



**East West University**

A/2, Jahurul Islam City, Aftabnagar, Dhaka 1212

Intern report on

**Digital Signature Certificate of dataedgeid of data edge Ltd**

Submitted to:

Dr. M. Mofazzal Hossain

Associate Professor

Department of Electronics & Communication Engineering

Submitted By:

Arif Arman

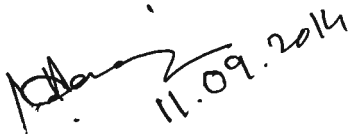
ID: 2009-2-55-030

Date of Submission:

11<sup>th</sup> September 2014

## Acceptance of Report (Supervisor)

This internship report presented to the Department of Electronics and Communication Engineering, East West University as a partial fulfillment of the course ETE-498 ( Industrial Training ) as well as for the Bachelor of Science Degree in Electronics and Telecommunications Engineering (ETE).

  
11.09.2014

---

Dr. M. Mofazzal Hossain

Professor

Electronics & Communication Engineering

East West University

Dhaka

## Approval of Report (Company Supervisor)

This internship report is prepared by Arif Arman, Department of Electronics & Communication Engineering, East West University, Dhaka, Bangladesh. He worked as an intern in dataedge Certifying Authority, in our company data edge Ltd. under my supervision.

As per my knowledge this report will partially fulfilled the requirement for completion of the academic course ETE-498 (Industrial training) for his B. Sc. Degree.

This report is approved and accepted. I wish him every success for his future endeavor.



---

**Samiran Chakraborty**

Manager

CA Operation

data edge Ltd

# Acknowledgement

---

First I would like to express my gratitude to almighty ALLAH for giving me the strength to perform my responsibility as an internee and complete the report within due time.

My special thanks goes to supervisor **Dr. M. Mofazzal Hossain**, Dean and Professor of Electronics and Communications Engineering, East West University, Dhaka who was my academic supervisor for the course ETE-498 (Industrial Training). He allocated valuable time throughout the internship period to guide me for successfully completion of the internship and preparing the report.

I would specially like to convey my company supervisor **Mr. Samiran Chakrabarty**, manager of dataedge CA who gave the opportunity of the internship under his department and guiding me with lots of effort and time.

Last but not the least; I would like to convey my gratitude to my colleagues, friends and teachers who gave good advices, suggestions, inspections and support.

Arif Arman

**Intern Report on**  
**Digital Signature Certificate of dataedgeid of data edge limited**

**Abstract**

This intern report represents the concepts of Digital signature Certificate along with SSL and Public Key Infrastructure and their implementation in Bangladesh. Public Key Infrastructure provides a model of secured network of communication where an individual or a organization can transmit and receive data securely and Digital signature Certificate is the key by which an individual or organization can get the access to the network for secure transmission of data. Moreover it contains a idea of the Public Key Infrastructure in Bangladesh published by Office of the Controller of Certifying Authority (CCA) under ICT Division of Bangladesh government and Certificate Practice Statement of data edge ltd. To do analysis with practical work, some related theories are discussed in this intern report.

Table of Content		
Chapter	Titels	Page
1.Company profile	1.1 At a glance	2
	1.2 Products and Services	2
	1.3 Focus Area	5
	1.4 Clients	6
	1.5 Alliances	7
2.Public Key Infrastructure	2.1 Introduction	9
	2.2 The Cryptographic Building Block	9
	2.3 Definition:	11
	2.4 The PKI Architecture Model	11
	2.5 PKI Management Function	14
	2.6 PKI Management Protocol	15
	2.7 PKI Certificate Discovery and Validation Protocols	17
	2.8 PKI in Bangladesh	17
3.Digital Signature Certificate	3.1 Definition	23
	3.2 Applications of digital signatures	23
	3.3 Putting the private key on a smart card	24
	3.4 Digital signatures vs. ink on paper signatures	25
4.Certificate Practice Statement of dataedgeid	Certificate Practice Statement	26
Conclusion		27

# Chapter 1

## Company Profile



## **1.1 At a glance:**

In the span of 10 years of operation data edge limited, a Super brand, has been credited with pioneering some major turn-key ICT projects that includes Bangladesh Automated Clearing House (BACH), Machine Readable Passport and VISA, Payment Card Solutions & Core Banking Systems, Call Centre Solutions for Telco's, etc.

Now, dataedge is providing Digital Certificate & Digital Signature along with required solutions and services under the brand dataedgED. dataedge has invested in cutting-edge technology platform and skill acquisition to achieve global operational standards and reliable services to it's customers. dataedgED is ready to serve the country's first authenticity & security based solutions.

## **1.2 Products and Services:**

### **Core Banking Solution:**

dataedge represents Oracle Financial Solution's (formerly i-flex solutions ltd.) FLEXCUBE—the number one core banking solution in the world as per IBS (UK) rating since 2002, as well as other solutions portfolio from i-flex. i-flex is currently an Oracle Company having more than 700 customers across 130 countries. FLEXCUBE supports the complete business operations of commercial banks including retail, corporate & treasury operations as well as interfacing with all common delivery channels. Based on open systems and providing customers a wide range of choice of hardware & OS, FLEXCUBE ensures one of the lowest Total Cost of Ownership (TCO) and highest Return on Investment (ROI) in the industry. dataedge has successfully marketed i-flex's products and services to several major private sector banks in the country with all the banks running successfully for 3 years or above.

### **Payment Card Management and ATM Switching Solution:**

dataedge represents Payment Card Management and ATM switching solutions from TietoEnator Corporation. Immensely modular, the solution can be used for a number of business purposes by banks (issuers and acquirers), financial institutions with in-house processing infrastructure, as well as multi-bank processing and clearing centers. Openness in hardware and OS platforms enabling seamless API, reliable technologies (Oracle, BEA Tuxedo), immense scalability in line with card business development, compliance with international standards (VISA, Master, Amex and EMV readiness), support for all standard ATM and POS protocols, etc. makes our solution unique and attractive.



### **Telephony, Voice & Call Centre Solutions:**

dataedge represents Avaya GlobalConnect Limited, and offers full range of AVAYA contact center/call center graded switch, AVAYA IVR and CTI, Video and Audio conferencing and Voice logging solutions. dataedge also partners with Servion Global Solutions, offering end-to-end call center solutions to customer focused companies as part of their business response solution.

Depending on customer requirements, dataedge offers complete call center/telephone banking solution to the Telecoms, Banks and other service providers based on Avaya and/or Servion components. We have customers in both telecom & banking sector using our solution.

### **Surround Applications for Banking Industry:**

Apart from Integrated Core Banking Applications, dataedge also provides the full range of surround applications that a bank may need from leading solution providers in the world. Such solutions include Data Warehouse System/Reveleus from Oracle Financial Solutions, Lending Application Processing System/LAPS from SysArc Infomatix Pvt Ltd., Credit Risk Management System/Cream from Digital Business Solutions W.L.L., Debt Management and Recovery Solutions from Porfitera, etc.

### **Card Personalization Solution:**

dataedge represents card personalization solutions from Matica-Digicard. Matica offers a wide range of products as per customer's requirement for production volumes and speed and currently provides world's fastest card production machine. Matica products offer immense versatility in terms of single pass or multiple pass production, photo-printers, combined embossing and photo printing, combined embossing, indenting, etc. The equipment and printing software offered by Matica has built-in EMV support ensuring investment protection for customers who are currently using Magstripe, but plans to move to EMV at a later stage. Matica systems are also certified with world's leading EMV solutions. Several banks are already using our Card Personalization Solutions.

### **Enterprise Server & Storage Hardware, IT Infrastructure Management and Optimization Solutions:**

dataedge also partners with Hewlett-Packard (HP) for providing Enterprise Server and Storage (SAN, NAS) Solutions as well as IT Infrastructure Management and Optimization Solutions to its wide customer-base. HP is world's leading brand in terms technology innovations, product portfolio and performance. dataedge has a strong team well-versed with the HP range of hardware and software products to identify customer requirements, assess performance matrices, growth and capacity trend and chose the right products and solutions for the customer. With world's leading application solutions running on running on world's leading and most reliable hardware and IT management solutions – dataedge's offering remains unmatched in this market!

### **ATM, POS & HSM Products:**

dataedge partners with various ATM, POS & HSM solution providers while providing end-to-end payment card network infrastructure to its customers. dataedge has a strong support team providing support for its ATM, POS, HSM and Card Embossing and Printing Hardware Solutions. The team is also

well-versed with the integration between the hardware & software components, key management complexities related to the overall solution, etc.

#### **Digital Certificates and PKI (Public Key Infrastructure) based solutions:**

As a sales affiliate of SafeScript and Safenet dataedge offers and implements Digital Certificates and PKI (Public Key Infrastructure) based solutions. The offerings include Integration of the certificates into applications ranging from e-mail systems to intranets, VPNs, ERP systems or any other customer applications. Security through PKI solutions to a wide range of business to consumer (B2C) and business to business (B2B) applications over the Internet.

#### **Juniper, HP, 3Com, Extreme, CISCO & Allied Telesyn Registered Partner:**

As the registered partner dataedge markets full range of Juniper, HP, 3Com, Extreme, CISCO & ATI networking products in Bangladesh. Using its expertise and experience, dataedge can currently offer the best value for money to clients taking into account the customer's business requirements, mission criticality, response requirements and budget and sizing the network accordingly.

#### **Fiber and Twisted Pair Cabling:**

A robust network infrastructure is the heart of any mission-critical business enterprise. dataedge partners with world's leading Network Component Manufacturer, AMP NETCONNECT (Tyco Electronics) to provide design and implementation of end-to-end passive network cabling for enterprises comprising of Twisted Pair and/or Optical Fibre cabling along with all accessories and components as required. dataedge also promotes customers to undergo proper "Certification of Cabling" to ensure quality and longevity.

#### **Unified Threat Management (UTM) Solutions:**

dataedge offers end-to-end security solutions in Bangladesh market offering world's leading hardware and software based solutions including Check Point Software, Fortinet, Cyberoam, Websense & others. As authorized resellers dataedge also provides several anti-virus solutions to customers based on customer's requirements such as Symantec, e-trust and escan.

#### **Bandwidth Management and Network Acceleration Solutions:**

In today's highly connected world, it is absolutely necessary to manage the expensive bandwidth and ensure that applications use bandwidths optimally by removing bottlenecks and accelerating the application performance where possible. dataedge represents world's leading bandwidth management and network acceleration solutions from Packeteer, Blue Coat and Allot Communications.

#### **Custom Software Application Development:**

Besides providing support for its enterprise applications supplied by partners, dataedge also consists of a strong software development team developing various surround and complimentary solutions for its customer-base that include HR & Payroll Management System, Finance and Accounts application, Fixed Asset Management System, Portfolio Management System, ALCO System, Foreign Exchange Reporting

System, Collection Monitoring, etc. dataedge endeavours to put into its offered products the best practices, flexibility and enriched functionality experienced through working with global products.

#### **Data Center Infrastructure:**

dataedge immense expertise on design and implementation of data center and data recovery site infrastructure. We have the solution of all related products data center including Raised Floor, Uninterrupted Power System, Precision Air Cooling System, Power Generator, Surge Protection System, Automatic Detection and Protection Fire System, Environment Monitoring and Controlling System, Structured Cabling with CAT 7 or fiber cable, Floor Insulation System, Access Control System, IP Surveillance System, Electrical, Earthing and Grounding System, Civil Works etc.

#### **Project Management/IT Service Management:**

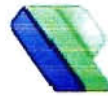
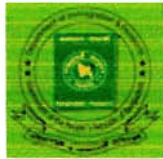
Based on background and professional expertise of individuals dataedge also provides outsourced Project Management and IT Service Management Services to multitudes of customers. For specialized projects dataedge also partners with Accenture, Price Waterhouse Coopers, Planetcom and other reputed SIs for Project Delivery.

### **1.3 Focus Area:**

dataedge primarily focuses on the following segments in Bangladesh. However, owing to the changing nature of business the focus area may often shift or change.

1. Banking and Non-Banking Financial Institutions (FIs)
2. Telecoms
3. Local Conglomerate
4. Multinational Companies
5. Govt. ICT Sector
6. Pharmaceuticals
7. Hospitality Industry
8. Education Sector

## 1.4 Clients:



15 Alliances:



# **Chapter 2**

## **Literature Review**

### **Public Key Infrastructure**

## **2.1 Introduction:**

The electronic information systems today are as complex as the business relationships they need to serve. The words 'Information Security' are now familiar at the highest levels of corporate structures. The security consultant is taking his place as an advisor along with the legal and accounting experts that are essential to conducting business today. Information security, when approached from a corporate perspective, is an enabler of traditional business goals in an electronic environment. Improved revenue through access to new markets, reduced costs through the efficiencies of extranet and internet delivery of information, compliance with government and industry regulations regarding the privacy of personal information, and reduced risk of liability are only a few examples of the business objectives that can be enabled by having a cogent security policy and security delivery infrastructure. The question today is not whether to build a security infrastructure but rather which one to build. [ROI]

One of the most crucial questions in any business transaction is the identity of the entity with which the transaction is being conducted. Historically, personal relationships, face to face contract signings, notaries, and third party counsel are used to help establish trust in this most important aspect of conducting our business. As the reliance on paper shifts to electronic transactions and documents, so must the reliance on traditional trust factors shift to electronic security measures to authenticate our electronic business partners, customers, and suppliers before engaging in the exchange of information, goods, and services. Similarly, the need for confidentiality and confidence in the integrity of exchanged information is critical. Extending this list of security services, there may be further need to establish the non-repudiation of agreements, and to digitally notarize and securely timestamp transactions. [BUS]

## **2.2 The Cryptographic Building Block:**

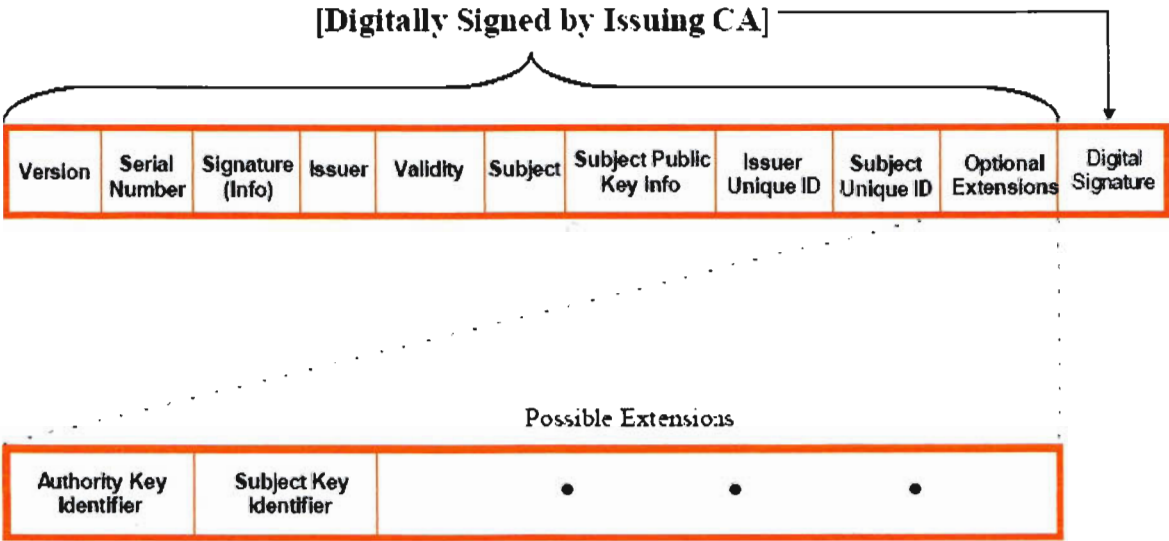
Cryptography is fundamentally based on the use of keys that are used to encrypt and decrypt data<sup>1</sup>. There are two types of cryptography: 1) secret key or symmetric and 2) public key or asymmetric. Secret key cryptography is characterized by the fact that the same key used to encrypt the data is used to decrypt the data. Clearly, this key must be kept secret among the communicating parties; otherwise the communication can be intercepted and decrypted by others.

Public key cryptography is based on the use of key pairs. When using a key pair, only one of the keys, referred to as the private key, must be kept secret and (usually) under the control of the owner. The other key, referred to as the public key, can be disseminated freely for use by any person who wishes to participate in security services with the person holding the private key. This is possible because the keys in the pair are mathematically related but it remains computationally infeasible to derive the private key from knowledge of the public key. In theory, any individual can send the holder of a private key a message encrypted using the corresponding public key and ONLY the holder of the private key can read the secure message (i.e. can decrypt it). Similarly, the holder of the private key can establish the integrity and origin of the data he sends to another party by digitally signing the data using his private key. Anyone who receives that data can use the associated public key to validate that it came from the holder of the private key and verify the integrity of the data has been maintained.

This entire concept was revolutionary. One of its initial uses was to facilitate the delivery of keys to be used in symmetric cryptographic functions. Prior to this, the delivery of secret keys was arduous to set

up and could not even be accomplished if the persons involved did not know each other. It also reduces the number of keys that must be used within a system. To keep communications secure using symmetric cryptography, each person in the system must have a different key for each person with whom he communicates; in the system of  $n$  users, there are on the order of  $n^2$  keys. Under a public key scheme, there only needs to be one key pair per person in the system, or  $n$  key pairs in the system. This is a valuable advantage.

A Public Key Infrastructure is designed to provide this trust. Using a data element called a digital certificate or public key certificate, which binds a public key to identifying information about its owner, the infrastructure is designed to create the binding, and manage it for the benefit of all within the community of use. Figure 2-1 illustrates the Version 3 public key certificate as defined in X.509.



**Figure 2-1: Version 3 Public Key Certificate.**  
**Data Fields and Extensions are defined in the X.509 standard.**

Although PKI derives its name from Public Key Cryptography, some of the services it provides have their technical roots in techniques that are outside this branch of cryptography. PKI embodies the best of these well-understood techniques. PKI represents the integration of public key cryptography used for digital signatures and key management, and symmetric key cryptography used for encryption.

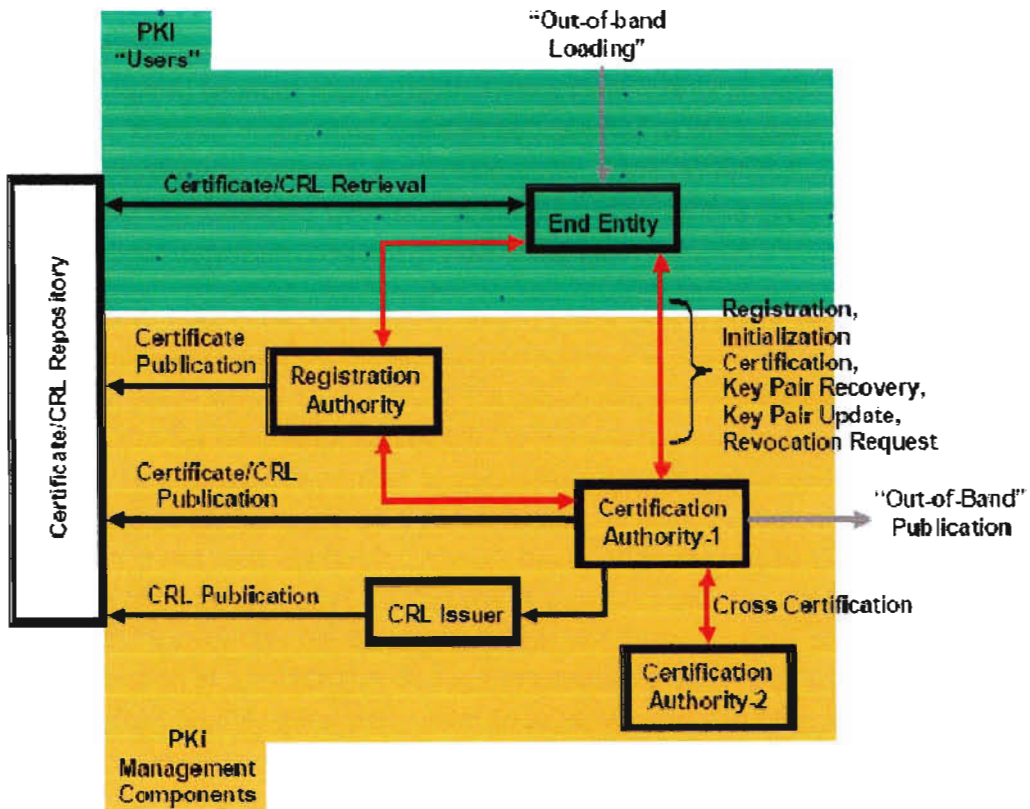


**2.3 Definition:** First and foremost, PKI is an authentication technology. Using a combination of secret key and public key cryptography, PKI enables a number of other security services including data confidentiality, data integrity, and key management. The very foundation or framework for PKI is defined in the ITU-T X.509 Recommendation [X.509]. The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509 that is suitable for deploying a certificate-based architecture on the Internet. The purpose of this section is to describe this model, and to summarize the key management functions that are realized through this infrastructure.

### 2.4 The PKI Architecture Model:

The basic PKIX architecture model has remained largely unchanged since it was first published in the original Internet Certificate and Certificate Revocation List (CRL) Profile [RFC2459]. The latest model is reflected in the most recent version of the Internet Certificate and CRL Profile [RFC3280]. Figure 2-2 illustrates our interpretation of this model, and Table 3-1 identifies the name and purpose of each component represented. These components are described in greater detail in the subsections that follow.

Fig: 2-2 PKI Architecture Model



COMPONENT	PRIMARY ROLE
<ul style="list-style-type: none"> <li>End Entity</li> </ul>	End Entity is a generic term used to denote end-users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI-related services.
<ul style="list-style-type: none"> <li>Certification Authority (CA)</li> </ul>	The CA is the issuer of certificates and (usually) CRLs. It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.
<ul style="list-style-type: none"> <li>Registration Authority (RA)</li> </ul>	The RA is an optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity registration process, but can assist in a number of other areas as well.
<ul style="list-style-type: none"> <li>Repository</li> </ul>	A repository is a generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.
<ul style="list-style-type: none"> <li>CRL Issuer</li> </ul>	The CRL Issuer is an optional component that a CA can delegate to publish CRLs.

Table: 2-1 PKI Component

**END ENTITIES:** End Entities are sometimes thought of as end-users. Although this is often the case, the term End Entity is meant to be much more generic. An End Entity can be an end-user, a device such as a router or a server, a process, or anything that can be identified in the subject name of a public key certificate. End Entities can also be thought of as consumers of the PKI-related services. There are even cases when a provider of PKI-related services is considered to be an End Entity. For example, a RA is considered to be an End Entity from the point of view of the CA.

**CERTIFYING AUTHORITY (CA):** Public keys are distributed in the form of public key certificates. The CA is the very foundation of the PKI since it is the only component that can issue public key certificates. Public key certificates are digitally signed by the issuing CA (which effectively binds the subject name to the public key). CAs are also responsible for issuing CRLs unless this has been delegated to a separate CRL Issuer. CAs may also be involved in a number of administrative tasks such as end-user registration, but these are often delegated to the Registration Authority (RA). In implementation practice, CAs can also serve as the key backup and recovery facility although this function can also be delegated to a separate component. CAs are often thought of as the “source of trust” in a PKI. The PKI Forum Note, CA Trust, endorses standardized frameworks for the establishment and auditing of the policies and procedures required for the operation of a PKI [CAT]. Typically, End Entities are configured with one or more “trust anchors” which are then used as the starting point to validate a given certification path.<sup>3</sup> See the PKI Forum white paper on Certification Path Construction for additional information. [CPC]

**Registration Authority (RA):** A Registration Authority (RA) is an optional component that can be used to “offload” many of the administrative functions that a CA would have to assume in the absence of a RA. As stated earlier, the RA is normally associated with the End Entity registration process. This would include the verification of the identity of the End Entity attempting to register with the PKI. However, the RA can perform a number of other functions, including:

- Validating the attributes of the subject who is requesting the certificate
- Verifying that the subject has possession of the private key being registered (known as “Proof of possession”)
- Generation of shared secrets to support the initialization and certification process
- Public/private key pair-generation
- Conducting interactions with the CA (or several CAs) as an intermediary of the End Entity, including key compromise notifications and key recovery requests
- Parameter validation of public keys presented for registration

- ANSI X9 standards provide guidance with algorithm-specific details [ANS]

Note that although the RA can offload many functions from the CA, the RA can never be the issuer of a public key certificate. Judicious deployment of RAs can provide two primary advantages. First, RAs can help to reduce overall costs. This is especially true in large, geographically dispersed organizations that require their users to be physically present before certain PKI related activities are permitted. A typical example would be end-user registration, but other PKI-related functions such as end-user initiated requests for certificate revocation or key pair recovery might also apply. There may also be other practical considerations, such as when an organization elects to outsource the CA service but retain control of the registration process. Second, offloading the administrative functions from the CA allows an organization to operate their CA off-line, which reduces the window of opportunity to mount remote attacks against that CA.

### **Repositories:**

The term repository is often associated with a directory, but this is not necessarily the case. In the context of a PKI, a repository is a generic term used to denote any method for storing and retrieving PKI-related information such as public key certificates and CRLs. A repository can be an X.500-based directory with client access via the Lightweight Directory Access Protocol (LDAP), or it may be something much simpler such as retrieval of a flat file on a remote server via the File Transfer Protocol (FTP) or the Hyper Text Transfer Protocol (HTTP). The IETF PKIX working group has addressed several “operational protocols” to facilitate the distribution of public key certificates and CRLs, including LDAP, HTTP, and FTP. It is also possible to offload certain functions from the client system to a trusted third party. For example, the Online Certificate Status Protocol [RFC2560] can be used to “ask” a trusted third party about the revocation status of one or more certificates. Arguably, this could also be viewed as a repository since the revocation status is derived and returned to the client system in response to a request for PKI related information. The PKIX working group is also working on several protocols to offload the certification path construction and validation process from the client system. In any case,

the key here is that End Entities must have some mechanism to retrieve the necessary certificates and CRLs, or they must be able to request that this is done on their behalf.

**Certificate Revocation List Issuer:** The CRL Issuer is just as its name implies – it is the issuer of a CRL. Typically, the CA that issues a given set of certificates is also responsible for issuing revocation information associated with those certificates. However, it is possible for a CA to delegate that function to another entity. CRLs that are issued by another entity are referred to as indirect CRLs. Although the fact that this appears to be a new component in the PKI architecture model, the notion of indirect CRLs has been standardized in the X.509 Recommendation for some time. This is simply now more explicit in the PKIX architecture model.

## 2.5 PKI Management Function:

PKIX identifies a number of management functions that “potentially need to be supported by management protocols” [RFC3280]. Figure 2-2 illustrates the interaction between the various PKI components and it summarizes the types of management functions that might occur between these components. These particular management functions are discussed in more detail in the subsections that follow. Note that one or more of these functions may also occur off-line. Also note that additional functions may be supported. The PKI management protocols that might be used to realize these functions.

**Registration :** End Entities must “enroll” into the PKI before they can take advantage of the PKI enabled services. Registration is the first step in the End Entity enrollment process.

This is usually characterized as the process whereby an End Entity first makes itself known to a CA [RFC3280]. This step is usually associated with the initial verification of the End Entity’s identity. The rigor or “level of assurance” associated with the registration process will tend to vary based on the target environment, intended use of the certificate, and the associated policies. As noted above, the process of registration could be accomplished directly with the CA or through an intermediate RA. This process may also be accomplished on-line or off-line (or a combination of the two). Once the identity of the End Entity is verified in accordance with the applicable policies, the End Entity is typically issued one or more shared secret(s) and other identifying information that will then be used for subsequent authentication as the enrollment process continues. The distribution of the shared secret(s) is typically performed out-of-band and may in fact be based on pre-existing shared secret(s).

**Initialization:** Initial registration is followed by initialization. At a minimum, this involves initializing the associated trust anchor with the End Entity. Additional information such as applicable certificate policies may also be supplied. In addition, this step is usually associated with initializing the End Entity with its associated key pair(s). Key pair generation involves the creation of the public/private key pair associated with an End Entity. Key pair generation can occur in advance of the End Entity enrollment process or it can take place in response to it. Key pairs can be generated by the End Entity client system, RA, CA or some other component such as a hardware security module. The location of the key pair generation is dictated by operational constraints and applicable policies. Often, the intended use of the keying

material plays a critical role in determining where the key pairs should be generated. It is possible that portions of this step may occur at different times. On the Internet, for example, browsers are initialized with the public keys of numerous root CAs that might be used as trust anchors. However, the end-user portion of initialization would not occur until an explicit certificate request is made. Further, end-users may import additional trust anchors over time.

**Certification:** Certification is the natural conclusion to the End Entity enrollment process. As its name implies, this step involves the issuance of the End Entity public key certificate by the CA. If the key pair is generated external to the CA, the public key component must be conveyed to the CA in a secure manner. Once generated, the certificate is returned to the End Entity and/or published to a certificate repository. Although we have presented registration, initialization and certification as separate management functions, note that two or more of these can be combined into a single protocol operation [RFC3280]. For example, this is the case with the PKIX Certificate Management Protocols [RFC2510]

**Key Pair Recovery:** Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. When a key pair is used for encryption/decryption, it is important to provide a mechanism to recover the necessary decryption keys when “normal” access to the keying material is no longer possible, otherwise it will not be possible to recover the encrypted data.<sup>4</sup> Normal access to the decryption key can result from forgotten passwords/PINs, corrupted disk drives, damage to hardware tokens, et cetera. Key pair recovery allows End Entities to restore their encryption/decryption key pair from an authorized key backup facility (typically, the CA that issued the End Entity’s certificate). It is also possible that an End Entity’s association with an organization can change (for example, in the case of employee resignation, dismissal, or personal injury), and the organization has a legitimate need to recover data that has been encrypted by that End Entity. It is also possible that access to the keying material may be required in association with legitimate law enforcement requirements. Key pair recovery can be used to support both of these requirements as well.

**Key Pair Update:** Certificates are issued with fixed lifetimes (referred to as the “validity period” of the certificate). While these fixed lifetimes can be rather generous (say two to five years or so), the certificate will eventually expire. Key pair update may also be required as a result of certificate revocation, Key pair update involves generation of a new key pair, and the issuance of a new public key certificate<sup>5</sup>. Key pair update can occur in advance of a given key pair’s expiration. This will help to ensure that the End Entity is always in possession of a legitimate key pair. Although the PKIX working group recommends against the use of this feature on the Internet [RFC3280, Section 4.2.1.4], it is possible to establish different validity periods for the private and public keys that are used to digitally sign and verify. This would force a key pair update before the associated public key actually expires. It also provides a window of time where the non-expired public key certificate can be used to verify digital signatures that were created with the now expired private key. This will help to minimize irrelevant warning messages that would otherwise be displayed to the End Entity.

## Revocation Request

As mentioned above, public key certificates are issued with fairly generous lifetimes. However, the circumstances that existed when the certificate was issued can change before the certificate would naturally expire. Reasons for revocation include private key compromise, change in affiliation, name change, et cetera (specific reason codes are defined in X.509). Therefore, it is sometimes necessary to revoke a certificate before its expiration date. The Revocation Request allows an End Entity (or RA) to request revocation of a given certificate. Of course, out-of-band mechanisms may also be supported/required, and the End Entity may not be involved with the revocation process at all. Certificate revocation information must be made available by the CA that issued that certificate or by the CRL Issuer to which the CA delegates this function. X.509 defines a method for publishing this information via Certificate Revocation Lists (CRLs). The frequency of publication and the type of CRLs used are a function of local policy. The publication and retrieval of CRLs is represented in Figure 2-2. The PKIX working group has also introduced several protocols that are designed to provide certificate status information on-line.

Note that End Entities, or trusted third parties operating on their behalf, must check the revocation status of all certificates in a given certification path. This includes revocation information about End Entity certificates as well as intermediate CAs.

## Cross-Certification

As illustrated in Figure 2-2, cross-certification occurs between CAs. A cross-certificate is a public key certificate that is issued by one CA to another CA. In other words, a cross-certificate is a public key certificate that contains the public key of a CA that has been digitally signed by another CA. Many interpret cross-certification to mean "inter-domain" cross-certification. However, "intra-domain" cross-certification is also possible. This can be illustrated by using the Government of Canada (GOC) PKI as an example. Major departments within the GOC PKI cross-certify with the Canadian Central Facility, which acts as a bridge CA between these departments. As these departments all "belong" to the GOC PKI, this is "intra-domain" cross-certification. The Canadian Central Facility is also responsible for cross-certification with external PKI domains such as the US Federal Bridge CA. This is "inter-domain" cross-certification. It should also be noted that cross-certification can be bi-directional or unidirectional. Bi-directional cross-certification typically occurs between peer CAs as described in the previous paragraph. Unidirectional cross-certification typically occurs in a hierarchical trust model where superior CAs issue cross-certificates to subordinate CAs, but the reverse is not true.

## 2.6 PKI Management Protocol:

Management protocols can be used to support on-line protocol exchanges between various PKI components. The IETF PKIX working group has developed two fairly comprehensive management protocols that can be used to support this component-level interaction. The first is the Certificate Management Protocols (CMP) based on RFC2510 and the associated Certificate Request Message

Format (CRMF) based on RFC2511. The second management protocol is the Certificate Management Messages over the CMS (CMC) based on RFC2797. CMP is arguably the most comprehensive PKIX management protocol. All of the management functions discussed in Section 3.2 are explicitly identified as specific protocol exchanges (or as attributes within a specific protocol message). The basic certificate request format is defined in RFC2511. CMP is designed to be a flexible protocol able to accommodate a variety of technical, operational, and business models. CMP is evolving based on multi-vendor interoperability experience co-sponsored by the PKI Forum and ICSA. A second draft of the CMP is under development (see [http:// www.ietf.org/html.charters/pkix-charter.html](http://www.ietf.org/html.charters/pkix-charter.html) for the latest Internet Draft) and is expected to achieve RFC status later this year. CMC is also a fairly comprehensive PKIX management protocol, although arguably some of the functions described in Section 3.2 above are not as explicit as they are in CMP. CMC is built upon the earlier work done with other standards such as CMS [RFC2630] and PKCS #10 [RFC2986]. CMC attempts to leverage existing implementations based on CMS and PKCS #10.

## 2.7 PKI Certificate Discovery and Validation Protocols:

As mentioned above, the PKI working group is developing protocols that address the need to offload portions (potentially all) of the certificate discovery and/or validation process from the client system. The forerunner to these protocols is the Online Certificate Status Protocol (OCSP) as defined in RFC2560. OCSP is a very simple request/reply protocol that allows clients to ask an “OCSP responder” about the revocation status of one or more certificates. The OCSP responder returns digitally signed responses regarding the status of the certificates identified in the request. OCSP is designed to return realtime responses to client queries, and can provide an efficient method for returning certificate status on demand. However, OCSP offers limited functionality, and work on more comprehensive protocols has been underway for some time.

## 2.8 PKI in Bangladesh:

In Bangladesh, **Office of the Controller of Certifying Authority (CCA)** of **ICT Division** has defined some rules PKI model and provides a platform for certificate using for CAs. It is published in 15<sup>th</sup> April 2010 under the ICT Act 2006. They are following:

### 1. Short title and commencement –

- (1) These Rules will be called Information Technology (Certifying Authorities) Rules, 2010.
- (2) They shall come into force immediately.

### 2. Definitions –

In these Rules, unless the context otherwise requires,–

- (a) “Act” means the Information, Communication and Technology Act, 2006 (Act no. 39 of 2006);
- (b) “applicant” means the person who applied for acting as Certifying Authority;

(c) "auditor" means internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority;

(d) "Electronic Signature" means electronic signature as defined in section 2(1) of the Act and for the purpose of these Rules, digital signature will also be considered as electronic signature;

(e) "information asset" means all information resources utilized in the course of any organization's business and includes all information, application of exhibited or developed or purchased software, and technology (hardware, system software and networks);

(f) "person" means an individual, or a company or association and shall include authorities of the Government of Bangladesh having knowledge of issuance of Electronic Signature Certificates;

(g) "Public key" means a specific value determined by the nominated authority, which is used as "encryption key" combining with "private key" to effectively encrypt information and electronic signature;

(h) "Private key" means secret information or electronic signature giver's known encryption or decryption key, which is used to encrypt information into electronic signature or public key used with private key;

(i) "Schedule" means schedule annexed to these Rules;

(j) "subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

(k) "trusted or dependable person" means any person whose: –

(i) principal responsibility is to ensure day-to-day activities, provide security and direct any other activities of a Certifying Authority under the Act and any Rules or Regulations formulated under the Act; or ii. duty involves verification of identity of a person who requested Electronic Signature Certificate from a Certifying Authority, and also issuance, renewal, cancellation or suspension of that Electronic Signature Certificate, creation of private key or administration of the computing facilities of the Certifying Authority.

### **3. Method in which information can be authenticated by means of Electronic Signature –**

(1) An Electronic Signature shall be created and verified by such cryptography which transform electronic records into seemingly unintelligible form and back;

(2) A method, known as "Public Key Cryptography", shall be used for creating and verifying electronic signature, which employs an algorithm using two different but mathematically related "keys" – one for creating an Electronic Signature or transforming data into a seemingly unintelligible form, and another key for verifying an Electronic Signature or returning the electronic record to original form,

(3) The process termed as hash function shall be used in both creating and verifying a Digital Signature.

### **4. Creation of Electronic Signature.-**



To sign an electronic record or any other item of information, the signer shall apply the following method:

(a) use hash function in the signer's own software, for all usage needs, which in the case of electronic record shall compute a hash result of standard length which is unique to the electronic record;

(b) use private key to transform the hash result of the signer's software into an Electronic Signature;

(c) the Electronic Signature created by following the method contained in sub-Rule

(a) and (b), shall be unique or uniform to both electronic record and private key used to create it; and

(d) The Electronic Signature shall be attached to the electronic record and appropriately protected and thereafter transmitted with the electronic record.

#### **5. Verification of Electronic Signature-**

(1) The verification of an Electronic Signature shall be accomplished by the following method:-

(a) By computing a new hash result of the original electronic record by means of the hash function used to create an Electronic Signature and by using the public key;

(b) The encrypted digital digest shall be decrypted by using public key;

(c) By comparing the new hash result with the decrypted hash;

(2) In instances, when:-

(a) Similar private and public key is used to create an Electronic Signature,

(b) Newly computed hash result is similar with the original result, and

(c) Which transforms into Electronic Signature during the signing process. the verifier shall verify the Electronic Signature.

(3) The verification software will confirm the Electronic Signature as verified if:- (a) in order to digitally sign the electronic record, the private key of the signer is used and the public key of the signer is used to verify the signature, in that instance the electronic record shall be considered to have been digitally signed;

(b) an electronic record will be deemed to be unaltered, if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

## **6. Authentication of Public Key –**

A public key shall be authenticated in the following manner-

(a) if the public key was generated by using secret cryptography; and (b) the Controller authenticates the said public key.

## **7. Standards –**

The Information Technology architecture followed by Certifying Authorities shall be of appropriate and acceptable standards and the activities of such authority shall be in accordance with the standards as set out in Schedule-2 or as prescribed by the Controller from time to time.

## **8. Standard of issuance of Electronic Signature Certificate-**

All Electronic Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 (or above) standard or similar standards and shall contain the following data, namely:-

(a) Unique Serial Number, which is assigned by Certifying Authority in the Electronic Signature Certificate in order to distinguish it from other certificate;

(b) Information for authentication of the algorithm process used to compute signature, which is used by the Certifying Authority for authentication of the process of computing signature for signing an Electronic Signature Certificate;

(c) Name of the issuer, which shall include the name of the Certifying Authority;

(d) Validity period of the Electronic Signature Certificate;

(e) Name of the subscriber, which can authenticate the public key in the Certificate; and

(f) Public Key information of the subscriber.

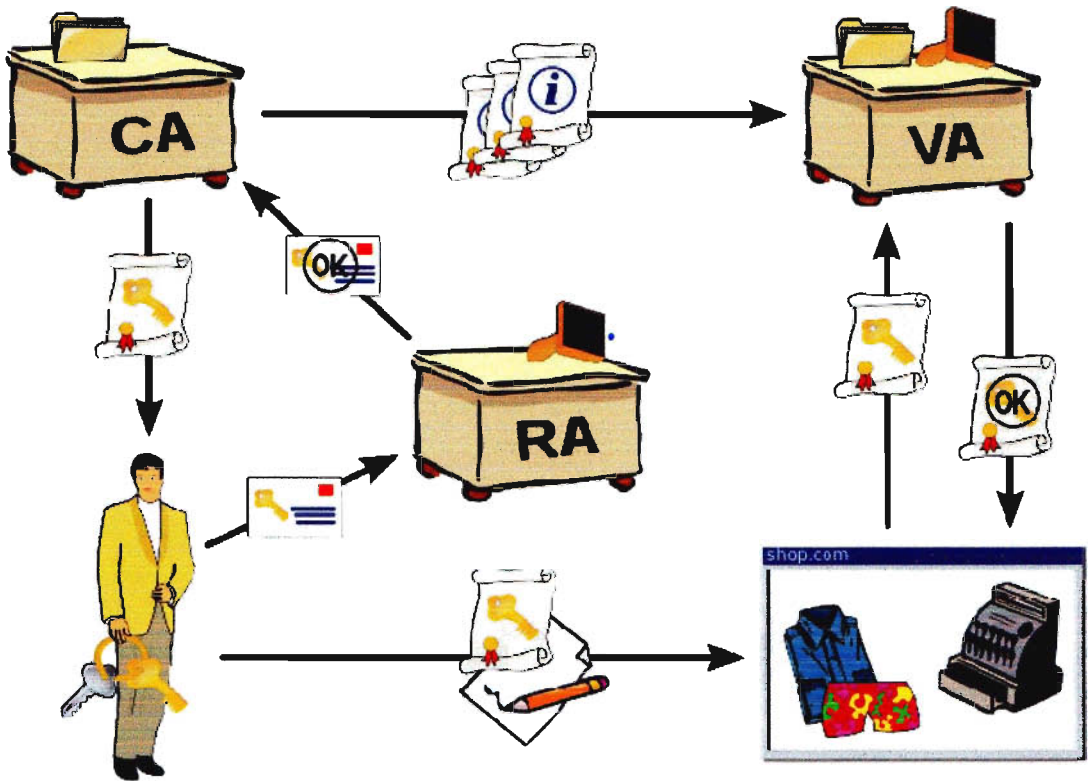
## **9. Licensing of Certifying Authorities.-**

(1) Any person interested to obtain license to issue Electronic Signature Certificate shall apply to the Controller at such time and manner as determined by the Controller, and shall, along with the application, furnish such information and pay such security and fees as may be prescribed time to time.

(2) A licence may be issued in favour of a citizen, association, company, partnership firm or any other entity, if -

(a) in the case of association or company, at least sixty percent of the shares of the association or company is owned or controlled by Bangladeshi citizens; and

(b) in the case of partnership firm or any other entity, the capital or proprietary right of the firm or the entity, is owned or controlled by Bangladeshi citizens.



**Fig 2-3: A simple use of PKI using Digital signature Certificate**

# Chapter 3

## Digital Signature Certificate

### 3.1 Definition:

A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

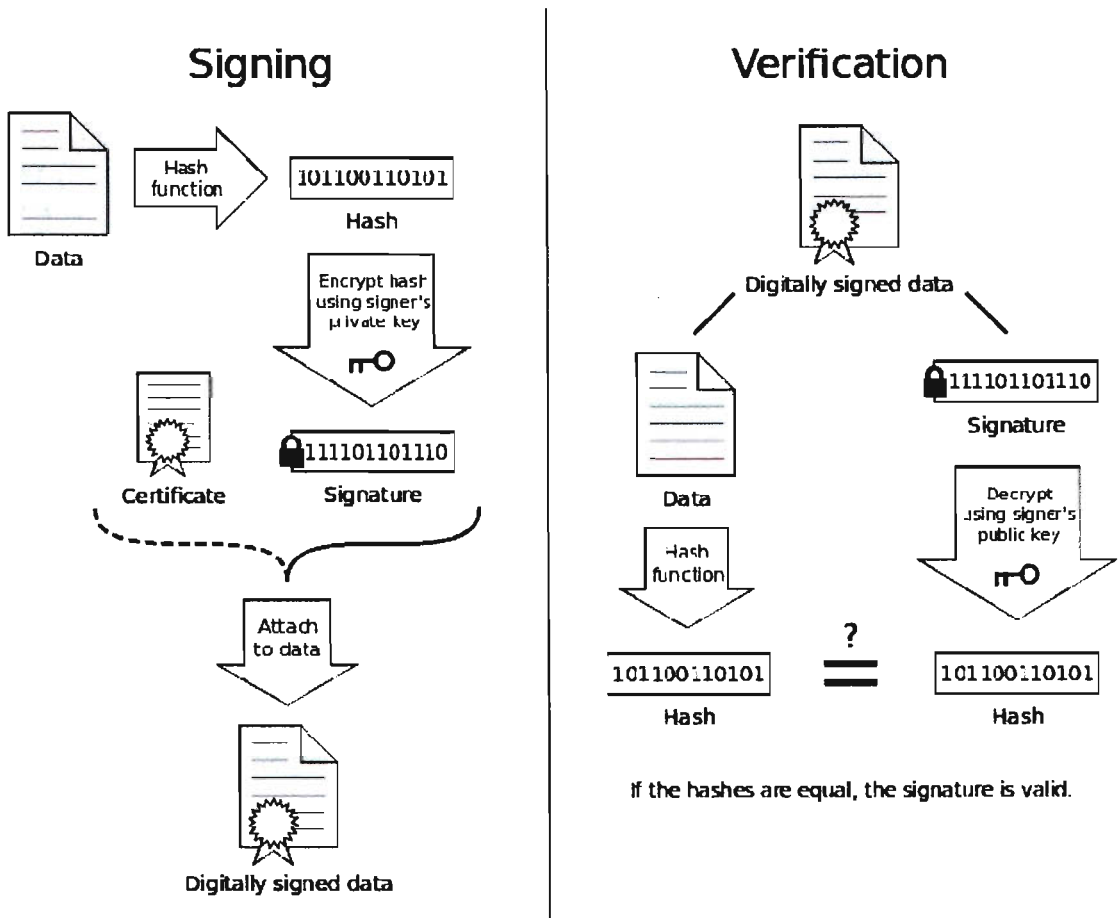


Fig 3-1 : Digital signature Certificate

### 3.2 Applications of digital signatures:

**1) Authentication:** Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the

message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

**II) Integrity:** In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

**III) Non-repudiation:** Non-repudiation, or more specifically *non-repudiation of origin*, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentication, non-repudiation etc. properties rely on the secret key *not having been revoked* prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.

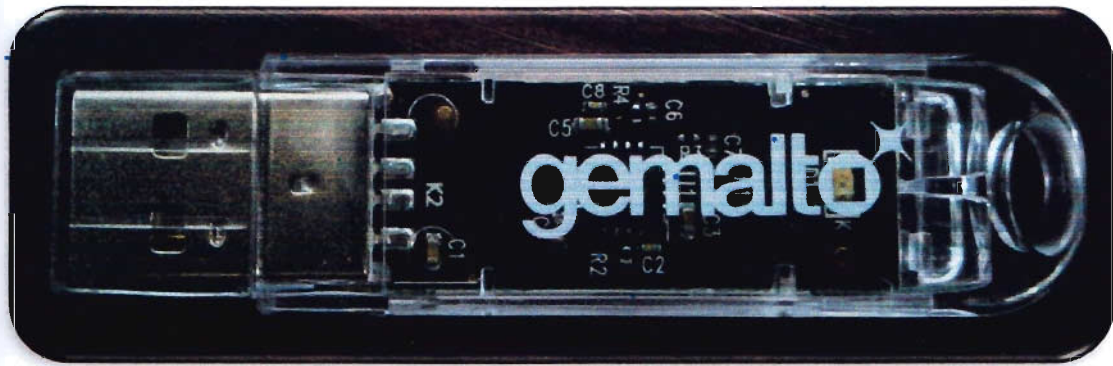
### 3.3 Putting the private key on a smart card:

All public key / private key cryptosystems depend entirely on keeping the private key secret. A private key can be stored on a user's computer, and protected by a local password, but this has two disadvantages:

- the user can only sign documents on that particular computer
- the security of the private key depends entirely on the security of the computer

A more secure alternative is to store the private key on a smart card. Many smart cards are designed to be tamper-resistant (although some designs have been broken, notably by Ross Anderson and his students). In a typical digital signature implementation, the hash calculated from the document is sent to the smart card, whose CPU signs the hash using the stored private key of the user, and then returns the signed hash. Typically, a user must activate his smart card by entering a personal identification number or PIN code (thus providing two-factor authentication). It can be arranged that the private key never leaves the smart card, although this is not always implemented. If the smart card is stolen, the thief will still need the PIN code to generate a digital signature. This reduces the security of the scheme to that of the PIN system, although it still requires an attacker to possess the card. A mitigating factor is

that private keys, if generated and stored on smart cards, are usually regarded as difficult to copy, and are assumed to exist in exactly one copy. Thus, the loss of the smart card may be detected by the owner and the corresponding certificate can be immediately revoked. Private keys that are protected by software only may be easier to copy, and such compromises are far more difficult to detect.



**Fig: A Smart Card for storing digital signature certificate**

### **3.4 Digital signatures vs. ink on paper signatures:**

An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult.

Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink and numbering all pages of the contract.

# **Chapter 4**

## **Certificate Practice Statement of dataedgeid**

**VERSION 1.0.2**  
**(dataedge/DOC/CPS/1.0.2)**  
**OID: 2.16.50.1.6.1**

**Date of Publication: November 2013**





## **NOTICE**

Save as otherwise provided as per the laws of Bangladesh, the services provided by dataedge shall, at any time, be in accordance with the applicable laws in Bangladesh and shall be subject to the jurisdiction of various courts, tribunals and authorities in Bangladesh, including but not limited to the law of information and communication technology law 2006 (IT Act), its rules and regulations and any amendment thereto.

Any person who uses the digital signature certificate in an improper manner or violate the provisions detailed under this dataedge Certification Practice statement shall render himself/herself liable for civil/criminal action and be proceeded against as per the provisions of applicable civil/criminal laws and IT act or any other act/acts that are relevant and in force from time to time. Attention is also drawn to the IT Act Chapter 6 wherein the duties of subscribers are specified.

## **EXECUTIVE SUMMARY OF data edge limited**

### **data edge limited - your technology partner**

data edge limited (dataedge), is a leading technology solution company in Bangladesh, providing technology strategy, implementation, business transformation and operational solutions for clients managing the business and technology complexities of the digital economy.

dataedge brings together the world's best technologies to address critical client business imperatives. It helps clients eliminate boundaries, collaborate in new ways, establish their customers' trust and continuously seek improvement. By partnering with dataedge, organizations gain the power of tried and tested products, strong domain knowledge, a pool of certified technology specialists and best of breed alliances. We bring the right solution tuned to the need, timely, industry specific that helps meet your business challenges while increasing operational efficiency.

We have leveraged our expertise and experience in meeting the IT needs of enterprises that enables us to offer comprehensive IT solutions that encompass best-of-breed products, best-practice IT services and best-in-class enterprise solutions. We help architect, implement and manage the entire IT lifecycle of our customers through a complete portfolio of IT Services. Our services are backed by over decade long experience handling complex integration projects locally and abroad. Multi-platform expertise, extensive reach and tested delivery mechanisms help us deliver reliable, high-quality, cost-effective IT services.

Our position in the IT business is built on a strong foundation of quality processes, Knowledge Management, Innovation & People processes. Our group also follows methodology to improve internal process performance in diverse areas to bring about quicker deliveries, higher reliability, and simplified processes for customers and employees, call response and personal productivity.

dataedge now consist of about 120 professionals, operating from two locations, a fully operational, process-oriented development center with all modern amenities and committed to quality product and services.

This Certification Practice Statement (CPS) describes the practices followed with regard to the management of the lifecycle of the certificates issued by dataedge CA

For more information visit,  
[www.dataedgeid.com](http://www.dataedgeid.com) or contact, [info@dataedgeid.com](mailto:info@dataedgeid.com)

## dataedge CERTIFICATION AUTHORITY CERTIFICATE PRACTICE STATEMENT

This Certification Practice Statement is based on the RFC-3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

### **Components of dataedge CA Public Hierarchy**

dataedge CA's Bangladesh Public Hierarchy:

The dataedge CA's Bangladesh Public Hierarchy refers to that CA hierarchy from dataedge CA that is certified with the Root Certifying Authority of Bangladesh (RCAB). This root is envisaged to serve as the basis for inter operability amongst various licensed CA's in Bangladesh for consumer applications.

Under this hierarchy, the following Classes of Certificates are available:

- Class 1
- Class 2
- Class 3

The dataedge Public Hierarchy components and roots are explained in detail in the rest of the CPS. Each component hierarchy is governed by the dataedge CPS and its own unique policies and requirements – hence each of these is outlined separately in each section /sub-section of this CPS. The individual Subscribers and Relying Parties are required to take cognizance of the sections / subsections relevant to them

Under each component hierarchy, dataedge CA also offers the following arrangements:

Sub CA: Under this scheme, a “technical CA” with its own set of keys is specially created for the customer (usually an organization, community or a Closed User Group (CUG)). This technical CA is signed by dataedge CA, thus making it a “sub CA” under dataedge CA hierarchy.

RA (Registration Authority)<sup>1</sup>: Under this scheme, a customer can choose to be an RA under the appropriate dataedge sub CA. Once again, the choice of hierarchy and class is available to the customer.

Refer CPS 1.3 for further details on the above.

### **IMPORTANT NOTE:**

(1). This CPS (as amended from time to time) is intended to be an all-encompassing CPS that covers all the hierarchy components, classes, certificate types etc. However, not all services and products may be commercially available at all points in time. dataedge CA reserves the sole right to decide when and to whom to offer which type of service.

(2). dataedge reserves the right and discretion not to accept the request for issue of any Certificate or the class of the Certificates requested for. The verification and validation processes for different **hierarchy and classes** will be at the discretion of dataedge.

---

<sup>1</sup> See Definitions

For example such processes for **dataedge CA Class 3 certificate under the Bangladesh Root CA Public Hierarchy** may be more extensive and detailed than **dataedge CA Class 2 certificate under the same hierarchy**.

**(3) The term certificate and certification are used interchangeably throughout this document.**

### **The Certificate Policy**

The Certificate Policy is the principal statement of policy governing a PKI hierarchy. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing Digital Certificates within the PKI hierarchy and providing associated trust services.

## Table of Contents

Table of Contents .....	6
1. Introduction .....	13
1.1 Overview .....	13
1.2 Document name and identification .....	13
1.3 PKI participants .....	13
1.3.1 Certification Authorities .....	13
1.3.2 Subordinate CA .....	13
1.3.3 Registration Authorities .....	13
1.3.4 Subscribers .....	13
1.3.5 Relying parties .....	14
1.3.6 Other participants .....	14
1.4 PKI participants obligations .....	14
1.4.1 Certifying Authority and Registration Authority Obligations .....	14
1.4.2 Certifying Authority Obligations .....	15
1.4.3 Registration Authority Obligations .....	15
1.4.4 Subscriber Obligations .....	15
1.4.5 Relying Party Obligations .....	16
1.4.6 Repository Obligations .....	17
1.5 Certificate usage .....	17
1.5.1. Appropriate certificate uses .....	17
1.5.2 Prohibited certificate uses .....	17
1.6 Policy administration .....	17
1.6.1 Organization administering the document .....	17
1.6.2 Contact person .....	18
1.6.3 Person determining CPS suitability for the policy .....	18
1.6.4 CPS approval procedures .....	18
1.7 Definitions and acronyms .....	18
1.7.1 Definitions .....	18
1.7.2 List of acronyms and abbreviations used in this cps .....	19
2. Publication and repository responsibilities .....	20
2.1 Repositories .....	20
2.2 Publication of certification information .....	20
2.3 Time or frequency of publication .....	20
2.4 Access controls on repositories .....	20
3. Identification and authentication .....	20
3.1 Naming .....	20
3.1.1 Types of names .....	21
3.1.2 Need for names to be meaningful .....	21
3.1.3 Anonymity or pseudonymity of subscribers .....	22
3.1.4 Rules for interpreting various name forms .....	22
3.1.5 Uniqueness of names .....	22
3.1.6 Recognition, authentication, and role of trademarks .....	22

3.2 Initial identity validation.....	22
3.2.1 Method to prove possession of private key .....	22
3.2.2 Authentication of organization identity .....	22
3.2.3 Authentication of individual identity.....	22
3.2.3.1 Class 1 Certificates .....	23
3.2.3.2 Class 2 Certificates .....	23
3.2.3.3 Class 3 Certificates .....	23
3.2.3.4 SSL Certificates .....	23
3.2.4 Non-verified subscriber information .....	23
3.2.5 Validation of authority.....	23
3.2.6 Criteria for interoperation .....	23
3.3 Identification and authentication for re-key requests .....	23
3.3.1 Identification and authentication for routine re-key .....	24
3.3.2 Identification and authentication for re-key after revocation .....	24
3.4 Identification and authentication for revocation request.....	24
4. Certificate life-cycle operational requirements.....	24
4.1 Certificate Application .....	24
4.1.1 Who can submit a certificate application.....	25
4.1.2 Enrolment process and responsibilities.....	25
4.2 Certificate application processing .....	25
4.2.1 Performing identification and authentication functions.....	25
4.2.2 Approval or rejection of certificate applications.....	25
4.2.3 Time to process certificate applications.....	25
4.3 Certificate issuance.....	25
4.3.1 CA actions during certificate issuance .....	25
4.3.2 Notification to subscriber by the CA of issuance of certificate .....	25
4.4 Certificate acceptance .....	25
4.4.1 Conduct constituting certificate acceptance.....	26
4.4.2 Publication of the certificate by the CA.....	26
4.4.3 Notification of certificate issuance by the CA to other entities .....	26
4.5 Key pair and certificate usage .....	26
4.5.1 Subscriber private key and certificate usage.....	26
4.5.2 Relying party public key and certificate usage .....	26
4.6 Certificate renewal .....	26
4.7 Certificate re-key .....	26
4.8 Certificate modification .....	27
4.8.1 Circumstance for certificate modification .....	27
4.8.2 Who may request certificate modification.....	27
4.8.3 Processing certificate modification requests .....	27
4.8.4 Notification of new certificate issuance to subscriber .....	27
4.8.5 Conduct constituting acceptance of modified certificate .....	27
4.8.6 Publication of the modified certificate by the CA .....	27
4.8.7 Notification of certificate issuance by the CA to other entities .....	27
4.9 Certificate revocation and suspension .....	27
4.9.1 Circumstances for revocation.....	28

4.9.2 Who can request revocation .....	28
4.9.3 Procedure for revocation request .....	29
4.9.4 Revocation request grace period .....	29
4.9.5 Time within which CA must process the revocation request.....	29
4.9.6 Revocation checking requirement for relying parties .....	29
4.9.7 CRL issuance frequency .....	29
4.9.8 Maximum latency for CRLs .....	29
4.9.9 On-line revocation/status checking availability .....	29
4.9.10 On-line revocation checking requirements .....	30
4.9.11 Other forms of revocation advertisements available.....	30
4.9.12 Special requirements re key compromise .....	30
4.9.13 Circumstances for suspension .....	30
4.9.14 Who can request suspension .....	30
4.9.15 Procedure for suspension request .....	30
4.9.16 Limits on suspension period .....	30
4.9.17 Who can request for the Activation of Suspended Digital Certificate .....	31
4.10 Certificate status services .....	31
4.10.1 Operational characteristics.....	31
4.10.2 Service availability .....	31
4.10.3 Optional features.....	31
4.11 End of subscription .....	31
4.12 Key escrow and recovery.....	31
5. Facility, management, and operational controls.....	31
5.1 Physical controls .....	31
5.1.1 Site location and construction.....	31
5.1.2 Physical access.....	32
5.1.3 Power and air conditioning .....	33
5.1.4 Water exposures.....	33
5.1.5 Fire prevention and protection .....	33
5.1.6 Media storage.....	33
5.1.7 Waste disposal.....	33
5.1.8 Off-site backup .....	33
5.2 Procedural controls .....	34
5.2.1 Trusted roles.....	33
5.2.2 Number of persons required per task .....	34
5.2.3 Identification and authentication for each role .....	34
5.2.4 Roles requiring separation of duties .....	35
5.3 Personnel controls.....	34
5.3.1 Qualifications, experience, and clearance requirements.....	34
5.3.2 Background check procedures .....	35
5.3.3 Training requirements .....	35
5.3.4 Retraining frequency and requirements .....	35
5.3.5 Job rotation frequency and sequence.....	35
5.3.6 Sanctions for unauthorized actions.....	35
5.3.7 Independent contractor requirements .....	36

5.3.8 Documentation supplied to personnel.....	35
5.4 Audit logging procedures.....	35
5.4.1 Types of events recorded .....	35
5.4.2 Frequency of processing log .....	35
5.4.3 Retention period for audit log .....	36
5.4.4 Protection of audit log.....	36
5.4.5 Audit log backup procedures.....	36
5.4.6 Audit collection system (internal vs. external) .....	36
5.4.7 Notification to event-causing subject.....	36
5.4.8 Vulnerability assessments .....	36
5.5 Records archival.....	37
5.5.1 Types of records archived.....	37
5.5.2 Retention period for archive .....	37
5.5.3 Protection of archive .....	37
5.5.4 Archive backup procedures .....	37
5.5.5 Requirements for time-stamping of records.....	37
5.5.6 Archive collection system (internal or external) .....	37
5.5.7 Procedures to obtain and verify archive information .....	37
5.6 Key changeover .....	37
5.7 Compromise and disaster recovery.....	37
5.7.1 Key compromise .....	37
5.7.2 Disaster Recovery .....	38
5.7.3 Incident and compromise handling procedures.....	38
5.7.4 Computing resources, software, and/or data are corrupted .....	38
5.7.5 Entity private key compromise procedures .....	38
5.7.6 Business continuity capabilities after a disaster.....	38
5.8 CA or RA termination.....	38
6. Technical security controls .....	39
6.1 Key pair generation and installation.....	39
6.1.1 Key pair generation .....	39
6.1.2 Private key delivery to subscriber .....	39
6.1.3 Public key delivery to certificate issuer .....	39
6.1.4 CA public key delivery to relying parties .....	40
6.1.5 Key sizes.....	40
6.1.6 Public key parameters generation and quality checking.....	40
6.1.7 Key usage purposes (as per X.509 v3 key usage field) .....	40
6.2 Private Key Protection and Cryptographic Module Engineering Controls .....	40
6.2.1 Cryptographic module standards and controls .....	40
6.2.2 Private key (m of n) multi-person control .....	40
6.2.3 Private key escrow.....	40
6.2.4 Private key backup.....	40
6.2.5 Private key archival.....	41
6.2.6 Private key transfer into or from a cryptographic module.....	41
6.2.7 Private key storage on cryptographic module.....	41
6.2.8 Method of activating private key .....	41



6.2.9 Method of deactivating private key .....	41
6.2.10 Method of destroying private key .....	41
6.2.11 Cryptographic Module Rating.....	41
6.3 Other aspects of key pair management .....	41
6.3.1 Public key archival .....	41
6.3.2 Certificate operational periods and key pair usage periods.....	41
6.4 Activation data.....	41
6.4.1 Activation data generation and installation .....	42
6.4.2 Activation data protection.....	42
6.4.3 Other aspects of activation data .....	42
6.5 Computer security controls .....	42
6.5.1 Specific computer security technical requirements .....	42
6.5.2 Computer security rating.....	42
6.6 Life cycle technical controls.....	42
6.6.1 System development controls.....	42
6.6.2 Security management controls.....	42
6.6.3 Life cycle security controls.....	42
6.7 Network security controls .....	42
6.8 Time-stamping.....	43
7. Certificate, CRL, and OCSP profiles.....	43
7.1 Certificate profile.....	43
7.1.1 Version number(s).....	43
7.1.2 Certificate extensions .....	43
7.1.3 Algorithm object identifiers.....	43
7.1.4 Name forms .....	43
7.1.5 Name constraints.....	43
7.1.6 Certificate policy object identifier .....	43
7.1.7 Usage of Policy Constraints extension.....	43
7.1.8 Policy qualifiers syntax and semantics .....	43
7.1.9 Processing semantics for the critical Certificate Policies extension.....	44
7.2 CRL profile.....	44
7.2.1 Version number(s) .....	44
7.2.2 CRL and CRL entry extensions.....	44
7.3 OCSP profile .....	44
7.3.1 Version number(s) .....	44
7.3.2 OCSP extensions .....	44
8. Compliance audit and other assessments .....	44
8.1 Frequency or circumstances of assessment.....	44
8.2 Identity/qualifications of assessor.....	44
8.3 Assessor's relationship to assessed entity.....	44
8.4 Topics covered by assessment .....	44
8.5 Actions taken as a result of deficiency .....	45
8.6 Communication of results .....	45
9. Other business and legal matters.....	45
9.1 Fees.....	45

9.1.1 Certificate issuance or renewal fees.....	45
9.1.2 Certificate access fees .....	45
9.1.3 Revocation or status information access fees .....	45
9.1.4 Fees for other services.....	45
9.1.5 Refund policy .....	45
9.2 Financial responsibility .....	45
9.2.1 Indemnification by Subscribers and Relying Parties.....	45
9.2.1.1 Indemnification by Subscribers .....	45
9.2.1.2 Indemnification by Relying Parties .....	46
9.2.2 Fiduciary Relationships .....	46
9.2.3 Insurance coverage.....	46
9.2.4 Other assets.....	46
9.2.5 Insurance or warranty coverage for end-entities.....	46
9.3 Confidentiality of business information .....	46
9.3.1 Scope of confidential information.....	46
9.3.2 Information not within the scope of confidential information .....	46
9.3.3 Responsibility to protect confidential information .....	46
9.4 Privacy of personal information .....	46
9.4.1 Privacy plan.....	46
9.4.2 Information treated as private .....	47
9.4.3 Information not deemed private.....	47
9.4.4 Responsibility to protect private information .....	47
9.4.5 Notice and consent to use private information .....	47
9.4.6 Disclosure pursuant to judicial or administrative process .....	47
9.4.7 Other information disclosure circumstances .....	47
9.5 Intellectual property rights.....	47
9.6 Representations and warranties .....	47
9.6.1 CA representations and warranties.....	48
9.6.2 RA representations and warranties.....	48
9.6.3 Subscriber representations and warranties .....	48
9.6.4 Relying party representations and warranties.....	49
9.6.5 Representations and warranties of other participants .....	49
9.7 Disclaimers of warranties .....	49
9.8 Limitations of liability .....	49
9.9 Indemnities.....	50
9.10 Term and termination .....	50
9.10.1 Term.....	50
9.10.2 Termination .....	50
9.10.3 Effect of termination and survival .....	50
9.11 Individual notices and communications with participants.....	50
9.12 Amendments .....	50
9.12.1 Specification Change Procedures .....	50
9.12.2 Items that Can Change Without Notification .....	50
9.12.3 Items that Can Change with Notification .....	50
9.12.3.1 List of Items .....	51

9.12.4 Notification Mechanism .....	51
9.12.5 Comment Period.....	51
9.12.5.1 Mechanism to Handle Comments .....	51
9.12.6 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer .....	51
9.12.7 Procedure for amendment.....	51
9.12.8 Notification mechanism and period.....	51
9.12.9 Circumstances under which OID must be changed.....	51
9.13 Dispute resolution provisions.....	52
9.13.1 Disputes among dataedge CA and Customers .....	52
9.13.2 Disputes with End-User Subscribers or Relying Parties.....	52
9.13.3 Role of the Controller of Certifying Authorities .....	52
9.14 Governing law.....	52
9.15 Compliance with applicable law .....	52
9.16 Miscellaneous provisions.....	52
9.16.1 Force Majeure .....	52
9.16.2 Entire agreement.....	52
9.16.3 Assignment .....	52
9.16.4 Severability .....	53
9.16.5 Enforcement (attorneys' fees and waiver of rights).....	53
9.17 Other provisions .....	53

# 1. Introduction

## 1.1 Overview

The dataedge CA utilizing Public Key Infrastructure (“PKI”) technology and operating as a Licensed Certification Authority (“dataedge CA”) under the Root Certificate Authority of Bangladesh, will issue a public key certificate to external subscribers for use in relying party applications. This Certification Practice Statement (“CPS”) describes the policies and practices of the dataedge CA, and sets forth the obligations of subscribers who use the certificates. A subscriber (“Subscriber”) is an individual, a named employee named or an agent of an organization who is issued a certificate under the Bangladesh Root CA Hierarchy by dataedge CA. By receiving a certificate the subscriber agrees to the provisions of the CPS.

## 1.2 Document name and identification

This CPS is called the dataedge Certification Authority Certificate Practice Statement. Object Identification (OID): 2.16.50.1.6.1

## 1.3 PKI participants

The following are roles to relevant to the administration and operation of the dataedge CA.

### 1.3.1 Certification Authorities

data edge limited located in Dhaka, Bangladesh operates the dataedge CA.

The dataedge CA will issue a certificate, which links a public and private key pair, to a Subscriber. In general, any individual may be a subscriber, although the dataedge CA may issues server certificates (SSL Certificates or Server Certificates) and object code-signing certificates. Certificates may be issued in several ways. Some certificates would be issued after the subscriber follows defined steps to generate online through a website set-up for this purpose by the CA – browser based certificates. Other certificates may be issued on a Token – Token Based Certificates. Unless otherwise noted, the obligations set forth in the CPS apply to server-based, browser-based and token-based certificates.

### ~~1.3.2~~ Subordinate CA

Sub CA is a “technical CA” with its own set of keys specially created for the customer (usually an organization, community or a Closed User Group (CUG)). This technical CA is signed by dataedge CA, thus making it a “Sub CA”. The key pair of these Sub-CAs are managed and operated by dataedge CA.

### 1.3.3 Registration Authorities

A Registration Authority is authorised personnel of the dataedge CA or an external agent appointed by the CA that collects and processes Subscriber requests containing information about the Subscriber’s identity, roles and other information and authorised the request for issuance or rejects the same.

### 1.3.4 Subscribers

A Subscriber is a named individual who is issued a digital certificate. This certificate may be required to access relying party applications. In addition to the certificate other security methods may be employed by the relying party application.

A Subscriber must follow request and retrieve the certificate from a specified website of the dataedge CA in accordance with the procedure identified in this CPS.

In the case of Server and Code Signing certificates, a designated Technical Contact would be issued the certificate upon request and in compliance with the procedures laid down in this CPS.

### 1.3.5 Relying parties

Parties relying on the certificate ("Relying Parties") are application providers who permit the Subscriber to use the certificate to access the applications except in the case of Server Certificate and other object code-signing certificate. Relying parties would be those applications and application providers who provide application services and recognised certificates as per the Bangladesh ICT Act.

### 1.3.6 Other participants

Parties other than the signer, relying parties or issuing certifying authorities would constitute other participants.

## 1.4 PKI participants obligations

### 1.4.1 Certifying Authority and Registration Authority Obligations

The dataedge CA is responsible for:

1. Acting in accordance with the guidelines of the Controller of Certifying Authorities, Bangladesh; policies and procedures designed to safeguard the certificate management process, including certificate issuance, certificate renewal, certificate revocation and audit trails and to protect dataedge CA private key.
2. Validating the information provided by the authorised RAs.
3. Issuing a certificate to a Subscriber after properly formatted and verified certificate request is received by the dataedge CA.
4. Creating and maintaining an accurate Certificate Revocation List ("CRL")
5. Maintaining this CPS
6. ~~C~~reating and auditing an accurate audit trail

An RA is responsible for the following:

1. Validating information submitted to the RA by the Subscriber concerning the request for certificate and the certificate request
2. Forwarding a validated certificate request to the dataedge CA
3. Intimating the Subscriber or other end entity of authorization codes after receiving a properly completed and verified certificate request from Subscriber or end entity.
4. Confirming certificate revocation requests with the Subscriber.
5. Confirming and initiating validated certificate renewal requests
6. Creating and maintaining an accurate audit trail.

These responsibilities of the dataedge RA and other appointed RA's are illustrative and not exclusive. Any one or more responsibilities may be brought in by dataedge CA.

The dataedge CA will issue certificates to a Subscriber within a reasonable time after a properly formatted certificate request is received and verified by the dataedge CA. See section CPS # 4.3 for certificate issuance process.

A certificate will be revoked as soon as possible following receipt of a revocation request and its confirmation, but action on a revocation request made over a weekend or holiday may be delayed until following business day of the RA, except as otherwise provided. Revoked certificates are published in a CRL and or pushed to the OCSP server.

#### 1.4.2 Certifying Authority Obligations

Technical CA's and sub CAs perform the specific obligations appearing throughout this CPS. The provisions of the CPS specify obligations of each category of technical CAs and sub CA's: dataedge CA in its CA centre and PKI Customers.

In addition, dataedge CA uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within dataedge CA's Sub-domain. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrolment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. Similarly, Resellers (where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by dataedge CA. The Subscriber Agreements and Relying Party Agreements used by dataedge CA, and Resellers must include the provisions required by CPS

PKI Customers are permitted to use Subscriber Agreements specific to them, although not required to do so. PKI Customers using Subscriber Agreements must include the provisions required by CPS. If a Managed PKI Customer or Reseller does not use its own Subscriber Agreement, the Subscriber Agreement of dataedge CA shall apply. If a Reseller has no Relying Party Agreement, the Relying Party Agreement of dataedge CA shall apply.

#### 1.4.3 Registration Authority Obligations

RAs assist dataedge CA by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. The provisions of the CPS specify obligations of each category of RAs.

#### 1.4.4 Subscriber Obligations

Subscriber obligations in the CP apply to Subscribers within dataedge CA's Sub-domain, through this CPS, by way of Subscriber Agreements. Certain Subscriber Agreements in force within dataedge CA's Sub-domain appears at: <http://www.dataedgeid.com/cps>

Within dataedge CA's domain of services, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscriber Agreements apply the specific obligations appearing in the CPS to Subscribers in Bangladesh and Bangladesh Root Certificate Authority hierarchy. Subscriber Agreements require Subscribers to use their Certificates in accordance with CPS. They also require Subscribers to protect

their private keys in accordance with CPS. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify the entity that approved the Subscriber's Certificate Application, either a sub CA or an RA, in accordance with CPS and request revocation of the Certificate in accordance with CPS, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under CPS.

Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the dataedge CA Public Hierarchy and shall not otherwise intentionally compromise the security of the dataedge CA Public Hierarchy CA Services.

#### 1.4.5 Relying Party Obligations

Relying Party obligations apply to Relying Parties within dataedge CA's domain of services, through this CPS, by way of dataedge CA's Relying Party Agreements. Relying Party Agreements in force within dataedge CA's Sub-domain appear at: <http://www.dataedgeid.com/cps>

Relying Party Agreements within dataedge CA's Sub-domain state that before any act of reliance, Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that dataedge CA, sub CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CPS and for purposes prohibited in CPS.

Relying Party Agreements further state that Relying Parties must utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Party Agreements also require Relying Parties to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CPS. If any of the Certificates in the Certificate Chain have been revoked, according to Relying Party Agreements, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

Relying Party Agreements state that if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the dataedge CA Public Hierarchy and shall not otherwise intentionally compromise the security of the dataedge CA Public Hierarchy CA Services.

### 1.4.6 Repository Obligations

dataedge CA is responsible for the repository functions for its own technical & sub CA s and the sub CAs of its PKI Customers. dataedge CA publish Certificates they issue in the repository set forth in Table below in accordance with CPS

CA	Entity Issuing the Certificate on Behalf of the CA	Applicable Repository
All dataedge CA technical & sub CAs	dataedge CA	dataedge CA Repository
PKI Customer	dataedge CA	dataedge CA Repository

Table – Applicable Repositories by Type of technical & sub CA

Upon revocation of an end-user Subscriber’s Certificate, dataedge CA publishes notice of such revocation in the repository required by Table above. dataedge CA issues CRLs for its own technical & sub CAs of PKI Customers, within its Sub-domain, pursuant to CPS. In addition, for PKI Customers who have contracted for Online Certificate Status Protocol (“OCSP”) services, dataedge CA provides OCSP services pursuant to CPS

## 1.5 Certificate usage

### 1.5.1. Appropriate certificate uses

The digital signature certificate usage is issued for the purposed indicated the certificate usage field of the certificate. These are to be used in relying party application for the purpose of online authentication and carrying digital signatures on electronic records.

### 1.5.2 Prohibited certificate uses

Using a certificate for any other purpose other than those indicated in the Usage field is prohibited. In addition it is prohibited to use a certificate which constitutes an offence under Chapter 8 of the ICT Act 2006.



## 1.6 Policy administration

### 1.6.1 Organization administering the document

This CPS is administered by the dataedge CA. dataedge CA may be contacted at the following location <http://www.dataedgeid.com>

Mail Address:  
 data edge limited  
 Sadharan Bima Bhaban – 2 (10<sup>th</sup> & 13<sup>th</sup> Floor),



139 Motijheel C.A.  
Dhaka – 1000.  
Tel: +88 02 9585949 - 52;  
Fax: +88 02 9585955  
Email: info@dataedgeid.com

### 1.6.2 Contact person

Md. Asifuzzaman, Managing Director.  
Tel: +88 02 7112783  
Fax: +88 02 9585955  
Email: asif@dataedgeid.com

### 1.6.3 Person determining CPS suitability for the policy

The dataedge Certifying Authority is the person who would determine the suitability of the CPS for the policy in accordance with the guidelines provided by the CCA, Bangladesh.

### 1.6.4 CPS approval procedures

Amendments to this CPS shall be made by dataedge CA and approved by Controller of Certifying Authorities, Bangladesh. The amendments shall either be in whole CPS document form or an update. Amended versions or updates shall be linked to the dataedge CA Repository located at: dataedge CA Website. Updates always supersede any designated or conflicting provisions of the referenced version of the CPS.

## 1.7 Definitions and acronyms

### 1.7.1 Definitions

The following definitions are to be used while reading this CPS. The following terms shall bear the meanings assigned to them hereunder and such definitions shall be applicable to both the singular and plural forms of such terms:

- **“Act”**: Unless otherwise specified the word ‘Act’ or ‘IT Act’ in this CPS refers to “the law of information and communication technology law 2006” & amendments there to
- **“dataedge CA”** a brand name, refers to dataedge Certificate Authority, owned by data edge limited, which is licensed by Controller of Certifying Authorities (CCA), Govt. of Bangladesh under ICT Act, and includes the associated infrastructure as mentioned in this CPS for providing Certification & Trust services .
- **“data edge limited”** refers to a Matrix company which is a registered Private Company limited by Shares.
- **“Applicant”** or **“User”** means a person, entity or organization that has requested for a digital signature certificate to be issued by dataedge CA.
- **“Auditor”** means any Audit organizations appointed by dataedge CA and empanelled by Controller of Certifying Authorities (CCA) for auditing of Licensed CA.

- **"Digital signature"** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of the IT Act;
- **"Digital signature certificate"** or the **"certificate"** means a digital signature certificate issued by dataedge CA to the Applicant. It also means a Digital Signature Certificate issued under Section 36 of ICT Act
- **"CA"** refers to dataedge Certificate Authority, as licensed by CCA, Bangladesh to issue digital signature certificate.
- **"Controller"** means the Controller of Certifying Authorities appointed as per Section 18(1) of the Act.
- Unless otherwise specified, the word **"CPS"** used throughout this document refers to Certification Practice Statement of dataedge CA
- **"Private Key"** means that part of cryptographic key pair generated for creating Digital Signature and is held privately by the subscriber.
- **"Registration Authority"** or **"RA"** means an entity or organization trusted under dataedge CA hierarchy that has the right to verify the credentials of the applicant/subscriber before forwarding to dataedge CA for issuance and revocation of certificate etc.
- **"Subscriber"** means a person, entity or organization in whose name the Digital Signature Certificate is issued by the Certificate Authority.
- Note: The contextual meaning of the terms may be considered for such terms that are used in this CPS but not defined above.

### 1.7.2 List of acronyms and abbreviations used in this cps

Acronym	Term
CA	Certifying Authority
CCA	Controller Of Certifying Authorities
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ITU	International Telecommunications Union
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Sockets Layer
SUB-CA	Subordinate Certifying Authority
URI	Uniform Resource Indicator
URL	Uniform Resource Locator

## 2. Publication and repository responsibilities

### 2.1 Repositories

dataedge CA uses directory service following the LDAP protocol for publishing and distributing the certificate issued to its Subscribers. The dataedge CA maintains a certificate revocation list "CRL", a list of all the certificates revoked and made non-operations and is accessible to relying party applications.

The dataedge CA maintains a repository for its CPS and the certification policies it support. This repository is located at the dataedge CA Website URL <http://www.dataedgeid.com/cps>

### 2.2 Publication of certification information

Certificates issued by dataedge CA are published into the directory server. This is accessible over the Internet. Relying parties and subscribers can download certificates.

### 2.3 Time or frequency of publication

Certificates are published into the directory on a real time basis by the CA software. CRLs are published once every 24 hours. Further, dataedge CA makes available an OCSP server to registered relying parties for online validation of certificates.

### 2.4 Access controls on repositories

The repositories are accessed for updating only by the CA software; all other access is only for reading certificate information. Users can access the directory and need to provide relevant certificate information to access the certificate.

## 3. Identification and authentication

### 3.1 Naming

dataedge technical CA Certificates contain X.500 Distinguished Names in the Subject fields as per Certificate Interoperability Guidelines - 2012 from the office of CCA, Bangladesh.

dataedge technical CA Subject Distinguished Names consist of the components specified in Table below.

<b>Attribute</b>	<b>Value</b>
<b>dataedge CA:</b>	
Common Name (CN) =	dataedge CA
House Identifier	Sadharan Bima Bhaban-2 (13 <sup>th</sup> Floor)
Street Address	139 Motijheel C.A, Dhaka
Postal Code	1000
Organizational Unit (OU) =	Certifying Authority
Organization (O) =	data edge limited
Country (C) =	BD

dataedge technical Sub-CA Subject Distinguished Names consist of the components specified in Table below.

<b>Attribute</b>	<b>Value</b>
<b>dataedge Sub-CA:</b>	
Common Name (CN) =	dataedge sub-CA for "Branding Name"
Organizational Unit (OU) =	Sub-CA
Organization (O) =	data edge limited
Country (C) =	BD

End-user Subscriber Certificates contain an X.500 distinguished name in the Subject name field as per Certificate Interoperability Guidelines from the office of CCA, Bangladesh and consist of the components specified in Table below:

<b>Attribute</b>	<b>Value</b>
<b>Subscriber :</b>	
Common Name (CN) =	Name string of maximum 64 characters constructed in the following manner: "Surname" "Given Name" "Initials"
Serial Number =	Serial Number will be generated by individual CAs complying uniqueness.
Unique Identifier =	This is a reserved attribute for future use and shall be used in the future for SHA 256 hash of National ID or any other Unique ID for individuals.
Locality =	Max Length: 60 Characters This attribute value MUST be populated with the name of the State / Province of Subject's residential or office address (if any).
Postal Code =	Post Code for the for Subject's residential or office address
Organizational Unit (OU) =	Max Length: 64 Characters This attribute MUST either contain the name of the department or sub-division of the organization the person belongs to if the certificate is being issued for official purposes OR must not be used. The Organizational unit must not be present when the organization has been marked as "personal"
Organization (O) =	Max Length: 64 Characters This attribute MUST contain either Name of the organization the person belongs to – if such information has been verified by the CA OR Contain string "Personal"
Country (C) =	Max Length: 2 Characters For Bangladesh Country code is BD

### 3.1.1 Types of names

### 3.1.2 Need for names to be meaningful

Names used shall identify the person or entity to which they are assigned in a meaningful way. The name assigned to the Common Name attribute is composed of the Subscriber's first name, followed by a space, followed by the Subscriber's Surname.

### 3.1.3 Anonymity or pseudonymity of subscribers

Subscribers are required to provide verifiable names to be included in the certificate. A Certificate is used for authentication and hence it is necessary to include only names that can be validated against established credentials like Machine Readable Passport, National ID Card or other such documents issued by a competent authority.

### 3.1.4 Rules for interpreting various name forms

Rules for interpreting names would follow X.500 convention.

### 3.1.5 Uniqueness of names

dataedge CA ensures that Subject Distinguished Names are unique within the domain of a specific CA through automated components of the Subscriber enrolment process.

### 3.1.6 Recognition, authentication, and role of trademarks

dataedge CA follows the X.500 standards for names and would follow the guidelines provided by the Controller of Certification Authorities, Bangladesh in implementing the standards applicable to naming conventions.

## 3.2 Initial identity validation

As a part of the validation process, the subscriber's identification information from trusted third party credentials such as Passport, Driving License, National Identity Card is used to validate the information provided by the subscriber.

### 3.2.1 Method to prove possession of private key

The dataedge CA will have proof that the Subscriber possesses the private key, by validating a Subscriber's Digital Signature which is included as part of the Subscriber's certificate request.

### 3.2.2 Authentication of organization identity

Subscriber Organization included in the certificate is authenticated by validating certificate of existence of establishment issued by a competent authority where the organization is established. This information is validated against a published trusted third party database or certified by a member of notary.

### 3.2.3 Authentication of individual identity

For all Classes of individual Certificates, dataedge CA confirm that:

- the Certificate Applicant is the person identified in the Certificate Application,
- the Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS # 3.2.1, and
- the information to be included in the Certificate is accurate, except for Non-verified Subscriber Information.

In addition, dataedge CA performs the more detailed procedures described below for each Class of Certificate.

### 3.2.3.1 Class 1 Certificate

The only verification is a simple check of the non-ambiguity of the common name and email id combination within the dataedge CA repository, plus a limited verification of the e-mail address.

### 3.2.3.2 Class 2 Certificates

dataedge CA validates certificate applications for Class 2 Certificates by determining if identifying information in the certificate application matches with information mentioned with identity proof submitted along with certificate application form..

### 3.2.3.3 Class 3 Certificates

The authentication of Class 3 individual Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before an authorized dataedge representative, or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent or other official checks the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a Machine Readable Passport or National Identity Card which carries a photograph of the individual.

### 3.2.3.4 SSL Certificates

dataedge CA validates certificate applications for SSL Certificates by determining the ownership of domain name through third party domain registration database and validating legality of the applicant company against the government issued proof of right to do business certificate.

### 3.2.4 Non-verified subscriber information

Subscriber's address is not verified and not included in the certificate. These are collected as a part of the standard application form.

### 3.2.5 Validation of authority

Wherever any one is authorised to receive a certificate on behalf of an organization, then a certificate from an authorised signatory of the organization where company is used to validate the same. The authorised signatory should support his or her claim with a board resolution that certifies the list of authorised signatories.

### 3.2.6 Criteria for interoperability

Interoperability guidelines issued by the CCA, Bangladesh would be considered in establishing the criteria to recognize interoperability.

### 3.3 Identification and authentication for re-key requests

Re-key requests from Subscriber's should be accompanied with an original certificate and fresh CSR containing the new key pair.

#### 3.3.1 Identification and authentication for routine re-key

Routine re-keys from subscribers are treated as fresh certificates request and complete validation of the subscriber as applicable to fresh certificate is carried out.

#### 3.3.2 Identification and authentication for re-key after revocation

Re-key request after revocation from subscribers are treated as fresh certificates request and complete validation of the subscriber as applicable to fresh certificate is carried out.

### 3.4 Identification and authentication for revocation request

Prior to the revocation of a Certificate, dataedge CA verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber's Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

## 4. Certificate life-cycle operational requirements

### 4.1 Certificate Application

For dataedge CA Certificates, all end-user Certificate Applicants shall undergo an enrolment process consisting of:

- Completing a Certificate Application and providing the required information,
- Generating, or arranging to have generated, a key pair in accordance with CPS,
- The Certificate Applicant delivering his, her, or its public key, directly or through an RA, to dataedge CA, in accordance with CPS,
- Demonstrating to dataedge CA pursuant to CPS that the Certificate Applicant has possession of the private key corresponding to the public key delivered to dataedge CA, and
- Manifesting assent to the relevant Subscriber Agreement.

Certificate Applications are submitted either to dataedge CA, or RA for processing, either approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CPS may be two different entities as shown in the following table.

<b>Certificate Class/Category</b>	<b>Entity Processing Applications</b>	<b>Certificate</b>	<b>Entity Issuing Certificate</b>
Class 1	dataedge CA or dataedge RA		dataedge Class 1 CA
Class 2	dataedge CA or dataedge RA		dataedge Class 2 CA
Class 3	dataedge CA or dataedge RA		dataedge Class 3 CA

#### 4.1.1 Who can submit a certificate application

The subscriber or an authorised representative can submit a certificate application. However, for class 3 certificates and other certificates the subscriber should present himself or herself to a registration authority or agent for the purpose of registration.

#### 4.1.2 Enrolment process and responsibilities

The subscriber should enrol for the certificate. The subscriber is responsible for the correctness of information provided in the enrolment and key pair generation and safe keeping of private key. The subscriber should further receive the certificate upon intimation.

### 4.2 Certificate application processing

#### 4.2.1 Performing identification and authentication functions

Registration Authority or Agents are the authorised representative of the Certifying Authority who will carry out the identification and authentication functions.

#### 4.2.2 Approval or rejection of certificate applications

Based on the validation process, the application may be approved or rejected by the Registration Authorities or Agents.

#### 4.2.3 Time to process certificate applications

The certificate applications would be taken up for processing and completed within 2 working days.

### 4.3 Certificate issuance

dataedge CA issues certificate to Subscribers and End Entities subject to the following practice details below in the following sections.

#### 4.3.1 CA actions during certificate issuance

A Subscriber or End Entity submits certificate request to the dataedge RA or other authorised RA along with the prescribed documents. The RA validates the information provided approves or rejects the request.

A Certificate is created and issued following the approval of a Certificate Application or following receipt of an RA's request to issue the Certificate. dataedge CA creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.



#### 4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA would notify the subscriber through mail of the issuance of certificate and the subscriber is expected to pick up the certificate as instructed in the mail notification.

### 4.4 Certificate acceptance

Upon Certificate generation, dataedge CA notifies Subscribers that their Certificates are available and notifies them of the means for obtaining such Certificates.

Upon issuance, Certificates are made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate. For example, dataedge CA may send the Subscriber a PIN, which the Subscriber enters into an enrolment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail message. Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

#### 4.4.1 Conduct constituting certificate acceptance

A subscriber is deemed to have accepted the certificate when they have not explicitly intimated the CA about their refusal to accept the certificate citing reasons within 2 days of receiving certificate issuance intimation from the CA.

#### 4.4.2 Publication of the certificate by the CA

The CA will publish the certificate in the directory immediately after issuance.

#### 4.4.3 Notification of certificate issuance by the CA to other entities

The CA will only notify the subscriber of certificate issuance and publish the certificate in the repository.

### 4.5 Key pair and certificate usage

Key usage is specified in the certificate. The subscriber is responsible for the private key and its usage. The CP specifies the usage of certificate for specific relying party applications. For E.g. A subscriber's certificate with a key usage field indicating Authentication and Non-repudiation can be used only for authentication and carrying digital signatures. This certificate cannot be used for encryption of data. Likewise a certificate with Key Usage field set as Key Encipherment should be used only for encryption and not for non-repudiation.

#### 4.5.1 Subscriber private key and certificate usage

Subscriber private usage is set in the certificate based on the class policy definition in the CP. Subscriber and application should follow the key usage attributes and not violate the key usage attributes.

#### 4.5.2 Relying party public key and certificate usage

Relying party receives the Public key of the subscriber and can use the same as per the key usage field set in the certificate.

## 4.6 Certificate renewal

No stipulation.

## 4.7 Certificate re-key

Certificate re-key is not supported, Certificate can re- issue.

## 4.8 Certificate modification

### 4.8.1 Circumstance for certificate modification

Not supported, subscriber to seek fresh certificate and follow the enrolment process applicable for new certificates.

### 4.8.2 Who may request certificate modification

Not applicable, please refer CPS #4.8.1

### 4.8.3 Processing certificate modification requests

Not applicable please refer CPS #4.8.1

### 4.8.4 Notification of new certificate issuance to subscriber

Not applicable please refer CPS #4.8.1

### 4.8.5 Conduct constituting acceptance of modified certificate

Not applicable please refer CPS #4.8.1

### 4.8.6 Publication of the modified certificate by the CA

Not applicable please refer CPS #4.8.1

### 4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable please refer CPS #4.8.1

## 4.9 Certificate revocation and suspension

An end-user Subscriber Certificate is revoked if:

- dataedge CA or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- dataedge CA has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- dataedge CA has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the

Certificate was issued without the authorization of the person named as the Subject of such Certificate,

- dataedge CA has reason to believe that a material fact in the Certificate Application is false,
- dataedge CA determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with CPS
- Statutory, law enforcement or any other authorized government bodies' request for the revocation of a subscriber's certificate or any other order affecting the usage of the certificate.

dataedge CA may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

dataedge CA Subscriber Agreements require end-user Subscribers to immediately notify dataedge CA of a known or suspected compromise of its private key in accordance with the procedures in CPS

**The revocation of the Certificate shall be done after adopting the process prescribed in the Bangladesh ICT Act and rules and regulations made there under.**

#### 4.9.1 Circumstances for revocation

dataedge CA will revoke sub CA, RA, or infrastructure Certificates if:

- dataedge CA discovers or has reason to believe that there has been a compromise of the sub CA, RA, or infrastructure private key,
- The agreement between the sub CA or RA with dataedge CA has been terminated,
- dataedge CA discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- dataedge CA determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- The sub CA or RA requests revocation of the Certificate.
- Statutory, law enforcement or any other authorized government bodies' request for the revocation of a subscriber's certificate or any other order affecting the usage of the certificate.

The revocation of the Certificate shall be done after adopting the process prescribed in the Bangladesh ICT Act and rules and regulations made there under.

#### 4.9.2 Who can request revocation

The following entities may request revocation of Subscriber Certificate:

- dataedge CA or the RA that approved the Subscriber's Certificate Application may request the revocation of any Subscriber or Administrator Certificates in accordance with CPS
- Individual Subscribers or Administrator or RA may request revocation of their own individual Certificates.

- Statutory or Law Enforcement agency of the Govt of Bangladesh

The following entities may request revocation of a sub CA, RA, or infrastructure Certificate:

- Only dataedge CA is entitled to request or initiate the revocation of the Certificates issued to its own sub CAs, RAs, or infrastructure components.
- Statutory or Law Enforcement agency of the Govt of Bangladesh

#### 4.9.3 Procedure for revocation request

Revocation request must be submitted in writing or electronically by a Subscriber and confirmed by the RA in order to be processed and validated.

A Subscriber requesting revocation is required to communicate the request to dataedge CA or the RA approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly.

dataedge CA may only initiate sub CA Certificate revocation.

#### 4.9.4 Revocation request grace period

Revocation requests must be submitted as promptly as possible within a reasonable period.

#### 4.9.5 Time within which CA must process the revocation request

The CA will process the request for revocation within 2 (Two) days or reasonable time after firmly establishing the genuineness of such request.

#### 4.9.6 Revocation checking requirement for relying parties

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

A "CRL reference Table" is posted in the Repository to enable Relying Parties to determine the location of the CRL for the relevant CA.

#### 4.9.7 CRL issuance frequency

dataedge CA publishes CRLs showing the revocation of dataedge CA Certificates and offers status-checking services. CRLs for CAs that issue end-user Subscriber Certificates are published daily. CRLs for CAs that only issue sub-CA Certificates are published quarterly and whenever such a CA Certificate is revoked. Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration.

#### 4.9.8 Maximum latency for CRLs

CRLs will be published every 24 hours by the CA. Download of CRL and validation latencies are network and relying party application dependent and the CA is not responsible for any such latencies.

#### 4.9.9 On-line revocation/status checking availability

In addition to publishing CRLs, dataedge CA provides Certificate status information through query functions in the dataedge CA repository.

dataedge CA also provides OCSP Certificate status information for specific Relying Parties. Relying parties who contract for OCSP services may check Certificate status with OCSP. The URL for the relevant OCSP Responder is communicated to then subscribing Relying Party.

#### 4.9.10 On-line revocation checking requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using one of the applicable methods specified in CPS.

#### 4.9.11 Other forms of revocation advertisements available

No stipulation.

#### 4.9.12 Special requirements re key compromise

In addition to the procedures described in CPS, dataedge CA will make commercially reasonable efforts to notify potential Relying Parties of such a compromise.

#### 4.9.13 Circumstances for suspension

dataedge CA, by itself or on the recommendation of the RA or on the request of a subscriber may suspend a Digital Signature Certificate as per Bangladesh ICT ACT section 39 in the following circumstances:

- Non-payment of applicable Digital Signature Certificate fees
- Any circumstance which RA or the Subscriber believes that it requires suspension of the digital certificate

#### 4.9.14 Who can request suspension

The following entities may request revocation of Subscriber Certificate:

- dataedge CA or the RA that approved the Subscriber's Certificate Application may request the revocation of any Subscriber or Administrator Certificates in accordance with CPS
- Individual Subscribers or Administrator or RA may request revocation of their own individual Certificates.
- Statutory, law enforcement or any other authorized government bodies' request for the revocation of a subscriber's certificate or any other order affecting the usage of the certificate.

#### 4.9.15 Procedure for suspension request

Suspension request must be submitted in writing or electronically by a Subscriber and confirmed by the RA in order to be processed and validated.

A Subscriber requesting suspension is required to communicate the request to dataedge CA or the RA approving the Subscriber's Certificate Application, who in turn will initiate suspension of the certificate promptly.

#### **4.9.16 Limits on suspension period**

Subscriber should request for activation of suspended Digital Signature Certificate within 15 days of the date of suspension, if request is not received within 15 days, dataedge CA reserve the right to revoke the suspended Digital Signature Certificates of its Subscribers.

#### **4.9.17 Who can request for Activation of the Suspended Digital Certificate**

Subscriber can initiate a request for activation of his suspended Digital Signature Certificate, RAs may only initiate the request for activation for those Digital Signature Certificate for which they had initiated the suspension.

A Digital Signature Certificate shall be activated only if dataedge CA is satisfied that the reason for suspension is no longer valid.

### **4.10 Certificate status services**

Online certificate status is available to register relying parties and other subscribers. This is standards compliant OCSP responder which provides a standard OCSP response from registered relying parties.

#### **4.10.1 Operational characteristics**

A standards compliant OCSP client can place a request to the dataedge OCSP responder. The OCSP responder would provide a standard response based on the status of the certificate.

#### **4.10.2 Service availability**

The service would be available 24 x 7 to registered relying parties only. The process of registration and details of usage are separately provided under a separate agreement between dataedge CA and the relying party.

#### **4.10.3 Optional features**

Not applicable

### **4.11 End of subscription**

On expiry of the validity period of the certificate or on its revocation by the subscriber or by any other authorised body as described in this CPS, the subscription ends.

### **4.12 Key escrow and recovery**

Key escrow services are not currently provided by dataedge CA. As and when these services become available the description for the same would be included in the CPS.

## **5. Facility, management, and operational controls**

dataedge has implemented the dataedge Security Policy, which supports the security requirements of this CPS.

## 5.1 Physical controls

### 5.1.1 Site location and construction

dataedge CA is located in secure building which implements access control mechanism to the CA operations centre. The CA computer and network infrastructure are housed in 3 tier model with procedure to mitigate covert or overt penetration into the center. The centre is designed as per best practices and guidelines of ICT Act and CCA guidelines.

CA Office and documents is located in Tier 1

Subscriber validation documents is located in Tier 2

Sensitive servers are located in Tier 3

Online CA Cryptographic modules are stored in Tier 4 Online.

Offline CA cryptographic modules stored in Tier 6

### 5.1.2 Physical access

dataedge CA systems are protected by three tiers of physical security, with access to the lower tier required before gaining access to the higher tier. In addition, the physical security system includes three additional tiers for key management security. The characteristics and requirements of each tier are described in Table below.

<b>Tier</b>	<b>Description</b>	<b>Access Control Mechanisms</b>
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge. Physical access to tier one is automatically logged and video recorded.  Also have 24X7 manned security.
Physical Security Tier 2	Tier two is the tier at which sensitive validation documents will be stored.	Access to this tier requires the use of a proximity card and Bio-Metric badge. Physical access to tier two is automatically logged and video recorded.
Physical Security Tier 3	Tier three is the first tier at which sensitive CA operational activity takes place. Sensitive CA operational activity is any activity related to the lifecycle of the certification process such as authentication, verification, and issuance.	Tier 3 enforces individual access control through the use of two-factor authentication including biometrics. Individuals approved for unescorted tier 3 access must satisfy the Trusted Employee Policy. Unescorted personnel, except those authorized, including un-trusted employees or visitors, are not allowed into a tier-three secured area. Physical access to tier three is automatically logged and video recorded.

<b>Tier</b>	<b>Description</b>	<b>Access Control Mechanisms</b>
Physical Security Tier 4	Tier four is the tier at which especially sensitive CA operations occur.	The tier four enforces dual access control. each with two-factor authentication including biometrics. Individuals approved for unescorted tier four accesses must satisfy the Trusted Employee Policy. Physical access to tier four is automatically logged and video recorded.
Key Management Tiers 5-6	Key Management tiers five to six serve to protect offline storage of tokens / keys and keying material.	Offline Tokens / Keys are protected with locked safes, cabinets and containers. Access to Tokens / Keys and keying material is restricted in accordance with data edge's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers are logged for audit purposes. Progressively restrictive physical access privileges control access to each tier.

Table - Physical Security Tiers

### 5.1.3 Power and air conditioning

dataedge CA's secure facilities are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

### 5.1.4 Water exposures

dataedge CA has taken reasonable precautions to minimize the impact of water exposure to dataedge CA systems.

### 5.1.5 Fire prevention and protection

dataedge CA has taken reasonable precautions for the prevention and to extinguish fires or other damaging exposure to flame or smoke. dataedge CA's fire prevention and protection measures are designed to comply with local fire safety regulations.

### 5.1.6 Media storage

Store within dataedge CA facilities and in secure offsite storage facility, all media containing production software and data, audit, archive, or backup information are stored within dataedge CA facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

### 5.1.7 Waste disposal

Shred sensitive documents and material before disposing. Magnetic and other storage Media used to collect or transmit sensitive information are rendered unreadable before disposal. Destruct



Cryptographic devices or initialise it as per manufacturer's guidance before disposal. Dispose other waster as per dataedge CA's normal waste disposal requirements.

### 5.1.8 Off-site backup

dataedge CA performs routine backups of critical system data, audit log data, and other sensitive information.

## 5.2 Procedural controls

### 5.2.1 Trusted roles

Employees, contractors and consultants who have access to or control authentication or cryptographic operations and may materially affect:

- The validation of information in Certificate Applications;
- Carry out or participate in the certificate life cycle operations processing activities such as Certificate Applications, issuance, renewal or revocation requests, or renewal requests, or enrolment information, access to repository
- Or the handling of Subscriber information or requests.

Are said to carry trusted operations

Trusted Persons include, but are not limited to:

- Personnel who perform customer services, cryptographic business operations, security personnel, system administration, designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.
- Examples of Trusted Persons in the context of dataedge CA
  - Key Manager – The person who is responsible manages the CA and SUB CA keys
  - Security Officer – The person who is responsible for the security operations of the CA
  - Private Key Share Holders – The people who hold shares of the dataedge CA private key.
  - Validation Officers
  - Dataedge Registration Authorities

dataedge considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of CPS

### 5.2.2 Number of persons required per task

dataedge maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (HSM or Hardware Security Module) and associated key material require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA HSM is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the

device. Persons with physical access to modules do not hold “Shares” and vice versa. Requirements for CA private key activation data and Shares are specified in CPS

### 5.2.3 Identification and authentication for each role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing dataedge CA HR [or equivalent] or security functions and a check of well-recognized forms of identification (e.g., passports and driver’s licenses). Identity is further confirmed through the background checking procedures in CPS 5.3.1.

dataedge CA ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities;
- Issued electronic credentials to access and perform specific functions on dataedge CA, RA, or other IT systems.

### 5.2.4 Roles requiring separation of duties

Security Manager, Key Manager, System Admin, Application Admin, Network Admin, Database Admin, Backup operator, Share Holders and RA’s would require role separation.

## 5.3 Personnel controls

### 5.3.1 Qualifications, experience, and clearance requirements

Employees full time, part time or contractual will need to meet the qualification and experience criteria specified from time to time. All employees will be cleared for appointment after background checks are carried as per the security policy of dataedge CA.

### 5.3.2 Background check procedures

Background checks will be conducted on the dataedge CA staff, prior to their assignment to a trusted role in the CA operations. The check would apply to not employees but also those who work on contract or consultant to dataedge CA

### 5.3.3 Training requirements

dataedge provides its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. dataedge CA periodically reviews and enhances its training programs as necessary.

### 5.3.4 Retraining frequency and requirements

dataedge would carry out retraining of CA personnel once every year.

### 5.3.5 Job rotation frequency and sequence

No stipulation

### 5.3.6 Sanctions for unauthorized actions

Depending upon the unauthorised action to be carried out by a CA personnel, the Certifying Authority will be notified of the said action and the same may sanctioned only by the CA.

### 5.3.7 Independent contractor requirements

Independent contractors performing operations of dataedge CA will meet the same stipulations as applicable dataedge employees. Contractors who are carrying repair functions or other maintenance functions will do so in the presence of authorised dataedge CA personnel.

### 5.3.8 Documentation supplied to personnel

Standard operating procedures and product manuals specific to the role will be available only for reference.

## 5.4 Audit logging procedures

### 5.4.1 Types of events recorded

dataedge CA manually or automatically logs the history of operational activities including CA key life cycle management, CRL, Certificate Subscriber applications and documents, Security-related events like , security system actions performed by dataedge CA personnel, security profile changes, Firewall and router activity, Visitor entry and exit records for CA operations center

Periodic review of dataedge CA's practices, procedures, and policies will be performed by internal auditors and CCA empanelled auditors.

### 5.4.2 Frequency of processing log

The logs are examined once every month.

### 5.4.3 Retention period for audit log

The logs are retained on archival media throughout the life of the CA.

### 5.4.4 Protection of audit log

Audit logs are digitally signed and rendered tamper evident by the CA application.

### 5.4.5 Audit log backup procedures

Audit log backup are carried out as per the Backup Policy.

### 5.4.6 Audit collection system (internal vs. external)

Carried out as stipulated by the Controller of Certifying Authorities, Bangladesh

### 5.4.7 Notification to event-causing subject

Such notification which are internal are reported to the CA and events affecting the subscribers are notified to the Controller of Certifying Authorities, Bangladesh

#### 5.4.8 Vulnerability assessments

Once every six months public facing servers are subject to VA and PT.

### 5.5 Records archival

The dataedge CA and RA records will be kept in accordance to the Bangladesh ICT Act and guidelines provided by the CCA.

#### 5.5.1 Types of records archived

All subscriber applications, CA data based, repositories are archived.

#### 5.5.2 Retention period for archive

Archive is retained for the life of the CA. Paper records are retained as per applicable Bangladesh laws

#### 5.5.3 Protection of archive

Multiple copies of archived data on removable media are made and stored in fire proof cabinets under securely.

#### 5.5.4 Archive backup procedures

Follows the backup procedures of dataedge CA backup policy.

#### 5.5.5 Requirements for time-stamping of records

CA logs are digitally signed for tamper evidence. Digital signatures carry time which is in sync with UTC source.

#### 5.5.6 Archive collection system (internal or external)

Data archival happens on two sets of backup media. One is stored in situ and the other is sent to the off site.

#### 5.5.7 Procedures to obtain and verify archive information

The Security Manager is the custodian of the archives. On a regular basis these tapes would be handed to the CA System Administrator to verify the archived information.

### 5.6 Key changeover

dataedge CA changeover is carried out on expiry of the CA keys. The CCA, relying parties and subscribers are notified about the key change over activity and its impact through the dataedge CA Website.

## 5.7 Compromise and disaster recovery

### 5.7.1 Key compromise

Upon the suspected or known Compromise of a dataedge CA, dataedge CA infrastructure or dataedge CA's Key Compromise Response procedures are enacted by the Compromise Incident Response Team (CIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other dataedge CA management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from dataedge CA executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the dataedge CA repository in accordance with CPS
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected participants
- The CA will generate a new key pair in accordance with CPS, except where the CA is being terminated in accordance with CPS.

### 5.7.2 Disaster Recovery \*

dataedge CA is in the process of setting up a DR. dataedge CA will provide back-up capability and use its best efforts to restore dataedge CA functionality at an alternate disaster recovery location in the event of system failure at dataedge CA.

### 5.7.3 Incident and compromise handling procedures

Incident and compromise handling procedures are stipulated in the dataedge Security Policy documents.

### 5.7.4 Computing resources, software, and/or data are corrupted

The entire CA and the data can be reconstructed using the backup material available in the event such software / data are corrupted.

### 5.7.5 Entity private key compromise procedures

dataedge CA recommends following the same standard for all subscribers in all its domain of services, irrespective of which hierarchy the subscriber is subscribing to. Subscriber Agreements state that Subscribers failing to meet these Standards are solely responsible for any loss or damage resulting from such failure.

dataedge CA would also like to point out here that the Bangladesh ICT Act holds the subscriber solely responsible for the protection of his or her private key.

### 5.7.6 Business continuity capabilities after a disaster

dataedge CA is in the process of setting up a DR. dataedge CA will provide back-up capability and use its best efforts to restore dataedge CA functionality at an alternate disaster recovery location in the event of system failure at dataedge CA.

## 5.8 CA or RA termination

dataedge CA reserves the right to terminate its function. In the event that it is necessary for a dataedge CA to cease operation, dataedge makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, dataedge will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable in line with the provisions of the ICT Act and rules and regulations made there under:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and other affected parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to sub-CA by dataedge,
- The preservation of the CA's archives and records for the time periods required in CPS
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services. The revocation of unexpired un-revoked Certificates of end-user Subscribers and subordinate CAs, if necessary. Compensation payments, if necessary, to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor or another CA,
- To dispose CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA, if applicable and necessary

## 6. Technical security controls

### 6.1 Key pair generation and installation

#### 6.1.1 Key pair generation

CA key pair generation is performed using Trustworthy pre-selected and trained people following trusted systems and procedures and required cryptographic key strength. FIPS 140-1 Level 2 or higher cryptographic modules are used for key generation for all CAs -- including dataedge CA and Sub- CAs. All CA key pairs are generated in pre-planned procedures for key generation. The activities performed in each key generation process are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by dataedge CA Management.

RA's generate key pair using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software or cryptographic token.

Subscriber key pair is generated by the subscriber typically using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software or cryptographic for key generation.

For server certificates (SSL), the subscriber typically uses the key generation utility provided with the web server software to generate the key pair.

### 6.1.2 Private key delivery to subscriber

End-user Subscriber key pairs are typically generated by the end-user Subscriber; therefore in such cases, private key delivery to a Subscriber is not applicable.

### 6.1.3 Public key delivery to certificate issuer

The subscriber will through the CSR provide the public key to the Issuer, namely dataedge CA.

### 6.1.4 CA public key delivery to relying parties

dataedge CA will publish the certificate along with the Public key in its repository. Relying parties may pick up public keys from the repository upon providing the required user information.

### 6.1.5 Key sizes

dataedge CA key pairs are all 2048 bit RSA. dataedge CA recommends that Registration Authorities and end-user Subscribers generate at least 1024 bit RSA key pairs to ensure they comply with the requirements of the Interoperability Guideline – 2012 issued by Bangladesh CCA.

### 6.1.6 Public key parameters generation and quality checking

dataedge CA will enable key pair generation through a control in the browser context for meeting the Subscriber online enrolment requirements

### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The certificate policy class will determine the contents of the Key Usage Field. These are inline with the X.509v3 standards.

Key Usage field in Signing certificates would contain Digital Signature and Non-Repudiation, while Encryption Certificates would contain Key Encipherment.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

dataedge CA private keys are generated and used from Hardware Security Module conforming to FIPS Level 2 standards. These modules are housed in multi tiered CA centre and do not leave the premises. Access to HSM is always through multi level authentication.

### 6.2.2 Private Key (M of N) multi-person control

Private Key operations of the dataedge CA are controlled by the use of m of n. The share holders are subject of role separation and subject to employee verification processes. “m” Share holders, not less than 3, have to come together to carry out a CA private key operation.

### 6.2.3 Private Key escrow

dataedge CA private keys are cloned onto HSM and retained at the off site.

Subscriber private key escrow services are not currently provided.

#### **6.2.4 Private Key backup**

dataedge CA private keys are cloned onto to backup HSM and retained in high security vault in the CA centre. The backup of private key is controlled activity involving the Security Officer, Key Manager and Share holders.

#### **6.2.5 Private Key archival**

The HSM tokens containing the private are preserved in high security vault until destroyed following manufacturer specified destruction process.

#### **6.2.6 Private Key transfer into or from a cryptographic module**

Private Key is transferred from one HSM into another under the supervision of the Security Office by the Key Manager and Share Holders.

#### **6.2.7 Private Key storage on cryptographic module**

dataedge CA private keys are stored only on HSM conforming FIPS Level 2 certification. These are tamper proof devices, in the event the HSM is tampered the private volatilizes.

#### **6.2.8 Method of activating private key**

The Key Manager activates the private key, it requires multiple persons to be available for activation.

#### **6.2.9 Method of deactivating private key**

The Key Manger deactivates the private key in accordance with the dataedge Key Management guidelines.

#### **6.2.10 Method of destroying private key**

Private key on HSM are destroyed as per OEM recommendations.

#### **6.2.11 Cryptographic Module Rating**

dataedge CA uses best in class HSM conforming to FIPS Level 3

### **6.3 Other aspects of key pair management**

Key expiry and key history are maintained by the Key Manager.

#### **6.3.1 Public key archival**

dataedge CA public is archived as a part of the standard archival process. It is also published in the dataedge CA website.

#### **6.3.2 Certificate operational periods and key pair usage periods**

dataedge CA certificate operational periods and key pair usage period are as per the Interoperability Guideline – 2012 issued by Bangladesh CCA



## 6.4 Activation data

Activation data such as key shares are stored in special purpose keys and these are in turn secured in lockers. Access to these keys required multiple people to pass through multiple levels of authentication.

### 6.4.1 Activation data generation and installation

Key Shares are generated by the HSM and installed on secure keys. These keys are in turn stored in high security lockers. Access to these lockers is governed by multiple people and multiple security tiers in the CA centre.

Where password or PINs are used, these are split into two portions and vested with two individuals. Both these individuals need to come together to activate.

### 6.4.2 Activation data protection

Activation data is stored secure tokens or keys as stipulated in CPS #6.4.1

### 6.4.3 Other aspects of activation data

Passwords conform to standard password security methods.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

dataedge CA deploys standard Intel Server with hardened Linux operating systems. Standard Penetration Testing and Vulnerability assessment are carried out twice every year to ascertain the effectiveness of security controls.

### 6.5.2 Computer security rating

Not Applicable in Bangladesh.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

dataedge CA is not a development environment. The product development environment follows high security standards applicable to information security products. Independent security controls are applied to ensure security levels are maintained.

### 6.6.2 Security management controls

No stipulation.

### 6.6.3 Life cycle security controls

No stipulation.

## 6.7 Network security controls

The CA servers are protected by Firewalls, IDS. The CA in itself is completely isolated from the Network and not exposed to the Internet.

## 6.8 Time-stamping

The logs and certificates are time stamped using a time stamping server and UTC is obtained from a GPS time source within the CA infrastructure.

## 7. Certificate, CRL, and OCSP profiles

### 7.1 Certificate profile

CPS defines dataedge CA's Certificate Profile and Certificate content requirements for Bangladesh Root CA Certificates issued under this CPS.

dataedge CA Certificates conform to the Interoperability Guideline – 2012 issued by Bangladesh CCA:

- (a) ITU-T Recommendation X.509 Version 3 and
- (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC 5280").

#### 7.1.1 Version number(s)

Digital Certificate X.509v3 and CRL Version V2 are supported

#### 7.1.2 Certificate extensions

X.509v3 Certificate extensions are supported

#### 7.1.3 Algorithm object identifiers

X.509v3 Signature Algorithm is RSA 2048 with support for SHA256

#### 7.1.4 Name forms

No specific stipulations

#### 7.1.5 Name constraints

No Specific stipulations

#### 7.1.6 Certificate policy object identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in this CPS.

#### 7.1.7 Usage of Policy Constraints extension

No stipulation

### **7.1.8 Policy qualifiers syntax and semantics**

dataedge CA populates X.509 Version 3 Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the dataedge CPS. In addition, some Certificates contain a User Notice Qualifier that points to the applicable Relying Party Agreement.

### **7.1.9 Processing semantics for the critical Certificate Policies extension**

No stipulation.

## **7.2 CRL profile**

dataedge CA issues CRLs that conform to RFC 5280. At a minimum, dataedge CA CRLs contain the basic fields and contents specified the RFC 3280

### **7.2.1 Version number(s)**

dataedge CA currently issues X.509 Version 2 CRLs.

### **7.2.2 CRL and CRL entry extensions**

No stipulation.

## **7.3 OCSP profile**

dataedge CA provides OCSP services in conformance to the Interoperability Guideline – 2012 issued by Bangladesh CCA.

### **7.3.1 Version number(s)**

dataedge CA provides OCSP services in conformance to RFC 2560

### **7.3.2 OCSP extensions**

dataedge CA provides OCSP services in conformance to RFC 2560

## **8. Compliance audit and other assessments**

### **8.1 Frequency or circumstances of assessment**

Internal audit would be carried out once every six months. External assessment once a year.

### **8.2 Identity/qualifications of assessor**

The external assessment is carried out by CCA empanelled assessor.

### **8.3 Assessor's relationship to assessed entity**

The Assessment is carried out as per the CCA guidelines.

## **8.4 Topics covered by assessment**

The Assessment is carried out as per the CCA guidelines.

## **8.5 Actions taken as a result of deficiency**

The recommendations of the assessor are carried out.

## **8.6 Communication of results**

Audit assessment results are communicated to the CCA.

# **9. Other business and legal matters**

## **9.1 Fees**

### **9.1.1 Certificate issuance or renewal fees**

Certificate fees are designed as per the guidelines from Office of the Controller of Certifying Authorities, Bangladesh.

### **9.1.2 Certificate access fees**

No fee is charged. Certificate can be accessed from the directory repository.

### **9.1.3 Revocation or status information access fees**

CRL's are published in the dataedge Website and can be accessed by relying party applications without any paying any access fees.

### **9.1.4 Fees for other services**

Relying parties and other users to contact dataedge CA service for fees applicable for OCSP, Time Stamping and other PKI related services.

### **9.1.5 Refund policy**

No Stipulation. dataedge CA would not refund certificate fees once it is accepted or deemed to be accepted.

## **9.2 Financial responsibility**

### **9.2.1 Indemnification by Subscribers and Relying Parties**

#### **9.2.1.1 Indemnification by Subscribers**

To the extent permitted by applicable law, dataedge CA's Subscriber Agreements require, and other Subscriber Agreements shall require, Subscribers to indemnify dataedge CA and any dataedge CA sub CAs or RAs for:

- **Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,**

- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

#### **9.2.1.2 Indemnification by Relying Parties**

To the extent permitted by applicable law, dataedge CA's Subscriber Agreements and Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify dataedge CA and any non-dataedge CA sub CAs or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

#### **9.2.2 Fiduciary Relationships**

Issuance of a certificate does not make the dataedge CA an agent, fiduciary, trustee or other representative of a Subscriber or any other party.

#### **9.2.3 Insurance coverage**

No Stipulation

#### **9.2.4 Other assets**

No Stipulation

#### **9.2.5 Insurance or warranty coverage for end-entities**

No Stipulation

### **9.3 Confidentiality of business information**

#### **9.3.1 Scope of confidential information**

dataedge CA Internal policies and marketing plans for CA services are confidential.

#### **9.3.2 Information not within the scope of confidential information**

Information published on the dataedge CA website, in this CPS are available to public access

#### **9.3.3 Responsibility to protect confidential information**

Any confidential information provided to the Subscriber, relying party or third parties are to be protected by the respective entities.

## **9.4 Privacy of personal information**

dataedge CA has implemented best in class measures to protect private information and would not share any such information with any third party other than authorities on request.

### **9.4.1 Privacy plan**

Documents and other media containing private information are protected by dataedge security policy guidelines are accessed only on a need to know basis.

### **9.4.2 Information treated as private**

Information contained in the certificate is not treated as private. Information collected from subscribers and relying parties under a confidentiality agreement are treated as private.

### **9.4.3 Information not deemed private**

Information available in the public domain is deemed not private.

### **9.4.4 Responsibility to protect private information**

The receiver of private information is responsible to protect private information.

### **9.4.5 Notice and consent to use private information**

Any use of private information by the dataedge CA would be made only with the express consent of the party.

### **9.4.6 Disclosure pursuant to judicial or administrative process**

dataedge reserves the right to divulge private information pursuant to administrative or judicial process to interested parties without obtaining specific consent.

### **9.4.7 Other information disclosure circumstances**

Subscriber, relying party information may be disclosed to authorities as per applicable laws of Bangladesh.

## **9.5 Intellectual property rights**

No Specific Stipulations

## **9.6 Representations and warranties**

All responsibilities, including liabilities associated with any certificate under any class or any sub CA under any class of any dataedge CA hierarchy ultimately rests with dataedge CA

The warranties, disclaimers of warranty, and limitations of liability among dataedge CA, Resellers, and their respective Customers within dataedge CA's Sub-domain are set forth and governed by the agreements among them. This CPS relates only to the warranties that certain technical & sub CAs (dataedge CA, and PKI Customers) must make to end-user Subscribers receiving Certificates from

them and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties. .

dataedge CA uses, and (where required) Resellers shall use, Subscriber Agreements and Relying Party Agreements in accordance with CPS and PKI Customers have the option of using a Subscriber Agreement. These Subscriber Agreements shall meet the requirements imposed by dataedge CA (in the case of Resellers). Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to those PKI Customers, and Resellers that use Subscriber Agreements. dataedge CA adheres to such requirements in its Subscriber Agreements. dataedge CA's practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to dataedge CA. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

### 9.6.1 CA representations and warranties

dataedge CA's Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,  
There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,  
Their Certificates meet all material requirements of this CPS, and  
Revocation services and use of a repository conform to this CPS in all material aspects.

dataedge CA's Relying Party Agreements contain a warranty to Relying Parties who reasonably rely on a Certificate that:

All information in or incorporated by reference in such Certificate, except Non-verified Subscriber Information, is accurate,  
In the case of Certificates appearing in the dataedge CA repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CPS, and  
The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate.

### 9.6.2 RA representations and warranties

The warranties, disclaimers of warranty, and limitations of liability between an RA and the sub CA or technical CA it is assisting to issue Certificates or the applicable Reseller, are set forth and governed by the agreements between them.

### 9.6.3 Subscriber representations and warranties

dataedge CA's Subscriber Agreements require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,

- No unauthorized person has ever had access to the Subscriber’s private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a sub CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a sub CA or otherwise.

**9.6.4 Relying party representations and warranties**

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CPS

**9.6.5 Representations and warranties of other participants**

No warranty is extended by dataedge CA to other parties other than specifically mentioned in this CPS.

**9.7 Disclaimers of warranties**

To the extent permitted by applicable law, dataedge CA’s Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, dataedge CA’s possible warranties, including any warranty of merchantability or fitness for a particular purpose.

**9.8 Limitations of liability**

The issue of Certificates by dataedge CA are based on verifications done on best practices adopted and on best endeavour basis and it is inherent that neither dataedge CA nor any technical CA or sub CA or RA performing activities under this CPS can underwrite the conduct or activities of the subscribers or otherwise assure the bonafide of the actions. dataedge CA, the technical CA, sub CA and RA do not accept any liability to the Relying Party on this account. Further even in other eventualities to the extent permitted by applicable law, dataedge CA’s Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements shall limit, dataedge CA’s liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following liability caps limiting dataedge CA’s damages concerning a specific Certificate:

<i>Class</i>	<i>Liability Caps</i>
<b>dataedge CA Bangladesh Root CA Public Hierarchy:</b>	
Class 1	NIL BDT
Class 2	2000 BDT
Class 3	3000 BDT

Table - Liability Caps



## **9.9 Indemnities**

dataedge CA or RA does not make declare any warranties on the financial transactions which the Subscribers and the relying parties perform. Responsibilities will fall upon to the subscriber and relying parties for any losses or damages or any other consequences.

## **9.10 Term and termination**

Not Applicable

### **9.10.1 Term**

Not Applicable

### **9.10.2 Termination**

Not Applicable

### **9.10.3 Effect of termination and survival**

Not Applicable

## **9.11 Individual notices and communications with participants**

No specific stipulations

## **9.12 Amendments**

### **9.12.1 Specification Change Procedures**

Amendments to this CPS shall be made by dataedge CA and approved by Controller of Certifying Authorities, Bangladesh. The amendments shall either be in whole CPS document form or an update. Amended versions or updates shall be linked to the dataedge CA Repository located at: dataedge CA Website. Updates always supersede any designated or conflicting provisions of the referenced version of the CPS.

### **9.12.2 Items that Can Change Without Notification**

dataedge CA reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. dataedge CA's decision to designate amendments as material or non-material shall be within dataedge CA's sole discretion.

### **9.12.3 Items that Can Change with Notification**

dataedge CA shall be entitled to make at its absolute discretion material amendments to the CPS in accordance with this CPS

### 9.12.3.1 List of Items

Material amendments are those changes that dataedge CA, under CPS # 8.1.1, considers being material.

### 9.12.4 Notification Mechanism

dataedge CA's operations team will post proposed amendments to the CPS in the dataedge CA Website.

Notwithstanding anything in the CPS to the contrary, if dataedge CA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the dataedge CA, dataedge CA shall be entitled to make such amendments by publication in the dataedge CA Repository. Such amendments will be effective immediately upon publication.

### 9.12.5 Comment Period

Except as noted under CPS # 8.1.2.2, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the dataedge CA Repository.

#### 9.12.5.1 Mechanism to Handle Comments

dataedge CA's Management and Operations group will consider any comments on the proposed amendments. dataedge CA will either

- a) allow the proposed amendments to become effective without any changes,
- b) make changes to the proposed amendments and republish them as a new amendment under CPS # 8.1.2.2, or
- c) withdraw the proposed amendments.

dataedge CA is entitled to withdraw proposed amendments by providing notice in the dataedge CA Website. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under CPS # 8.1.2.3.

### 9.12.6 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer

See CP

Note: dataedge CP will need to draft based upon the Bangladesh CP.

### 9.12.7 Procedure for amendment

No Specific Stipulation

### 9.12.8 Notification mechanism and period

No Specific stipulation

### 9.12.9 Circumstances under which OID must be changed

Controller of Certifying Authorities, Bangladesh in consultation with the CA can mandate changes to OID.

## **9.13 Dispute resolution provisions**

### **9.13.1 Disputes among dataedge CA and Customers**

Disputes between dataedge CA and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between the parties.

### **9.13.2 Disputes with End-User Subscribers or Relying Parties**

To the extent permitted by applicable law, dataedge CA's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, a dispute resolution clause.

### **9.13.3 Role of the Controller of Certifying Authorities**

Under the Bangladesh ICT Act, the Controller of Certifying Authorities (CCA) is also authorized to resolve disputes arising out of CA services. His role is described in detail in the ICT Act and its associated rules and regulations.

## **9.14 Governing law**

Subject to any limits appearing in applicable law, the laws of Bangladesh shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all participants within dataedge CA's domain of services, no matter where they are located.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

## **9.15 Compliance with applicable law**

Applicable law in Bangladesh is the ICT Act, Bangladesh

## **9.16 Miscellaneous provisions**

### **9.16.1 Force Majeure**

To the extent permitted by applicable law, dataedge CA's Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements shall include, a force majeure clause protecting dataedge.

### **9.16.2 Entire agreement**

Agreements between dataedge CA and the subscriber, relying parties and other entities supersede anything contained in this document.

### **9.16.3 Assignment**

No specific stipulation

#### **9.16.4 Severability**

To the extent permitted by applicable law, dataedge CA's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

#### **9.16.5 Enforcement (attorneys' fees and waiver of rights)**

dataedge CA shall not bear.

#### **9.17 Other provisions**

No specific Stipulations

## Conclusion:

As there was an opportunity to serve dataedgeid in many ways, I have gathered a lot of experiences throughout the internship program in this company. There was a scope of observe the RA, CA, VA servers very closely. Not only observe but run some operations on these servers. And most important thing was I've learnt about the network architecture of these systems. As I worked on a project named 'Digital Signature Certificate Distribution and Training Program along with Cryptographic Token' run by Ministry of Posts, Telecommunications and Information Technology, Information & Communication Technology Division it teaches me a lot about the whole process of PKI.