Ethiopian PKI Site Preparation Guideline

Draft Version 1.0

INFORMATION NETWORK SECURITY AGENCY

2012 E.C.

Document Control

Document Name	Ethiopian PKI Site Preparation Guideline
Status	Draft
Version	0.1
Last Update	New Release
Document Owner	INSA

Table of Contents

1. Introduction

1.1. Executive Summary

The Electronic Signature Proclamation no.1072/2018 states that Information Network Security Agency (INSA) is the National RCA of the Ethiopian Public Key Infrastructure (PKI). The Ethiopian PKI has a hierarchical structure, INSA as a trust anchor of the hierarchy.

INSA as a root CA has a self-signed root certificate that issues Public Key Certificates to the CA while licensed certificate providers in turn issue Digital Certificates to end-users.

This guideline will enable the cryptographic operation site design to be considered early in the building development process, contributing to the architectural considerations, by providing information that cuts across the multidisciplinary design efforts; promoting cooperation in the design and construction phases. Adequate planning during building construction or renovation is significantly less expensive and less disruptive than after the facility is operational.

The guideline specifies a generic physical security tiers, site location, electromechanical and environmental monitoring capabilities, building management system and broad specifications of the requirements.

1.2. Purpose

The purpose of this framework is to provide site specification requirements and guidelines for the design and installation of a certifying cryptographic operation site. It is intended for use by the CA who need a comprehensive understanding of site specification guidelines including the facility planning, site and building selection and decoration.

1.3. Scope

The scope of this site preparation and selection guideline is to provide site selection, preparation, site security, construction of cryptographic operation center and electromechanical guidelines for CA.

1.4. Normative References

This section defines standards that shall be followed by all CA for carrying out their functions. Every CA shall observe the following standards for carrying out different activities associated with its functions.

Electronic Signature Proclamation No. 1072/2018.

ANSI/TIA/EIA-569-B: Commercial Building Standard for Telecommunications Pathways and Spaces

ANSI/TIA-942 Standard: Standard serves as a baseline to design and build a reliable and efficient data center.

Ethiopian X.509 Federal Republic of Ethiopia, Ethiopian X.509 Certificate Policy

NFPA 72: National Fire Alarm and Signaling Code, provides the latest safety provisions to meet society's changing fire detection, signaling, and emergency communications demands.

Ethiopian Standard ES-EBCS 11 Code of practice for mechanical ventilation and air conditioning in building

EN 50600: European standards and equivalent of ISO, Information technology - Data center facilities and infrastructures.

1.5. Informative References

This reference defines standards that are more detailed technical documents and are meant to provide CAs with a starting point for implementing practices to execute their functions. It is helpful if the CAs observe the following standards for carrying out different activities associated with their functions.

RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

WebTrust for Certification Authorities - Web trust principles and criteria for certificate authorities

ES ISO – 7240: Fire Detection and Alarming System Ethiopian Standards identical with ISO 7240

ANSI/TIA-942- Telecommunications Infrastructure Standard for Data Centers

1.6. Terms and Definition

Security levels: physical access levels that takes in to the main cryptographic operation center

Cryptographic operation center/site It is the site that cryptographic operation and general key management lifecycle takes place.

2. Security Level

The certificate authority facility separated with 5 tire or zones in order segregate duty of each tire assigned and implement the maximum security every access points. Each tire has its own roll, functionality, equipment, sensor, access control etc. The more we close to the cryptography generation room or cryptography ceremony room the more it becomes secured and required to strong authentication and authorization.

The entry to the cryptographic operation site that involves generation and storage of cryptographic keys need to be accessed based on the security clearance of staff and entry is through a proximity access control system and the cabinet need to be locked. Physical access to this tier is automatically logged and management must be notified ahead.

2.1. Tier 1

The external zone of the CA building and lies outside of the premises. Entry to the CA facility site is after the entrance gate entry that employees use and verified by security officers.

The facility can be secured by:

- Armored door
- Surveillance camera monitoring the entrance
- Access card reader used to allow only authorized people to get in

2.2. Tier 2

Entry to the Site in the vicinity is after entry to along register for visitors and proper physical verification by the security guard at the reception room. The guards monitor the screen inside and outside of the CA facility.

The following technology is required in this tier

- Surveillance camera

- Camera monitoring and recording
- Fire and smoker detector
- Manual fire distinguisher

2.3. Tier 3

The entry to the working area is through a proximity access control system imposing the second tier of security. Physical access to tier three is automatically logged.

In this tier the following security facility is required in order to make the CA more secure

- Armored door
- Surveillance camera
- Biometrics access card used to allow only the authorized people to get in
- Raised floor
- Air conditioning system
- Stand by backup for air conditioning system
- Fire and smoker detector
- Automatic fire fighting system FM200 using harmless gas
- Safe for storing backup taps

2.4. Tier 4

The main room where cryptographic operation takes place should be constructed as per the details specified in Section 9.

This security barrier enforces individual access control through the use of two factor authentication including biometrics unescorted personnel, including untrusted employees or visitors, are not allowed in to a tier-four secured area. Physical access to tier four should be automatically logged and access to different rooms of the site is limited as per the security clearance of staff members and visitors.

This room include the offline root CA. This root CA kept offline and will be only turned on while generating new CA.

The following facility should incorporate on this tier

- Armored door to separate from tier 3

- Contact sensor are turned on if any an authorized person try to breach the get
- Surveillance camera
- Biometrics access card used to allow only the authorized people to get in. For gaining access this tier two authorized person should sign in.
- Motion detector sensor for monitoring the activity when no one is inside
- Fire and smoker detector

2.5. Tier 5

The entry to the cryptographic operation site that involves generation and storage need to be accessed based on the security clearance of staff and entry is through a proximity access control system and the cabinet need to be locked. Physical access to this tier is automatically logged and management must be notified ahead.

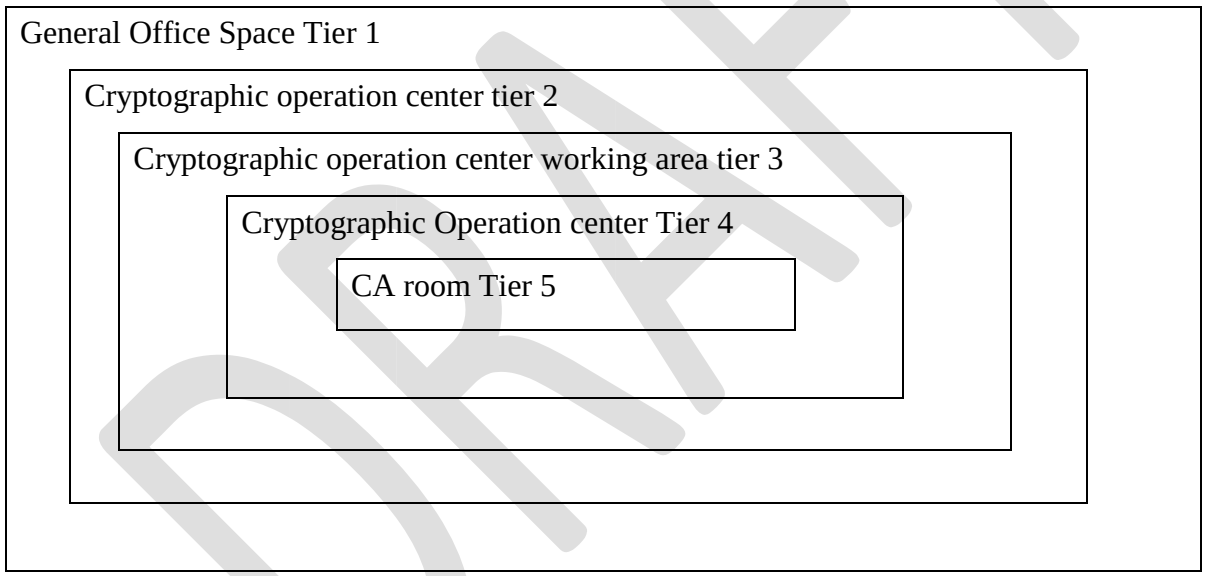

Figure 2-1 Site of Cryptographic Operation Centre

Besides the aforementioned tiers, additional ones can be added.

3. Construction of Cryptographic Operation Site

The Site selection and construction of PKI facility is very critical and we should be curious and consider a number of factors that include infrastructure requirements, climate control, the equipment's required by the facility, the fire protection systems and most importantly purpose of the facility.

The site should be protected from:

- break-ins
- natural disasters
- fires
- Failure of supporting telecommunications
- Failure power utilities
- Structural collapse
- Chemical contamination
- Explosions
- Water intrusion through floods or plumbing leaks.
- The facility should not be located in/near areas with high risk of flooding such as: basement, immediately below roof top, immediately below kitchen or canteen or chiller plant, below a building's water tank, adjacent to or near the toilets and pantry, near the staircases, building drains or pump room, on a floor surrounded by open platform or in open area.
- The building should have a sufficiently large loading dock, freight elevator, and pathway to handle all anticipated deliveries of supplies and equipment as per ANSI/TIA-569-B. Loading docks should not open directly into the cryptographic operation center and a staging area for all equipment should be provided that is not part of the main computer room.
- The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CA systems, shall be consistent with facilities used to house high value, sensitive information as per ANSI/TIA-942 Standard.

- The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the equipment's and records of CAs.
- The CA facility can have double or triple layer, floor-to-ceiling walls located in an area without windows or where windows can be secured effectively.
- External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. To add further security the certification room can be made of steel or metal or tamper proof closed steel cage of sufficient thickness.
- In the case of a cage, the system should be rack mounted and rack should be lockable. The cage should provide enough space for trusted persons to securely carry out operations on rack mounted CA systems and should be lockable from inside and outside.
- The construction must provide protection against the risks of cryptographic key loss, theft, and abuse. The cryptographic operation room should be located away from sources of EMI, RFI and X-Ray equipment, radio transmitters and Transformers.
- All the ducts like electrical, Air-conditioning and LAN should be built of noncombustible and dust-free materials, and should not, at any point provides physical access to the site from outside.

3.1. Raised Floor (Access Floor)

An access floor is actually a floor raised above a floor. Its purpose is to create a controlled area for wire management and air circulation.

Access floor could be:

- High in mechanical property
- Wear resistant
- Corrosion resistant
- Good in antistatic
- Pollution resistant
- Convenient for cleaning

Moisture below the floor can damage wiring or equipment and cause costly downtime. A sub-floor water detection system can provide immediate warning. Alarming can be provide via various audible, visual, in-band and out of band methods.

The construction of an access floor is comprised of square thick panel, of varies materials, and providing different weigh loading characteristics. The floor panels can be rearranged at any time to suit for the PKI facility needs.

3.2. Physical Access

The CA equipment including remote workstations used to administer the CA systems, shall always be protected from unauthorized access.

The security mechanisms shall be commensurate with the level of threat in the equipment environment.

All Personnel are required to wear visible identification.

Physical access to CA facility and equipment is limited to authorized individuals, protected through restricted security perimeters and is operated under multiple person (at least dual custody) control.

Regarding the access to the CA facility, there should only be one main entrance. All the side entrances for emergency exits must be permanently locked and it should be through:

Table 3-1Tier Access Control

Tier	Access Control	Remarks
1	Building security check	The security officers check individuals as normal physical security access
2	Log Register +Security	All individual shall sign in and sign out
3	Physical Keys Access Control Cards(	Steel Doors Open with keys
	Smart card, contactless key or cipher lock or combination)	And/or access card.

4	Physical Keys + Access Control Cards (Smart card key or, contactless cards cipher lock or a combination) + Biometric Control	Steel Doors Open with keys and/ or access control card Biometrics.
5	Physical Keys + Access Control Cards (Smart card, PIN code, contactless card key or cipher lock or a combination) + Biometric Control+ electronic locking systems for server cabinets	A simple mechanical locks to fully intelligent locking hardware and offer intelligently managed access to cabinets with same access cards and biometrics

3.3. Power and Air Conditioning System

3.3.1. Power

The CA facility must be equipped with an Uninterruptible Power Supply (UPS) and generator with proper backup depending upon the nature of operation. The power utility should be able to provide adequate power to supply to initial and future power requirements.

The power points such as socket outlets or securing outlets must be correctly installed. In order to avoid static charge from building up, the ground wire must be insulated and connected to the building's ground strap while all computer equipment should have a dedicated ground point. Data cables should not be laid adjacent to main electrical cables or system control cables. Emergency lighting should be installed to assist exit of personnel during power failure.

In addition, repositories (containing issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of one (1) hour operation in the absence of commercial power.

3.3.2. Air Conditioning System

The CA facility should have air-conditioning system and fresh air supply system. All air ducts, including insulation/lining, should be built of non-combustible and dust-free materials and should not have any ducts that could allow physical access to the certification facility.

The design of the air-conditioning system must take into consideration:

- Capacity requirement of all equipment's;
- Future capacity requirements;

- Normal maintenance;
- Mode of operation;
- Temperature, humidity and dust count level control;
- Load density;
- Sensible heat ratio;
- Outside air quantity;
- Amount of air circulated;
- Air distribution method;
- Vapor barrier for humidity control;
- Flexibility and ease of expansion;

The air-conditioning system should be usually designed to maintain the following:

  - Temperature around 22 degree centigrade
  - Humidity around 50 %

A relative humidity of less than 40% for sufficiently long period will induce static electricity problem.

3.4. Water Exposure

- Cryptographic operation Systems should be protected from water exposures.
- CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).
- The facility should install a moisture detector.

3.5. Fire Prevention and Protection

The wall enclosing the computer room should be constructed of non-combustible material which should be fire resistant for at least few hours. The fittings and furniture inside the computer room should also be made of non-combustible materials or materials having minimal fire propagation property.

The following points should be kept in view while planning the systems:

- Detectors should not be inserted into the ceiling but rather surface- mounted under the ceiling.

- Detectors should not be placed near air stream outlets or any sources, which would affect the integrity or functions of the detectors.
- The central fire alarm system of the building should be relayed to the computer room so that operation staff in the computer room are alerted if there is a fire in the building.
- Smoking inside CA facility should be prohibited.

The CA facility shall be equipped with heat and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment.

Fires can occur within the digital equipment, wires, cables, HVAC equipment, raised floors, suspended ceilings and other combustibles found in CA facility. These fire risks lead CA facility to address fire protection at three different levels – building level, room level and a rack-level (in-cabinet).

3.5.1. Building Level Fire Protection

The first level of fire protection is at the building level. The main goal is to protect the building and employees from fire. The type of fire protection most commonly used is fire sprinklers and handheld extinguishers. A building can also use passive fire protection, which is the installation of fireproof and fire-rated floor assemblies that considerably delay the spread of fire into other areas of the building.

3.5.2. Room Level Fire Protection

Fire Brigade or any other agencies of the Central or State Government that will set standard of room level protection of fire of CA Facility.

The two common clean agent gas systems are Novec 1230 and FM-200. They suppress the fire by reducing the heat of the fire through absorption. These gases have zero ozone depletion, which makes them safe for the environment and around humans. The physical footprint is smaller than inert gas systems because they don’t require as much agent to fill up an entire room. Clean agent gases are electrically non-conductive, non-corrosive and leave no residue upon evaporation. This makes them the ideal fire suppression agents in CA facility. Like fire sprinklers, these systems have a piping system installed throughout the room. The system activates through smoke and heat detection and the clean agent gas disperses evenly throughout the room through nozzles.

3.5.3. Rack Level Fire Protection

The last level of data center fire protection is at the rack level. This fire protection is essential to protecting specific equipment and limiting damage. The mandatory fire sprinklers will protect the building and the room from fire, but the equipment, valued higher percentages of the cost in the room, is not unprotected. This creates a need to protect the equipment from a fire at the rack level to save the investment. Installing a pre-engineered automatic fire suppression system will protect the equipment by detecting the fire within seconds and suppress it before the total flood or sprinkler system activates. This prevents equipment damage caused by a water based sprinkler and avoids the discharge of large amounts of agent in a total flood cylinder which is expensive to refill.

The pre-engineered system routes fire detection tubing through the individual racks and connects the tubing to a cylinder with clean agent. When a fire starts, the detection tubing senses the fire and activates the systems to suppress the fire in the specific rack. The systems use clean agent which protects the equipment from further damage and minimizes downtime in the data center. Reducing downtime is a key factor for each data center tier level to maintain their uptime.

3.6. Media Storage

- Storage media should be protected from environmental threats such as extreme temperatures, humidity, and magnetism.
- All media must be stored in a safe and secure environment in accordance with manufacturer specification.
- Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.
- Media that contains security audit, archive, or backup information shall be stored in a location separate from the CA equipment.

3.7. Environmental Protection

- CA facility and equipment should be protected from environmental hazards.
- Water, temperature and humidity detectors must be installed and shall be connected to audible alarms.

3.8. Waste Disposal

- Information on media used for storage of keys etc. shall be deleted securely or destroyed before released for disposal.
- Equipment containing storage media (i.e., fixed hard disks) should be checked to determine whether they contain any sensitive data prior to disposal or reuse.
- Storage devices containing sensitive information should be physically destroyed.
- Authorization is required for all media removed the organization and record of such removal to maintain an audit trail should be kept.

3.9. Automatic Status Monitoring

The site must be equipped to monitor and alert relevant personnel in the event of an abnormality in security operations, including physical security etc.

3.10. Video and Other Surveillance Equipment

A Video Surveillance System (VSS) with storage should be installed to properly monitor the entire premises on a 24/7 basis through a suitably installed set of cameras. It should operate in a failsafe mode. The system should possess the ability to reconstruct the events that occurred during the breach of security.

3.11. Off-Site Backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the CP. Backups shall be performed and stored offsite not less than once per week or when the CA is operational, whichever is less frequent. At least one backup copy shall be stored at an offsite location (separate from the LCA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational LCA system.

3.12. Disaster recovery site

Disaster recovery is an important aspect of service providers for providing uninterrupted services to its clients and end users. With a robust DR/BCP program in-place, various service provision outcomes can be achieved. Some of them are: improved service operations, improved performance, agility and availability, reduced disruptions and loss to business, and higher customer satisfaction.

For a DR strategy to work as per design, one of the important contributors is DR site as it will define service availability to customers during disasters. The following factors and approaches should be considered when DR site is selected.

- **Data Center Tier –** Datacenter tiers as per ANSI/TIA-942 Standard are divided across Tier 1 (basic datacenter with availability of 99.67%), Tier 2 (redundant infrastructure components with availability of 99.74%), Tier 3 (has all attributes of tier1 and 2 and in addition has multiple distribution paths, dual powered etc. with availability of 99.98%) and Tier 4 (has all capabilities of prior tiers with completely redundant and highly available infrastructure and availability of 99.995%). Based on the requirement of various applications and availability, DR site tiers have to be decided.
- **Distance from Primary Data Center –** Another factor which will help us determine site for DR is the distance between primary and DR site. This is crucial since it will affect latency and performance of applications. As an illustration, if DR data center is housed at a larger distance, client will not be able to mirror data in real time in an effective manner. This will cause a risk that data will be lost if we need to switch to DR site in event of a disaster. . On other hand, if distance is too small, data backup will be efficient but it will pose other environmental threats.

- **Seismic Zone Details –** Seismic zone is a region where seismic activity remains fairly constant. Each nation has divided entire area in various zones and the data is readily available in public domain. From DR site selection perspective, Primary and DR sites should be preferably in different seismic zones as it will help to curb issues arising from various seismic activities.
- **Environment Details –** Next factor to consider is environment details of the area, these could be weather details, environmental hazards etc. This will help to plan out

various things like resource availability, environmental cleaning mechanisms (if required), site construction and maintenance etc.

- **Third party services availability –** For any datacenter site, we require to interact with a number of third parties and service providers like utilities, telecom etc. This will become more critical in case of a DR site, as the site is not up and running for 100% of the time. Two important considerations are Availability of service (whether service is available 24/7 for 365 days or for some limited period) and SLAs (what are the SLAs for the services provided by third parties? This is critical parameter as based on this, company will confirm on the SLAs with business and its customers).
- **Accessibility of Data Center –** Next factor will be accessibility to DR site. This will become crucial in case disaster occurs and we need to switch operations to DR site. If the site is accessible, operations can be resumed faster. This will focus on Modes of transportation to reach DR site, Proximity to airport etc.
- **Capacity Available for Further Expansion –** Capacity and scalability of DR site has to be looked into considering future growth plans.
- **Network Latency –** For DR strategy to work as per requirement, data has to be copied from primary datacenter to DR. Network latency plays a major role in this and becomes a crucial factor while deciding for DR site.
- **Cost Implications –** Last but not the least is cost implications of building a DR site at a particular location. This involves both CAPEX and OPEX.
- DR Site Selection Approach involves requirement gathering, assessment, decision/report of the DR site based on the above factors.

4. Broad Specifications of system to be installed

Broad specification for the following cryptographic operation site preparation requirements is provided in this section;

- Multifactor access Control System o Access Control System
  - Biometric System
  - Electronic Burglar Alarm System
- Fire Detection, Alarming and Suppression System
- Data Safe
- Video Surveillance System (VSS)

4.1. Access Control System

Access control limits access to specific area of buildings, which house of network routers, firewalls, servers, offices, terminals, and a host of other devices and data that must be protected.

These are the minimum system specifications that required to be installed the access control systems in the CA facility:

- Micro computer based system
- Versatile – capable of interfacing with capable of interfacing with different types of readers as PIN code, biometric, barcode, proximity, contactless smart card etc.
- LCD/LED Display
- Feather touch keypad.
- Date, time day and reader status display
- Audio visual indications
- Reader controller and reader interface module enclosure having its power supply and battery charging and backup battery. Battery backup for a minimum of 24 hours in case of power failure.
- Memory storage capacity.
- Programmable time zoning capability.
- Multilevel password access for programming
- Modem connection option for downloading data from remote locations.
- PC connectivity

- Potential free relay for interfacing with electromagnetic locks.
- Door sensors indicates if the door is left open
- PIN (Personal Identification Number)
- User friendly software

4.2. Biometric System

It's part of access control system refers to the science of establishing individuals' identities based on their physical and behavioral traits such as fingerprints, face, iris, voice, and gait.

These are the minimum system specification that required to be installed in the CA facility:-

- LED / LCD Display of RTC, (date & time)
- LED / LCD display of verify passed or failed.
- Audio and display for pass / fail.
- Alarm /buzzer user programmable.
- Multi- port Option and interface for card reader.
- finger prints templates storage capacity
- Data log/records storage capacity.
- User friendly software
- Allow finger displacement to menus with fingerprint and/ or password or both.
- At least three levels users/security/access on the units.
- ON-LINE monitoring of logged data
- Support for multi user and multi user group environment in addition to user hierarchy
- Secured recording for evidence purposes and user authentication to protect data integrity.

4.3. Electric Burglar Alarm System

A system designed to detect intrusion – unauthorized entry – into a building or area. They are also called security alarms, security systems, alarm systems, intrusion detection systems, perimeter detection systems, and similar terms.

The system specification that required to be installed the Electric Burglar systems in the CA facility:

- Motion Sensor should enable detection of vibrations resulting from break-ins through the walls, (for e.g. hammering, chiseling, etc.)
- Vibration Sensors (Passive infra-red movement sensor- It detects the changes in the IR energy level of the surroundings, setting the alarm.).
- Audio/Visual Alarm indicators.

4.4. Fire Detection, Alarming and Suppression System

Fire detection systems are designed to discover fires early in their development when time will still be available for the safe evacuation of occupants and plays a significant role in protecting the safety of emergency response personnel.

The system should include:

- Automatic fire detection and alarm system including heat sensors, smoke sensors and audio alarms, preferably connected to the central alarm system of the building.
- Should have a battery-powered backup for sufficiently long time.
- Fire extinguishers should be as specified by the Government Rules or Fire Brigade. These fire extinguishers should be able to extinguish A, B, C category of fires.
- Routine and frequent inspection of the all fire detection system

4.5. Data Safe

Data safe are the mechanisms that shall be placed to protect the data.

The safe be protected against.

- Fire
- Magnetic fields
- Dust
- Unauthorized access
- Pilferage
- Accidental or malicious damage
- Humidity

- Electrostatics

4.6. Video Surveillance System (VSS)

For starters, cameras installed around the perimeter of CA facilities should be used to watch for any suspicious activity in and around the CA facility. Here are the recommended features the VSS system:

- Live Streaming Video In Real-time.
- Software should incorporate a friendly graphical user interface for control functions, operation indicators, and multiplexed video display of cameras connected to the VSS System.
- Scheduled or continuous video recording that is activated by motion detection for all or selected cameras.
- All images are time and date stamped.
- Multiple camera switching methods for the required number of cameras.
- Selectable camera zone coverage with motion detection
- Sensitivity controls for motion detection recording
- Alarm system compatibility for external sensor inputs Time & date stamping on video playback and video backup
- Sufficiently High screen resolution
- Image Searching
- Time based recording
- Motion Detection
- System Security

5. Acronyms

ANSI	American National Standards Institute
BCP	Business continuity plan
CA	Certificate Authority
CAPEX	Capital expenditure
CRLs	Certificate Revocation List
DR	Disaster recovery
DVR	Digital video recorder
EMI	Electromagnetic interference
HVAC	Heating ventilating and air conditioning
LAN	Local Area Network
LCP	Licensed certificate provider
OPEX	Operational expenditure
PKI	Public Key Infrastructure
RCA	Root Certificate Authority
RFI	Radio Frequency interference
SLA	Service level Agreements
TIA	Telecommunication Industry Association
UPS	Uninterruptable Power System