CA SITE SPECIFICATION

Version 2.0

March 2017

Controller of Certifying Authorities

Ministry of Communications and Information Technology

Document Control

Document Name	CA Site specification
Status	Release
Version	2.0
Last update	20 Mar 2017
Document Owner	Controller of Certifying Authorities, India

CA SITE SPECIFICATION

1. Security Levels : The CA facility must be protected by at least three tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

- Tier 1 – Entry to the Site in the vicinity is after entry to a log register for visitors and proper physical verification by the security guard at the entrance.

- Tier 2 – 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.

- Tier 3 – The main room where cryptographic operation takes place should be constructed as per the details given in the para 2. Activities related to the lifecycle of the certification process such as authentication, verification, and issuance takes place in this area. 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 into a tier-three secured area. Physical access to tier three is automatically logged.

In addition to the aforesaid tiers, additional tiers can be added.

2. Construction of Cryptographic Operation Site:

- Site should be protected from break-ins, natural disasters, fires, failure of supporting telecommunications or 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.
- Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. The Construction must be tamper-evident. Materials used for construction

shall be fire resistant and free of toxic chemicals. The facility shall monitor any physical break-in attempts such as hammering, exploding, chiseling etc.

- 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 evident 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.

- All the ducts electrical, Air-conditioning, LAN should be built of non-combustible and dust-free materials, and should not, at any point provides physical access to the site from outside.

- **Power and Air Conditioning System:** The CA facility must be equipped with an uninterruptible power supply (UPS) and generator with proper backup depending upon the nature of operation. All electrical installations must meet the standards specified by the central/state government. 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.

  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 equipments;
- 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 is 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.

- **Physical Access**:

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. It should be through

Tier	Access Control	Remarks
1	Log Register +Security Guard	All individual shall sign in and sign out.
2	Physical Keys Access Control Cards(Magnetic card key or cipher lock or combination)	Steel Doors Open with keys and/or access card.
3	Physical Keys + Access Control Cards (Magnetic card key or cipher lock or a	Steel Doors Open with keys and/ or access control card.

	combination) + Biometric Control	

- **Water Exposure**: Systems should be protected from water exposure

- **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 CA facility shall be equipped with heat and smoke detectors, alarms, and a fire suppression system appropriate for computer equipments. It should be in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government.

  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.

- **Media Storage**: Storage media should be protected from environmental threats such as extreme temperatures, humidity, and magnetism.

- **Environmental Protection**: Water, temperature and humidity detectors must be installed and shall be connected to audible alarms.

- **Waste Disposal**: Information on media used for storage of keys etc. shall be deleted securely or destroyed before released for disposal.

- **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.

- **Video and other surveillance equipment**: A Digital Video Recorder System (DVR) should be installed to properly monitor the entire premises on a 24 x 7 basis through a suitably installed set of cameras. It should operate in a fail safe mode. The system should posses the ability to reconstruct the events what occurred during the breach of security.

3. Broad Specifications of Systems to be installed

Broad specifications of the following systems are given below:

- Access Control System
- Biometric System
- Electronic Burglar Alarm System
- Fire Detection System
- Data Safe
- Surveillance System (DVR System)

3.1 Access Control System

- Micro computer based system
- Versatile – capable of interfacing with different types of readers such as bar code, proximity etc.
- LCD/LED Display
- Feather touch keypad.
- Date, time day and reader status display
- Audio visual indications
- In-built battery backup for minimum of 24 hours, in case of power failure of regular operation, even with electromagnetic lock.
- 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.

3.2 Biometric System

- 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 when connected to PC.
- Exhaustive MIS report.

3.3 Electronic Burglar Alarm System

- 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.

3.4 Fire Detection System

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.

3.5 Data Safe

The safe be protected against.

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

3.6 Surveillance System (DVR 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 DVR 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

****