# Seminar Paper
# On
# Implementing Digital Signature in Bangladesh: Issues and Problems


**Submitted by:**
**Md. Anwarul Habib**
**Deputy Secretary**
**Roll No.-134**


**126th Advanced Course on Administration & Development (ACAD)**

**Submitted to:**
**Dr.Mohammad Abu Yusuf**
**Member Directing Staff (R &C)**

**Research Supervisor**

**Dr. Mohammad Tarikul Islam**
**Associate Professor**
**Dept. of Government and Politics**
**Faculty of Social Science**
**Jahangirnagar University**

# To whom it may concern

This is to certify that Md.Anwarul Habib, Deputy Controller (Deputy Secretary), Controller of Certifying Authorities (CCA) bearing Roll number 134 of 126th Advanced Course on Administration and Development (ACAD) has prepared this seminar paper title on: **Implementing Digital Signature in Bangladesh: Issues and Problems.** The paper has been prepared under my direct supervision and guidance accomplishing all the activity satisfactory. The quality of the paper is above satisfaction to me and course management can accept the paper as a fulfilment of the course.

I wish him every success.

8.9.19

(Dr Mohammad Tarikul Islam)
Associate Professor and Research Consultant
Department of Government & Politics
Jahangirnagar University
&
Research consultant
126th Advanced Course on Administration and Development.

# Acknowledgements

Being assigned by the course management of 126th Advanced Course on Administration and Development to present a seminar paper, I have done it accordingly. To prepare this paper some individuals have helped me a lot to whom I am grateful.

My first acknowledgement is to the creator Almighty Allah.

I am also grateful to our course adviser Dr. Md. Zafar Iqbal ndc (MDS) and Dr. Mohammad Abu Yusuf (MDS) for their time to time advice and guideline to prepare this research paper.

I am very grateful to Dr. Mohammad Tarikul Islam, who is my supervisor of the seminar paper during the course. As a helpful and sincere guide, he helped me in my study and preparing this paper. Without his help this seminar paper will not come to a polish shape rather than a row report.

I am also thankful to course director Dr. Mohammed Amjed Hossain, course coordinators Md. Atikuzzaman and A.T.M Arif Hossain, for their valuable suggestions to write a correct seminar paper.

I have received a lot of helpful information from The Office of the Controller of Certifying authority and would like to thanks all officers specially Ms Naznin Akhter, Assistant Engineer for providing information and assistance she made during the study.

**Title: Implementing Digital Signature in Bangladesh: Issues and Problems.**

**Abstract:** Establishment of good governance is one of the major agenda of our present government Without proper using of information technology it can't be achieved. So the government has given top priority to develop ICT sector since 2009. With the increase of IT base activity data security is a big issue. Digital Signature has a very close relation with data security. To introduce digital signature CCA office was created in 2011 as per ICT Act-2006. But the progress was very slow in implementing digital signature. To identify the reason this research work has been conducted. By this research we try to explore the answer of two questions that is (1) To what extent digital signature set in action in Bangladesh and (2) How the relevant stakeholders (CCA and CA's) will work to make digital signature across level. I try to explore the possible reason by taking interview from three private CA's of our country. The study has been conducted mainly based on literature review. From the study it has been revealed that the present ICT Act didn't address use of Digital Signature as an obligatory action. Another obligation is our root certificate is not trusted and hence customers do not use certificates from our CA's and there is not enough PKI enabled applications.

**Key words:**

ICT : Information and Communication Technology
CCA : Controller of Certifying Authorities
CA : Certifying Authority
PKI : Public Key Infrastructure

**Introduction and Literature Review:** Information and communication technology plays a vital role in development all over the world today. Out government also realize this issue very seriously and vows to build digital Bangladesh by 2021 and to upgrade to a middle income country. Bangladesh step-up from a low income to a lower-middle income country in July 2015.Now our target is to upgrade to a middle income country by diversified use of information technology by 2021.Our ultimate target is to build a develop rich country by 2041.

Implementing "Vision-2021" and "Digital Bangladesh" is a political commitment of our government. Bangladesh Awami League declared to build Digital Bangladesh by 2021 in their election manifesto in 2008 before 9th parliament election and it become mandatory for government to implement when they came in to power in 2009. To ensure equal opportunity to all, poverty eradication, quality in healthcare, quality in education, overall development, create new job opportunity and to build knowledge based society government works continuously till 2009.

As a part of government commitment to build Digital Bangladesh and we are now on the way to facilitate e-commerce, e-transaction, e-procurement, and to establish e-government. To ensure legal validity and security of this new technology in 2011 Office of the Controller of Certifying Authorities was established as per "Information and Communication Technology Act, 2006

(amendment). This act gives the legal validity of Digital Certificates which is used for signing of Documents. The whole process will be done by the Certifying Authorities created as per direction of the ICT Law. The jurisdiction and legal enforcement of the Certifying Authorities are clearly given in the Act.

Any online activities authentication and secrecy has ensured by digital signature certificate. There is a provision to attested electronic record by information and communication technology act 2006 (amendment-2013) section-5.As per national Information and communication technology policy-2009, section 48 & 49 necessary initiatives has taken to ensure electronic filing system and other e-governance activity. Different government organizations has already taken initiative on various online activities such as software development, online application, different types of service, license & registration as a part of e-governance.

As per law CCA (Controller of Certifying Authorities) office acts as root CA which formulates policy, guidelines control and monitoring of CA's (Certifying Authority). In 2011 six certifying authorities got license from CCA office to provide digital signature certificate for consumer level. These are: Mango Teleservice Ltd, Dohatec New Media, Data Edged Ltd, Banglaphone Ltd, Computer Services Ltd and Bangladesh Computer Council (Government Organization).

Implementing digital signature is yet a big problem in our country. Though 6 (six) Certifying Authority got license from CCA office to provide digital signature certificate to consumer level but their activity is not up to the mark. Only 242 certificates are now active which is very disappointing.

In Asia India, Indonesia, Malaysia, South Korea has already introduced digital signature. Indian CCA was form in 2001.Initially they have face similar problem like Bangladesh. After long time now they are able to implement digital signature up to a label. In Bangladesh use of digital signature in not mandatory in e-services, so mass people are not very much interested to use this new technology. Generally mass people are always reluctant to take any new technology that may be a major cause for not using the digital signature.

**Problem statement:** Though digital signature is a new technology, it has a great advantage.
Here is a comparative chart of advantage of digital signature over paper based signing *(https://www.globalsign.com/en/resources/digital-signatures-for-aec-guide.pdf)* .

| Sl. | Paper based signing. | Digital signature |
|---|---|---|
| 1. | For paper based signing cost of printing, copying, postage, storage, filing, recycling, etc are higher. | On average, digital signatures reduce cost and time. |
| 2. | High chances of fraud | Create tamper-evident, time stamped, legally-binding documents |

| | | |
|---|---|---|
| 3. | More time required for preparing, organizing, and archiving files | Reduce time for printing, mailing, archiving and paper cost reduced. |
| 4. | Possibility of modification of documents during multiple steps of printing, scanning, and signing | No risk of modification of documents |

To work with digital signature at first a person need a digital certificate from a certified CA t digitally sign a document *(https://www.aeteurope.com)*. Digital certificates are like online passpo and digital signatures are like online notarized signature. Verification of client's identity is done b the CA serves and its act as the notary. Trusted timestamp verifies the date and time when th signature was applied. When a digital signature was applied a cryptographic operation binds hi digital certificate and the data being signed into one unique fingerprint. The main characteristic c digital signature is:

(1) Authentication: As the signature is verified by a third party, recipients know it was actuall you who signed it.
(2) Non-repudiation: As a CA certificate was used to sign the document, one cannot later clai that it wasn't he who signed.
(3) Message integrity: During verification it checks that the data in the original document, even a little change to the original document would cause this check to fail.

Besides this if we can able to introduce digital signature we can get the following facilities
(1) A strong barrier to start e-commerce will eradicate
(2) Facilitate online transaction
(3) Introducing in e-tender will stop tender manipulation.
(4) Tax return submission will be easier; as a result tax payer as well as government revenue earnin will be increase.
(5) Digital achieving, so that any transaction or document can be located easily.
(6) Paperless office
(7) As all transaction will be done by digital signature so it reduces extremism, terrorism and mone laundering this is big and very important issue around the globe.
(8) Helps to detect and reduce cyber crime.

**Objective:**

(1) The objective of this study is to find out the barrier to introduce digital signature in Bangladesh.
(2) Find out the possible steps to make it popular from government side and the other stakeholders.

**Research Question:** The study is looking at answering the following questions-

(1) Barrier to introduce digital signature Bangladesh?
(2) How the relevant stakeholders (CCA and CA's) will work to make digital signatu popular?

**Rationale of the study:** As a Government organization Information and Communication Technology Division plays the vital role in building Digital Bangladesh. Build a happy, prosperous, hunger and corruption free Bangladesh was the dream of Father of the Nation Bangabandhu Sheikh Mujibur Rahman .To make his dream into reality Government has taken various initiatives in the last 10 years to improve ICT backbone in the country. Without ICT backbone better service delivery and benefits of various development is impossible to reach to the mass people. To build up "A Digital Bangladesh within the year 2021" in charter of change of days in the year 2008 the honorable Prime Minister outlined the Digital Bangladesh having four priorities and created ICT Division in 2011 under ministry of Post, Telecommunication and Information Technology.

Building Digital Bangladesh and IT based society ICT Division has chosen 4 major fields as their target, these are (1) To establish high speed internet connectivity all over the country so that every citizen get the internet access easily. (2) To build an expert young IT based manpower to face the future challenges (3) Ensure e-governance by using information and communication technology. (4) To promote IT based industry. By optimum use of digital technology government is firm to reach every door of the people to provide them services. ICT division works continuously to upgrade Bangladesh to a middle income country by 2021. This Division also emphasis to achieve goals of SDG by 2030 and to build a develop country by 2041. Bangladesh is now gradually entering into a knowledge base economy from labor base economy.

Data Security is a big issue in e-services. To ensure data security by imposing digital signature CCA office was established in 2011 like other countries of the world. Activities of Controller of Certifying Authority are clearly defined in the ICT Act-2006. Section19 of ICT Act 2006 says,

(a) Exercising supervision over the activities of the certifying authority ;
(b) Laying down the standards to be maintained by the certifying authority ;
(c) Specifying the qualifications and experiences which employees of the certifying authority's should possesses;
(d) Specifying the conditions subject to which the certifying authorities shall conduct their business;
(e) Specifying the contents of written, printed or visual materials and advertisements that may be used in respect of a Digital Signature Certifying;
(f) Specifying the form and content of a Digital Signature Certificate;
(g) form and manner in which accounts shall be maintained by the certifying authorities ;
(h) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them for auditing certifying authorities ;
(i) Facilitating and establishment of any electronic system by a certifying Authority either solely or jointly with other either solely or jointly with other and regulation of such system.
(j) Specify the manner in which the Certifying Authorities shall conduct their dealing with their subscribers;

(k) Resolving any conflict of interests between Certifying Authorities and the subscribers;
(l) Laying down the duties and responsibilities of the Certifying Authorities' ;
(m) Maintaining computer based databases, which
  (i) Contain the disclosure record of every Certifying Authority containing suc particulars as may be specified by regulations; and
  (ii) Shall be accessible to the member of public;
(n) Perform any other function under the Act or Codes prepared under this Act.

As per the official records CCA office has already given license to 5 private organizations and government organization as Certifying Authority (CA) to provide digital signature at consumer leve and the organizations got CA certificates from CCA office after completing all formalities an completing technical infrastructure. After having licenses these organization starts to distribut digital signature to consumer and corporate level although the progress is very slow. So far the could sell only a few number of Digital Signature Certificate. All the six authorized CA hav distributed total 51,731 digital signatures among government officers and others from 2013 t October, 2018 which is valid for 1-2 years. Distribution of digital signature by various CA (6 nc since 2014 to October 2018 is shown in the table below.

**Year wise distribution**

| Year | Banglaphone Ltd | Dohatech New Media | Mango Tele Services Ltd | Dataedge Ltd | Bangladesh Computer Council | Computer Service Ltd | Tota |
|---|---|---|---|---|---|---|---|
| 2013-14 | - | - | 3 | 23,000 | - | - | 2300 |
| 2014-15 | 28 | 23873 | 60 | 1221 | - | - | 2518 |
| 2015-16 | 33 | 43 | 53 | 2040 | - | - | 216 |
| 2016-17 | 14 | 38 | 8 | 1150 | - | - | 121 |
| 2017-18 | 1 | 1 | 6 | 111 | - | - | 119 |
| 2018-19 Upto Oct/2018 | - | - | 5 | 43 | - | - | 48 |
| **Total** | **76** | **23955** | **135** | **27565** | - | - | **5173** |

But now only 242 digital signature certificates are active. CCA office tries to introduce digit signature in e-nothi, but due to some technical problem (interface) it does not work properly in nothi .

**Number of active digital signature certificate**

| Types of certificate | Banglaphone Ltd | Dohatech New Media | Mango Tele Services Ltd | Dataedge Ltd | Bangladesh Computer Council | Computer Service Ltd | Total |
|---|---|---|---|---|---|---|---|
| Class-1 | 1 | 0 | 0 | 79 | 0 | 80 | 80 |
| Class-2 | 45 | 9 | 35 | 13 | 0 | 0 | 102 |
| Class-3 | 4 | 10 | 4 | 42 | 0 | 0 | 60 |
| **Total** | **50** | **19** | **39** | **134** | **0** | **0** | **242** |

As a whole the picture of use of digital signature is very disappointing. So this study is taken to reveal the fact which is the barrier to use of digital signature and how to increase its use.

**Theoretical/Analytical/Conceptual Framework:** Digital signature is a new technology in Bangladesh. Even very little government employee and negligible number of mass people know about this new technology. They have no idea about the advantage and security of digital signature for various online services. This study try to reveal the actual cause of why digital signature in not popular and to recommend the possible ways to popular this new technology in our country for safe and hassle free e-services.

Digital signatures are basically "enciphered data" created using cryptographic algorithms. This algorithm creates a private key and public key pair. These key are linked in such a way that they performs inverse function to each other. The private key is used for signing purposes and the public key is used for verification of signatures. The private key should be kept carefully by the signer as he is the only user of the key.

To make digital signature popular to the mass people we have to take some initiative from both government and CA level.

**Definition of Digital Signature:**

A digital signature is a mechanism that is used to verify that a particular digital document, message or transaction is authentic *(www.aeteurope.com ,14-06-2017)*. It provides a receiver the guarantee that the message was actually generated by the sender and it was not modified by a third party. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI) , to provide the highest levels of security and universal acceptance.

**What is a digital certificate?**

Digital certificates are like identification cards such as passports or driving licenses. It is issued by recognized (government) authorities (CA). When someone needs a certificate he formally requests the certifying authority to provide a certificate with relevant documents *(www.aeteurope.com, 14-06-2017)*. Then the authority

verifies the identity of that person and if his entire document is perfect then they issue a digital certificate f him. Normally it contains the personal information of the used to identify and trace him.

**The use of a digital certificate to sign documents**

When the signer uses a certificate to digitally sign a document, other people (known as relyi parties) can trust the digital signature because they trust the CA has done their part to ensure t signer matches their digital identity.

**What is PKI:**

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedur needed to create, manage, distribute, use, store and revoke digital certificates and manage public-k encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for range of network activities such as e-commerce, internet banking and confidential email.

A PKI consists of:

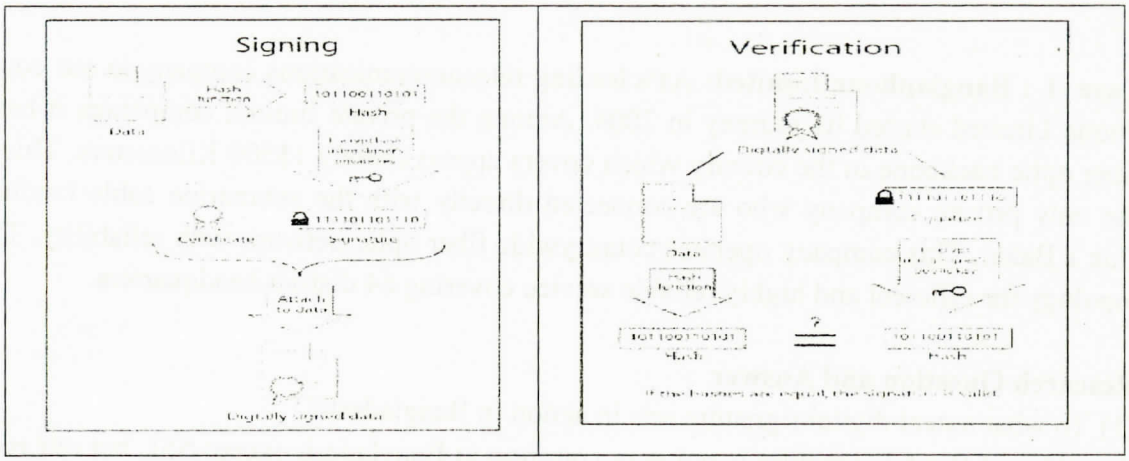
- A certificate authority (CA) that stores, issues and signs the digital certificates
- A central directory—i.e., a secure location in which to store and index keys
- A certificate management system managing things like the access to stored certificates or t delivery of the certificates to be issued.

**Private Keys:** For digital signature every user must have a private key. The public and private ke are linked up mathematically. The public key provides the authentication of the signer. It should kept secret and carefully otherwise any one can use this key to sign a document without sign consent.

**Public keys:** Public key is used to verify the identity of the signer in the receiving end. Signer c give his public key to anyone who wants to verify his signature.

**The digital signing process**

**Step1:** At first the document is converted to a hash-value by applying some cryptographic hashi algorithm *(https://www.signinghub.com › wp-content › uploads › 2017/05 › Basics-of-digit signature-and-PKI).* It consists of a sequence of bits which is originated from the document. In t transformation such mathematical transformations are used that if a single bit is changed from input document the original document can't be retrieved. For this reason it is impossible to char the document.




**Step 2:** Applying digital signature: Hash value obtained from the original document (first step) is then encrypted with the private key of the person who signs the document and thus an encrypted hash-value called digital signature is generated.

**DIGITAL SIGNATURE VERIFICATION:** Digital signature technology has the option of verification by the recipient of given signed document.

**Verification process**:

**Step 1:** Signed documents hash-value is calculated. Same mathematical algorithm is used as was used during the signing process. The obtained hash-value is called the present hash value as it is calculated from the present state of the document.

**Step 2:** The digital signature is decrypted with the help of same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key that was used during the signing of the message. As a result, we obtain the original hash-value .

**Step 3:** Then the system compare the present hash-value obtained from first step with the original hash-value obtained from second step, If the two values are identical, the verification is successful and proves that the message has been signed with the private key that corresponds to the public key used in the verification process. If the two values are different, this means that the digital signature is invalid and the verification is unsuccessful.

**Methodology:** The study has been conducted mainly based on literature review. Apart from this to substantiate findings based on literature review. At least 3 digital signature certificate providers are used and interviewed. For collecting the necessary information, two closed-ended questions were used.

**Case -1 : Banglaphone Limited:** As a leading telecommunications company in our country Bang Phone Limited started its journey in 2004. Among the private limited companies it has the large fiber optic backbone in the country which covers approximately 15500 Kilometers. This company the only private company who are connected directly with the submarine cable landing station Cox's Bazar. This company operates countrywide fiber optic network with reliability. They use ri topology for efficient and highly reliable service covering 64 district headquarters.

**Research Question and Answer**

(1) To what extent digital signature sets in action in Bangladesh?

Ans: Use of Digital signature is not very common in Bangladesh except SSL but our root certifica is not trusted and hence customers do not use SSL certificates from our CAs. Government is trying increase usage of DS but still we are in initial stage.

Personal use of DS is not very popular due to technical difficulties of using crypto token and there not enough PKI enabled applications.

(2) How the relevant stakeholders (CCA & CA's) will work to make digital signature across level?

Ans:

1. root certificate needs to be trusted to increase usage of SSL certificates
2. CCA and CAs should work on e-Sign because it will make things easy for customers
3. necessary modifications should be done in IT Laws
4. More use cases should be created in govt. sectors

**Case-2:Data-edge Ltd**

Data edge Ltd is another leading telecommunication company in Bangladesh which was establish in 2002. It provides various IT solutions in Bangladesh such as Banking and Non Banking Financi Institutions sector, Telecom, Multinational Companies, Pharmaceuticals, Govt. ICT Sector and Education Sector.

**Research Question and Answers**

(3) To what extent digital signature sets in action in Bangladesh?

Ans: As per ICT ACT digital signature legally sets in Bangladesh. Now at digital platfo digital signature use for legally authorization and authentication. Below few uses of digi signature in Bangladesh:

a) eTin: For eTin using digital signature. eTin subscriber getting digitally sign eTin.
b) eNothi: eNothi platform integrate with digital signature. For authorization of an eNo user digital signature.
c) RJSC: Register of Join Stock using digital signature certificate to provide digitally sign company certificate.
d) BUET: In various application BUET using digital signature certificate to authenticati and authorization.

e) National University :National University using digital signature certificate to authorized online documents.

(4) How the relevant stakeholders (CCA & CA's) will work to make digital signature across level?

Ans: Now for digital Bangladesh maximum Government to Citizen services are digitalized. Have to identify that applications and CCA , CAs can both work together to integrate digital signature on those applications.

**Case-3 Mango Teleservices Limited:** MANGO Teleservices Limited is another leading telecommunication company in Bangladesh. It started its journey in 2008 as the first private sector International Internet Gateway (IIG) operator. This company also works in the several government projects. Education, Real Estate, Hospitality Management and Banking Sector. This company started its operation as Certifying Authority (CA) from 19 January 2011.

**Research Question:**

(5) To what extent digital signature sets in action in Bangladesh?

We are not sure about other CA's statistics. However, may be have the highest no of DS in operation at present. But there are CA could sell none yet. Below is the summary of Digital Signature of Mango:

| Sl. No. | Company Name | No. of Issuance Certificate |
|---|---|---|
| 1 | Mango Teleservices Limited | 148 |

(6) How the relevant stakeholders (CCA & CA's) will work to make digital signature across level?

Ans: We think to make Digital Signature more popular and acceptable by concern users we need to reframe and amend the ICT Act 2006. Present ICT Act didn't address use of Digital Signature as an obligatory action, rather it patronize to use of Foreign Certificate rather than using our own. Some of the relevant clauses of the said act given below with our recommendation.

**ICT Act 2006, Clause 20 (1):** Clause 20 says about allowing companies to obtain digital signature or certificate from foreign CA. At present most of the companies are using certificate to secure their web or online resources from foreign CA such **Verisign**, **Comodo**etc. They neither took permission from CCA nor CCA is aware who is using who's certificate. This one hand allowing syphoning of foreign currency on the other hand native companies are drying for not getting any job. Government should not allow them any more without paying tax to our exchequer. Even if it is allowed, that should be for limited period, till the time native CA become capable of providing trusted certificate by themselves. Thus, we recommend to reframe the existing clause as given below:

Present description of Clause 20(1):

বিদেশী সার্টিফিকেট প্রদানকারী কর্তৃপক্ষকে স্বীকৃতি

২০।(১) প্রবিধান দ্বারা নির্ধারিত শর্ত সাপেক্ষে, সরকারের পূর্বানুমোদনক্রমে এবং সরকারী গেজেটে ও তদতিরিক্ত ঐচ্ছিকভাবে ইলেক্ট্রনিক গেজেটে প্রকাশিত প্রজ্ঞাপন দ্বারা, নিয়ন্ত্রক বিদেশী কোন সার্টিফিকেট প্রদানকারী কর্তৃপক্ষকে এই আইনের অধীন একটি সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ হিসাবে স্বীকৃতি প্রদান করিতে পারিবে।

(২) উপ-ধারা (১) এর অধীন কোন বিদেশী কর্তৃপক্ষকে সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ হিসাবে স্বীকৃতি প্রদান করা হইলে, উক্ত কর্তৃপক্ষ কর্তৃক ইস্যুকৃত ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট এই আইনের উদ্দেশ্য পূরণকল্পে বৈধ হইবে।

(৩) নিয়ন্ত্রক যদি এই মর্মে সন্তুষ্ট হন যে, কোন সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ উপ-ধারা (১) এর অধীন আরোপিত যে শর্তের অধীন স্বীকৃতিপ্রাপ্ত হইয়াছে উহার কোন শর্ত লঙ্ঘন করিয়াছে, তাহা হইলে তিনি, লিখিতভাবে কারণ লিপিবদ্ধ করিয়া, সরকারী

We recommend to reframe as under:

**২০।(১) প্রবিধানদ্বারানির্ধারিতশর্তসাপেক্ষে, সরকারের পূর্বানুমোদনক্রমে এবং সরকারী গেজেটে তদতিরিক্ত ঐচ্ছিকভাবে ইলেক্ট্রনিক গেজেটে প্রকাশিত প্রজ্ঞাপন দ্বারা নিয়ন্ত্রক বিদেশী কোন সার্টফিকে প্রদানকারী কর্তৃপক্ষকে এই আইনের অধীনে একটি সার্টফিকেট প্রদানকারী কর্তৃপক্ষ হিসাবে সাময়ি সময়ের জন্য ( দেশীয় সিএদের সক্ষমতা অর্জনের পূর্ব পর্যন্ত সময়ের জন্য) অনুমতি প্রদান করি পারিবে।**

1. ICT Act 2006, Clause 67: The clause 67 described about what is mean by the word "Compan in this act. We recommend to add one more sub clause under clause 67 so that companies a made liable to implement 'Digital Signature' at their own interest. We believe that if 'Digi Signature' is implemented, possibility of violating this act will be lesser. Thus, we recomme for adding one more sub clause under clause 67:

Present description of the Clause 67:

কোম্পানী, ইত্যাদি কর্তৃক অপরাধ সংঘটন

৬৭। কোন কোম্পানী কর্তৃক এই আইনের অধীন কোন অপরাধ সংঘটিত হইলে উক্ত অপরাধের সহিত প্রত্যতগ সংশিস্ন্ষ্টতা রহিয়াছে কোম্পানীর এমন প্রত্যেক পরিচালক, ম্যানেজার, সচিব, অংশীদার, কর্মকর্তা এবং কর্মচারী উক্ত অপরাধ সংঘটিত করিয়াছেন বলিয়া গণ্য হইবেন, যদি না প্রমাণ করা যায় যে, উক্ত অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছে অথবা উক্ত অপরাধ রোধ করিবার জন্য তিনি যথাসাধ্য চেষ্টা করিয়াছেন।

ব্যাখ্যাঃ এই ধারায়-

(ক) "কোম্পানী" বলিতে কোন বাণিজ্যিক প্রতিষ্ঠান, অংশীদারী কারবার, সমিতি, সংঘ এবং সংগঠনও অন্তর্ভুক্ত হইবে; এবং

(খ) বাণিজ্যিক প্রতিষ্ঠানের তেগত্রে "পরিচালক" বলিতে উহার কোন অংশীদার বা পরিচালনা বোর্ডের সদস্যকেও বুঝাইবে।

We recommend to add one more sub clause as under:

৬৭(১) বাংলাদেশের ভুখণ্ডে পরিচালিত সকল কোম্পানির তথ্য, দলিলদস্তাবেজ, আর্থিক লেনদেন ইত্যাদির নিরাপত্তা, স্বচ্ছতা, দায়বদ্ধতা এবং জবাবদিহিতা নিশ্চিত করার লক্ষ্যে অনুমোদিত সিএ কর্তৃক স্বস্ব ইলেক্ট্রনিক বা অনলাইন সিস্টেমে সংশ্লিষ্ট ব্যক্তিদের পরিচয় নিশ্চিত করার জন্য 'ডিজিটাল সিগনেচার' বাস্তবায়ন করা বাধ্যতামূলক।

(২) কোন কোম্পানী কর্তৃক এই আইনের অধীন কোন অপরাধ সংঘটিত হইলে উক্ত অপরাধের সহিত প্রত্যক্ষ সংশ্লিষ্টতা রহিয়াছে কোম্পানীর এমন প্রত্যেক পরিচালক, ম্যানেজার, সচিব, অংশীদার, কর্মকর্তা এবং কর্মচারী উক্ত অপরাধ সংঘটিত করিয়াছেন বলিয়া গণ্য হইবেন, যদি না মান করা যায় যে,উক্ত অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছে অথবা উক্ত অপরাধ রোধ করিবার জন্য তিনি যথাযথ 'ডিজিটাল সিগনেচার' বাস্তবায়ন করেছেন।

Clause-13 and Cluase-14 Need to rephrased and re-written since the clauses are ambiguous. Based on the concept these clauses can be written specifically for-

- Email transactions
- OCSP/CRL verification between sender and recipient transactions

Clause 15- In modern mobile computing this clause needs to be updated since location and transaction sources are variable

Cluse-19: New activities of CCA need to be added such as-

- Partnering and acknowledgement with international trusted root CA communities, states or organizations so that modern browser, operating system or other suitable applications may be seamlessly used by the end users.
- International cross certification program/initiative
- Centralized certificate online repository (though it is mentioned in the first para of Cluase-21)

Clause-30: Need to consider mobile/portable devices too.

Clause-46, Sub-Clause (2)- decryption is practically not possible unless CA holds both private and public key pairs.

Clause-54, 55, 56, 60, 61 & 66: Need to consider mobile/portable devices too.

**Findings of case study:**

After analyzing the answer from the three CA's. It was found that the major obstacle for implementing digital signature is

1. Root CA Certificate should be trusted.
2. According to the ICT Act Digital Signature is not an obligatory action.
3. Inadequate PKI enable applications as local software developer company has few knowledge on PKI.
4. Lack of awareness about benefit of Digital Signature.

5. Lack of awareness on cyber security among the online users.
6. Digital signature and PKI system is not user friendly.

**Implications and Recommendations:**

1. Some clause of ICT Act-2006 such as Clause should be amended.
2. International recognitation of Root CA (CCA).
3. Introduction of e-sign.
4. Introduction of mobile PKI.
5. Co-ordination with concern authorities to implement digital signature in e-Nothi,e-GP, e-Ta RJSC.
6. Take necessary action to introduce digital signature in all banks, financial institutions a online service delivery agency.

**Conclusions:**

Man is usually unwilling to accept any change or any new technology. Digital signature is a ne technology and not very user friendly. That's why mass people are not interested to use digit signature. To encourage the people massive campaign, showcasing, advertisement in need for bo government side and certifying authority side. Some incentive may give for the digital signatu users. Thus we hope that we can reach to a level with very short time. So far I know this sort research I have conducted for the first time in order to manage available data, I have no other choi to consult relevant scholarship to substantiate analysis. I am sure with my research work, futu generation researchers will be benefited to carry out in depth undertaking.

**References:**


1. <*https://www.aeteurope.com › news › digital-signature-digital-certificate*> accessed on 08-08-2019
2. <*https://www.signinghub.com › wp-content › uploads › 2017/05 › Basics-o...*> accessed on 17 08-2019
3. <*https://docplayer.net › 42321742-An-introduction-to-digital-signatures-for...*> *accessed on 20-08-2019*
4. <https://en.wikipedia.org/wiki/Digital_signature> accessed on 25-08-2019
5. *Information & Communication Technology Act, 2006.*
6. *Annual Report: office of the Controller of Certifying Authorities,2016-17*
7. *Annual Report: Information and Communication Technology Division, 2016-17*