / Impersonation
- Unauthorized disclosure
- Theft / Duplication of access token
- Denial of service attack
- Misinformation and propaganda
- Breach of anonymity
- Breach of accountability
- Failure to recover business information
- Loss or theft of monetary value

PUBLIC KEY INFRASTRUCTURE (PKI) IN E-GOVERNMENT

For the past ten years, governments around the world have been vitally

concerned with the establishment of secure forms of identification and improved identity management systems, in order to ascertain the true identities and legitimacy of their population. Yet, many organizations both in public and private sectors still rely heavily on their own constructed models of relevant online identities, which are based on captured data from single or multiple sources and transforming them into own data structures within their information systems.

With the revolution of digital networks, governments are realizing their roles to develop foundational infrastructure for digital identities. The term "digital identity" refers to a set of attributes and properties about an individual that are associated together and available in an electronic form to construct trusted digital credentials.

Evidently, governments have long played an authoritative role in identity provision in the physical world, and are now faced with demands to establish digital societies and identities in order to support e-government and e-commerce initiatives. It is the role of the government to associate digital identities to specific persons who will be authorized to perform certain actions in physical or digital forms.

This association is facilitated through digital certificates and digital signatures that altogether construct the digital identity. Thus many governments have considered PKI technology to establish and implement this binding through registration and digital certificate issuance process. In basic terms, PKI attaches identities to digital certificates for the purpose of assured, verifiable, and secure digital communications.

Public key infrastructure commonly referred to as PKI is an Information Technology (IT) infrastructure and is a term used to describe the laws, policies, procedures, standards, and software that regulate and control secure operations of information exchange based on public and private keys cryptography [4] . Table 1 summarizes the primary elements that make up the PKI components. The term PKI is used in this article to refer to the comprehensive set of measures needed to enable the verification and authentication of the validity of each party involved in an electronic transaction.

Table 2. Basic PKI Components

Component	Description
Digital Certificates	Electronic credentials, consisting of public keys, which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.
Certification Authoritie(S) – CAs	Trusted entities or services that issue digital certificates. When multiple CAs are used, they are typically arranged in a carefully prescribed order and perform specialised tasks, such as issuing certificates to

	subordinate CAs or issuing certificates to users.
Certificate Policy and Practice Statements	Documents that outline how the CA and its certificates are to be used, the degree of trust that can be placed in there certificates, legal liabilities if the trust is broken, and so on.
Certificate Repositories	A directory of services or other location where certificates are stored and published.
Certificate Revocation Lists (CRL)	List of certificates that have been revoked before reaching the scheduled expiration date.

PKI offers high levels of authentication of online users, encryption and digital signatures, which also support the maintenance of elevated echelons of data privacy, streamline workflow and enable access. The cornerstone of the PKI is the concept of private keys to encrypt or digitally sign information. One of the most significant contributions a PKI has to offer is non-repudiation. Non-repudiation guarantees that the parties involved in a transaction or communication cannot later on deny their participation.

PKI, in general, has grown both more slowly and in somewhat different ways than were anticipated [5]. It has had some success stories in government implementations; the largest PKI implementation to date is the Defence Information Systems Agency (DISA) PKI infrastructure for the Common Access Cards program. Many researchers pointed out the complexity of PKI, and that it is only sound in theoretical terms. We definitely do not agree with those who claim that PKI cannot be practiced and yield effective results. As with any technology, PKI is not without its own security risks due to its complex architectures. Indeed, there is no bullet-proof technology that could provide us with a fault free solution and meet all of our security needs.

In fact, studies conducted by academics and practitioners remain passionate about the promises of PKI to revolutionize electronic transactions (see for example. Undoubtedly, published studies in the existing literature contributed significantly to the development of the technology and explain its benefits. Nonetheless, those studies are believed to remain very much handy to technical researchers.

This is to say that although an awful lot of articles were written on this topic, they seem to be written to improve and develop theoretical frameworks while others tackle narrowed technological issues.

Looking at these studies, we note that although such research efforts have been comprehensive in specific areas, they do not assume a standard or a uniformed PKI approach. Interestingly, some researchers pointed to the fact that this field lacks fundamental theories to guide the development of clear path for PKI

practice in our world [8].

Others explain lack of adoption and wide failures in PKI industry to be due to not having enough PKI applications with clear business cases to support the roll out of the infrastructure [9]. Therefore, many implementations reported to have produced unnecessary costs when implemented without clear business cases [10]. Apparently, with the increasing complexity, the implementation of PKI systems becomes extremely challenging in light of the limited documented experiences that have included inefficient and short living implementations, with no clear ROI cases.

CONSIDERABLE PKI SERVICE IN BANGLADESH

Considerable PKI Service in Bangladesh [3]

– Government Procurement System

– Utility Bill Payment -Gas & Electricity

– Law Web Portal

– Process Automation –Bangladesh Bank

– Automatic Clearing House –Bangladesh Bank

– Bangladesh Post Office Online

– Service Ticketing System

MATERIALIZING PKI IN BANGLADESH

1. Spread – general use

The objective should be to make the use of digital certificates general and widespread. Experiments by other nations of the use of smart cards in transactions between the public sector and the general public, where individuals are expected to buy the cards, have failed [7]. Presumably, there are obstacles involved concerning both price and effort. However, in order to maintain a high level of security, some effort must accompany the process of identifying people through the appropriate method and delivering the certificate into the right hands. Innovative ways should be sought to stimulate the use and spread of digital signatures among the public and in the economy.

2. Market solutions – active competition. Versatile digital certificates

The objective should be that the public can use their digital certificates when communicating with the state, regardless of who issued the certificates and as long as they meet the conditions applied. This should be ensured by making requirements about the content and form of certificates and rules about their handling, which need to be met before they are accepted in communication with public institutions. The requirements should be based on European and international standards, and modelled on requirements made by other Nordic countries, e.g. Sweden. The requirements can be set forth either in framework agreements or a regulation based on the law.

3. The appropriate level of security - acceptable cost

A common mistake when implementing security systems such as public keys is to determine a certain level of security in advance and then choose a solution and apply it to the whole management. There is no single solution that works everywhere. Therefore, it is necessary for institutions to have a risk analysis carried out for each part of the activity and then choose the appropriate security system with regard to acceptable cost and results of the analysis. The financing of the system has to work, preferably so that the cost of participants is proportionate to the benefits realised by taking up the methods of e-government. In Sweden, a system is being implemented where the state is expected to accept certificates issued by or for others, in whose interest it is to deliver digital certificates to people. These others might be the commercial banks, various organisations etc. Government institutions will pay a fee to certificate authorities for the verification of signatures when electronically signed documents are received. Thus, the digital certificates of individuals can be used for a variety of services and communications.

CONCLUSION

Through this paper we have shown the importance of PKI for establishing e-governance in Bangladesh. In order to materialize PKI in Bangladesh we have proposed some methodologies such as spread-general use, market solution - active competition-versatile digital certificate, the appropriate level of security-acceptance cost. Though the vision of Digital Bangladesh can be achieved faster, we have aligned ourselves with Bangladesh Government vision of 2021. In future we shall try to reduce the time frame for achieving Digital Bangladesh.

References

[1] United Nations E-Government Survey 2012--E-Government for the people.

[2] OUTLINE PERSPECTIVE PLANS OF BANGLADESH 2010-2021 MAKING VISION 2021 A REALITY (Final Draft).

[3] PKI, Digital Signature & E-Government by Prof. Bae, Kyoung Yul (Sangmyung University), July 2011.

[4] Brands, S.A. (2000) Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press.

[5] Wilson, S. (2005) "The importance of PKI today", China Communications [Online]. Available from: www.china-cic.org.cn/english/ digital%20library/ 200512/3.pdf. Accessed: 01 February 2011.

[6] R. Anderson, B. Crispo, J. Lee, C. Manifavas, V. Matyas, F. Petitcolas, The Global Internet Trust Register, MIT Press, 1999.

[7] From the security policy for E-Government in Iceland [Online]. Available from: www.fjarmalaraduneyti.is/media/Utgefin_rit/PKI-Iceland.doc

[8] Nana, S. & Unhelkar, B. (2003) Progress Report on Development of Investigations Theory of PKI" and its applications to Australian Information Systems.

[9] Ashford, W. (2011) Why Public Key Infrastructure (PKI) has failed. ComputerWeekly [Online]. Available from: http:// www.computerweekly.com / blogs/read-all-about-it/2011/02/why-public-key-infrastructure.html. Accessed: 03 March 2011.

[10] Price, G. (2005) PKI Challenges: An Industry Analysis. Proceeding of the 2005 conference on Applied Public Key Infrastructure: 4th International Workshop: IWAP 2005.