Undertaking to be signed by State Key Management AuthorityNodal Officer on behalf of Respective State Governments.

Date: _____

I_____, working in Government of _____, in the capacity of_____, and also as State Key Management Authority (SKMA) Nodal Officer, hereby undertake on behalf of Government of_____to understand and implement the security processes as written in the following sections and enclosed annexure(I to V) . I am fully aware with the Technology Risk factors and Technology Presumptions as mentioned in Annexure V, in implementing the Symmetric Key Infrastructure for Driving License and Vehicle Registration Certificate applications in the State of_____.I hereby undertake to implement the Key Management Software, only as provided by Central Key Generation Authority on behalf of Ministry of Road Transport and Highways, Government of India, in the State of_____, where ever applicable. The duly signed SHA1 hash of these software are given in Annexure VI.

On and behalf of Government of_____

Name_____

Signature_____

Place_____

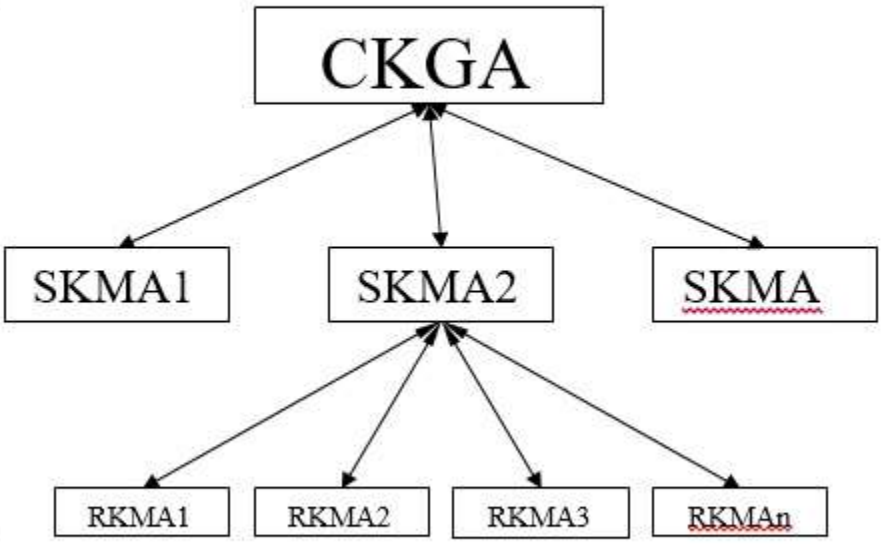
Date_____

In the presence of:

1.

2.

Annexure 1



Annexure II

Symmetric Key Infrastructure for Smart Card based Driving License and Vehicle RC Applications

(Author S.K.Sinha)

As an e-Governance initiative Ministry of Road Transport and Highways initiated the project of computerization of all the RTO's, and issuance of Smart Card based Driving License and Vehicle Registration Document. Ministry entrusted NIC to work as Technical Consultant for the complete project. In addition to development of Back-end process computerization software for RTO office, the Smart Card related front-end application development is a major part under

this project. This comprises following major activities related to Smart Card technology,

1. Smart Card Technology Standardization (SCOSTA).
2. Smart Card Data Format Design and Standardization.
3. Establishment of Symmetric Key Infrastructure.

The establishment of Symmetric Key Infrastructure (SKI) is the basic requirement for implementing Smart Card Security against fake duplication, illegal tempering of information and implementing the authority environment to carry out different functionalities on Driving License and Vehicle Card data. Software for implementing these requirements has been developed by NIC. The implementation of SKI requires, similar level of procedural and physical security as is the pre requisite for PKI based Digital Certification Authority (CA). Keeping this in view, Price Waterhouse Coopers (PwC), which are empanelled by Root CCA, Government of India, for performing Security audit for PKI based system, were hired to study and submit a document for SKI processes, physical security, Risk factors involved and their recommendations to mitigate them. The document submitted by PwC, deals in detail about Tiers of SKI implementation, Processes at various levels, Roles and responsibilities, Physical Security Infrastructure, Disaster Recovery, and Risk Factors. The report provides elaborated details under the following heads,

- Seed Key Management
- Master Key Management
- DL Keys Management
- Roles and Responsibilities
- General Security Risk Evaluation and Procedures
- Logical Access Controls
- Recommendations
- Risk Factors and General Assumptions

Below given is the summery in short about the SKI Framework and Key Management System.

1. Three Tier Structure of SKI
2. KMS Life Cycle
3. Seed Key Generation and Management
4. Disaster Recovery of Seed Cards
5. Generation of Authority Cards and Issuance
6. Issuance of DL and RC Cards at RTO
7. Risk Factors Involved

1. Three Tier Structure of SKI

The Symmetric Key Infrastructure will consist of three levels of operation for generation and Management of Keys and related Cards. These are,

i. Central Key Generation Authority

Central Key Generation Authority (CKGA), is the central level authority, which works as an overall custodian of the Key Management System across the country. CKGA is responsible for production of all kinds of authority cards and their distribution to respective SKMA's. CKGA maintains the mother keys required to produce different authority cards. CKGA maintains the database of all the authority cards issued to different States. CKGA processes are executed in a highest level of security as comparable to Digital Certification Authority Standards. CKGA

setup and key storage etc are highly sensitive and therefore adopt a well coded security methodology against compromise, sabotage or disaster etc.

ii. State Key Management Authority

State Key Management Authority (SKMA), which is the state custodian agency for Key Management System, will be basically responsible for distribution of authority cards among various Trusted Authorities within the state transport organization and law enforcement agencies. It will receive required authority cards on request from CKMA, personalize them and distribute it to various trusted authorities directly or through Regional / Sub Regional Key Authorities. Therefore distribution and management of authority cards is the major defined role of SKMA. Another important task that SKMA will perform is to recharge various Issuance Cards, which have exhausted their issuance limit. SKMA processes require a secure infrastructure for performing various KMS related operations.

iii. Regional Key Management Authority

Regional / Sub-Regional Key Authority (RKA) is the ultimate point of usage of various authority cards for issuance and other operations on DL/RC Cards. RKMA is the authority which is responsible for safe keeping and safe usage of various authority cards, *while they are in use*. Its responsibility is to ensure and see to it that all the defined security codes are strictly being followed at the field by various trusted authorities which are using authority cards for various functionality. RKA will also be responsible for originating the requirements of different type of authority cards on need basis. These requirements will be channeled to CKMA through SKMA.

2. KMS Process Cycle

Below given is the process flow and complete Process Cycle for KMS operations, after the Mother Keys are Generated and are in safe custody at NIC CA.

i. RKMA consolidates the requirements of various cards under his jurisdiction.
ii. Sends these requirements along with the details of trusted authorities, already earmarked for the purpose, to SKMA
iii. SKMA consolidates all such requirements for the State and forwards requirements to CKGA.
iv. CKGA after receiving request from SKGA gives a batch number to individual request.
v. CKGA processes the request by starting the process of production of required authority cards.
vi. CKGA produces the authority cards.
vii. CKGA dispatches the cards to SKMA nodal officer.
viii. SKMA nodal officer sends acknowledgement of receipt of cards along with card details and certifies the safe receipt of cards.
ix. SKMA personalizes each authority card from the information received from RKMA as mentioned in point number (ii) above in this section, and generates unique PIN/Password for individual card.
x. Personalized cards are dispatched to RKMA nodal officer.
xi. RKMA nodal officer receives the cards and acknowledges the receipt with certification to SKMA; also send the details of received cards.
xii. After getting satisfied from the acknowledgement, SKMA dispatches the PIN's.
xiii. RKMA receives the PIN's and acknowledges the safe receipt to SKMA.

RKMA stores the cards and the PIN's as per the coded procedure. Also if required so, issues to individual trusted authorities with due procedural formalities.

3. Seed Key Generation and Management

For SKI and KMS to be in place, Mother Seed Keys are required to be generated one time in the beginning of the System life. For all time to come, these Mother Seed Keys will be used to regenerate the Mother Keys for issuance of Authority Cards. There will be seven Mother Seed Key Cards (MSK Cards) containing Eight Mother Seed Keys. Any five of these Cards will be required at any point of time to generate the Mother Keys (Master Keys). The

seven MSK Cards will be distributed among four NIC and three MoRT&H, trusted agents. These MSK cards will be usable in conjunction with the CKGA Nodal Officer Key Card (CNOK). Software to perform these operations has been developed by NIC and audited by third party.

4. Disaster Recovery of Seed Cards

As MSK Cards are the root of nation wide KMS, there will be Disaster Recovery Backup sets of the MSK Cards, to be used in case of Damage, Disaster. These Disaster Recovery locations will be same as for NIC CA. One pre-constituted Incidence Response Team (IRT) will come in action in case of such urgency.

5. Generation of Authority Cards and Issuance

As explained in KMS Process Cycle above, all functionality authority cards containing required Master Key for the specific functionality will be generated at CKGA on the request of SKMA. Generation process will involve presence of any five trusted agents to use their MSK card at NIC CA, and the software developed by NIC for this functionality will generate required type and numbers of authority cards. Software to perform these operations has been developed by NIC and audited by third party.

6. Authority Cards

a. DL Authority Cards

i. Pair of Issuer Authority Cards (DLIA1 & DLIA2)
ii. Endorsement Authority Cards (DLEA)
iii. Endorsement Settlement (Judicial) Authority Cards(DLRA)

b. RC Authority Cards

i. Pair of Issuer Authority Cards(RCIA1 & RCIA2)
ii. Regional Permit Issuance Card (RPI)
iii. National/Inter-State Permit Issuance Card (NPI)
iv. Authorization Entry Card (AE)
v. Tax Data Update Card (RCTAX)
vi. Endorsement Authority Cards (RCEA)
vii. Endorsement Settlement Authority Cards(RCRA)
viii. Pollution Control Certificate Issuance Card(PUC)
ix. Insurance Information Update Card (INS)

x. Fitness Certificate Issuance Card (FIT)

7. Personalization and recharging of Authority cards at SKMA

All authority cards generated at CKGA, will be received by SKMA, who in turn will personalize these cards by earmarking the trusted agents details who will be responsible to use these card. The SKMA card will be issued by CKGA to each States for performing this functionality. Software to perform these operations has been developed by NIC and audited by third party

8. Issuance of DL and RC Cards at RTO

At each RTO, DL and RC Cards will be generated with the help of Issuer Authority (IA) Cards. To enhance the security against chances of compromise etc. a pair of these cards will be required for DL and RC cards generation. Each of the IA cards from the pair will be possessed and used by two different individuals from RTO office. Software to perform these operations has been developed by NIC and audited by third party

9. Recharging the Issuer Authority Card

All issuer cards will be issued for generation of limited number of DL/RC cards. After this limit is exhausted, IA cards will seize to issue further card till they are recharged by SKMA, using SKMA card.

10. Risk Factors Involved

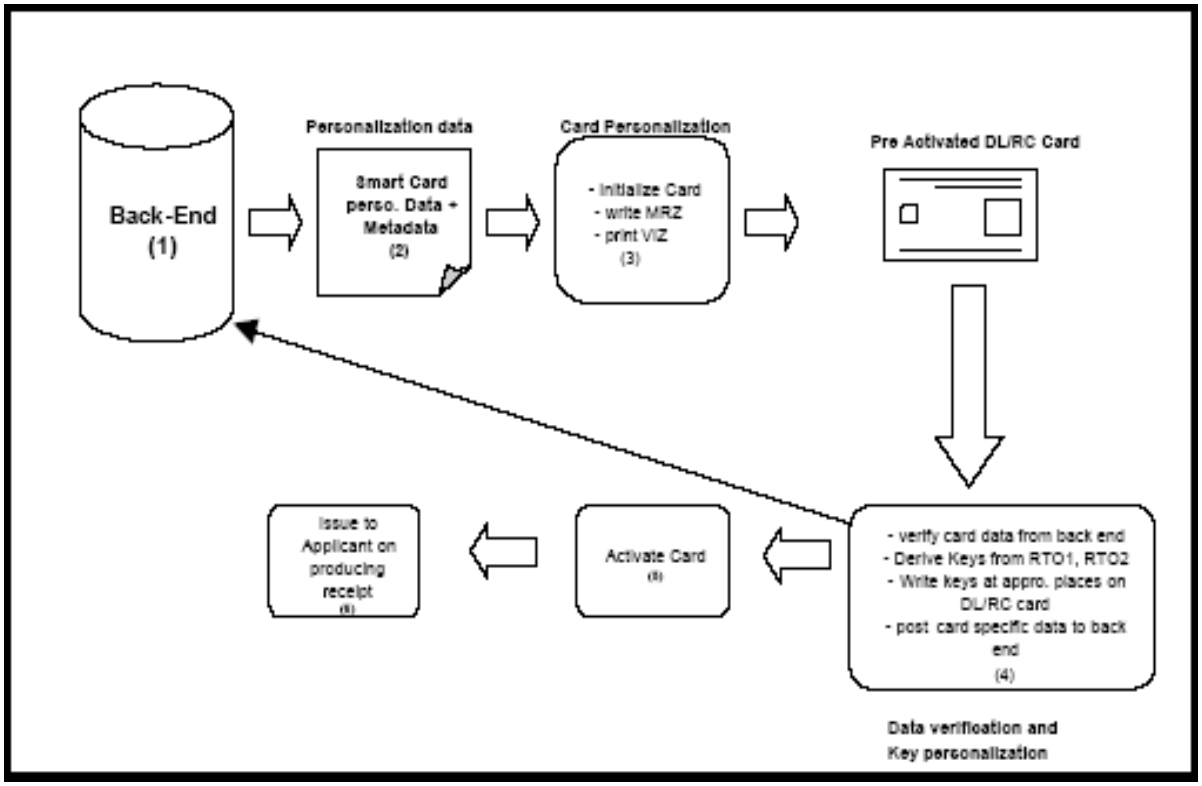
SKI System for DL/RC has been designed above certain technical assumptions and also while implementing this, few risk factors also involved. It is necessary that these technical assumptions and risk factors are brought to the notice before implementing the same.

Technical Assumptions/Risk factors

i. All keys are securely stored on the Smart Card, and there is no known/unknown method to intentionally or un-intentionally download the keys.
ii. No reverse engineering is possible to reverse engineer the 3DES algorithm, used in the Smart Card.

iii. The software developed to perform KMS functionality has incorporated all security precautions.

Workflow Process Model for Smart Card based DL/RC Issuance at RTO



Annexure III

State Key Management Authority
RTO Key Management Authority
Infrastructure Requirements and Security Processes

1. **Space Requirements**
2. **Safe and Secure Storage of Cards**
3. **Secure Access**
4. **Hardware**
5. **Networking**
6. **Software**
7. **Consumables**
8. **Personnel Security**

1. **Space Requirements** : SKMA requires a secure space against theft, burglary, fire, flood and other risks against storage and usage of Authority Cards at State level. It should not be located in the basement, immediately below roof top, immediately below kitchen or canteen or chiller plant, below a building's water tank, near the staircase, building drains or the pump room, on a floor surrounded by open platform or in open area.

2. **Safe and Secure Storage of Authority Cards** :

   a. The data safe which houses the active set of master seed key cards should be secured from the following:
   - Fire
   - Magnetic fields
   - Dust
   - Unauthorized access
   - Pilferage
   - Accidental or malicious damage
   - Humidity
   - Electrostatics

   In particular, the Data Safe should:

- Provide fire resistant performance as per IS 14562 for one hour rating
- Be burglary resistant in compliance of IS 5244 requirements
- Have adequate bolt work and locks that will resist forcible access and severe crow bar attack.
- Adequate storage arrangements with separate locker chambers

b. For further configuration and Authority Cards storage plan please refer to Annexure IV

3. Secure Access :

a. DL issuance rooms in RTO's and other data centers /computer rooms should be securely locked, when left unattended or outside normal working hours.

b. Signs indicating "Restricted Entry" or a similar message should be prominently posted at all entrances to SKI Premises.

c. Fire extinguishers should be installed at the SKMA/ RTO site and their precise locations clearly marked with appropriate signs.

d. Building, furniture, fittings, upholstery materials used in SKMA/ RTO locations in the key card generation/ issuance and IT equipment rooms shall be of non-combustible materials/ fire-resistant and free of toxic chemicals.

e. The SKMA/RKMA facility should have its own independent air-conditioning and fresh air supply system.

f. Temperature and humidity detectors must be installed and shall be connected to audible alarms.

g. It is recommended that the air-conditioning system maintain the following:
  - Temperature around 22 degree centigrade
  - Relative Humidity around 50 %

h. Physical access to the key generation/issuance/renewal premises in SKMA/ RTO should be controlled at all times and restricted to authorized personnel only.

i. The date and time of entry and departure of visitors and external third parties as well as the purpose of visit should be recorded in a visitors' log, especially at RTO sites. The visitors' log should be maintained both at the main building premises' security gate as well as the RTO facility.

j. Procedures should be instituted to ensure that access is granted to individuals on a need-to-use basis.

k. An up-to-date list of personnel who have the access to the key card generation room/ facility of RTO shall be regularly maintained and a log of entry and exit times of personnel should be maintained. The RTO nodal officers should ensure that the said list of personnel is always updated.

l. Personal information processing equipment of any nature, including but not limited to Laptops, Tape Drives, Zip Drives, PDA's etc. –whether belonging to employees or trusted third parties- should not be allowed inside the CKGA, SKMA and RTO facilities unless authorized by the respective nodal officers.

4. <u>Hardware :</u>

a. At SKMA : The requirement of hardware mentioned here is only of indicative nature and minimum, actual hardware requirement assessment must be done keeping the business load of the individual site.

- Low End Server System with Data Backup/CD Write facility
  i. OS : Windows 2000 Server
  ii. Database : SQL Server
- Client System : Window XP based system with Three Smart Card Readers to be connected on USB Ports.
- Dot matrix Printer for printing of PIN

b. At RKMA : The requirement of hardware mentioned here is only of indicative nature and minimum, actual hardware requirement assessment must be done keeping the business load of the individual site.

- Client System : Window XP based system with Three Smart Card Readers to be connected on USB Ports.

5. **Networking:**
    a. The Hardware used at SKMA will have its own Local Area Network (LAN) connecting SKMA Server System with SKMA Client systems. This LAN will be totally isolated from any other logical or physical connectivity to outside world.
    b. The Client Systems at RKMA will be connected to local LAN of RTO, and will be protected for the access through Personal Firewall on these clients, so that these systems are able to initiate connection to RTO Database Server Systems, and no system from the LAN including RTO Database Server is able to initiate a connection on these Client Systems, in any of its ports.
6. **Software** : All the Card Key Management System Software will be provided by NIC on behalf of Ministry of Road Transport and Highways.
7. **Consumables** : Following kind of consumables will be required at SKMA and RKMA
    - Printer Ribbons/ cartridges
    - Secure Stationary for PIN Printing
    - CD's, Tapes etc for backup
8. **Personal Security** : People are one of the most valuable assets of any organization. However, careless, uninformed, undisciplined or disgruntled employees may cause significant problems of information security. At the same time, employees are ultimately responsible for controlling the dissemination of confidential information. Therefore, policies, standards and procedures must be implemented to address the risks of human error, theft, fraud or misuse of facilities and assist all personnel in creating a secure Symmetric Key Infrastructure.
    a. **Definition of Trusted Agents**
    Trusted agents include all employees, vendors, consultants and other business associates at CKGA, SKMA and RKMA levels who are involved in:
        - the generation, issuance, revocation, distribution and destruction of master seed key cards;
        - the generation, issuance, revocation, distribution and destruction of master key cards;

- the receiving, scrutinizing, rejection, or other processing of DL/RC Applications and issuance/ destruction of DL/RC cards;
- Card vendor/ manufacturing and card personalization activities;
- endorsement and review activities;
- the authentication and access control–physical and logical- for the physical infrastructure and IT configurations of CKGA, SKMA and RTO;
- the acquisition of back up key cards from pre-designated secure disaster recovery sites.
- including personnel having access to restricted portions of the database/ repository at CKGA/ SKMA/ RTO

b. SKMA/RKMA must ensure that all personnel performing duties with respect to smart card based DL/RC are appointed in writing, be bound by contract or statute to the terms and conditions of the position they are to fill, not to disclose sensitive security –related information or applicant information and not to be assigned duties that may cause a conflict of interest.

c. In particular, all employees should sign information security agreements upon initiation of employment or contract. The following agreements should be stored in the individual's service file and will be renewed each year:

- Confidentiality or non-disclosure agreement
- Acceptable use of computing resources
- Statement of acknowledgement and consent to adhere to basic principles of Information Security

d. Computer terminals/ systems, printers and associated IT equipment should not be left logged on, when unattended. Key locks, power-on and screensaver passwords, or other controls should be used to protect them when not in use.

e. PCs or servers should not be left unattended with an administrator or a privileged user logged in. System Administrators should log out any privileged accounts before leaving the work area.

f. Computer media should be stored in suitable locked cabinets when not in use, especially after working hours.

g. PIN/ Password Management

Objectives

Access to information and data should be controlled in order to restrict access to authorized users only. If inappropriate access is granted, unauthorized amendments may be made to application software, information or data. Therefore, lack of strong user access management practices could affect the integrity of the information and result in unauthorized agents maliciously regenerating mother keys and/ or issuance of Authority cards.

i. PIN's / Passwords should be mandatory for all Authority Card and master key card users.
ii. Procedures should be put in place to ensure that strong PIN's/ passwords are selected. *Internationally-accepted best practices* recommend that passwords:

- be generated by the user of the Authority cards;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long sub string of the user's profile name

The passwords should not be based on anything that somebody else could easily guess or obtain using collateral information such as:

- One's personal life (e.g. names, telephone numbers and dates of birth etc.)
- Common words found in dictionary
- Technical words relating to NIC/ Ministry of Road Transport and Highways' computer systems environment
- Famous dates
- Prominent individuals

iii. Users should never share or divulge their PIN's/ passwords. All users will sign an undertaking to keep passwords confidential.

iv. Users will promptly change PIN's/ passwords that have been compromised or are suspected of being compromised.

v. Users should not store PIN's / passwords in readable format in batch files, log-in scripts, terminal function keys, files on local hard drives, "yellow stickers" or any other locations where unauthorized persons might discover them.

vi. PIN retries should be limited to a maximum of four attempted logons after which the user ID shall then be locked *(bad logon attempts).*

vii. After the PIN has been locked, all Authority Card and SKMA users should access the PIN Unblock Code (PUC) securely stored elsewhere. All IA, EA and RA master card users whose PIN has been locked should get in touch with the respective SKMA for unblocking the PIN.

viii. At the very outset, all Master Seed Key Card users should change their PIN's. The PIN's should then be committed to memory by the trusted agent.

ix. Procedures should be established to ensure that PIN's/ passwords are changed at regular intervals or based on the number of accesses. A password expiration period *("PIN/ password age")* of 60 days should be set so that Authority

Card users are forced to change their passwords after the expiry of this period. However, PIN's/ passwords for all SKMA and master card users should be changed in case of suspected compromise.

x. In the event of a Authority Card user being terminated or otherwise separated, the PIN/ password for privileged access should be changed as early as possible. The concerned officer should appoint a new trusted agent as the Authority Card custodian and he/ she should once again change the PIN.

xi. All PIN's/ passwords used shall be resistant to dictionary attacks and well- known password cracking algorithms.

xii. The practice of "recycling" or reusing the same PIN/ password *(PIN/ password uniqueness)* when prompted for a change will be prevented.

xiii. Default passwords, shipped with software, will be immediately changed upon installation of the software (if any).

xiv. System files holding authentication data or passwords, if any, will be protected from unauthorized access.

Annexure IV

Symmetric Key Infrastructure
Roles and Responsibilities

State Key Management Authority

- *Authority Card Issuance:* The SKMA nodal officer should access and collate the request received from the RTO's in the state for various classes of master key cards and forward them to the CKGA nodal officer. (Refer Form RTSK1)

- *Authority Card Issuance:* The SKMA nodal officer should ensure that he receives from the CKGA officer, the same number and types of Authority cards (viz. IA1, IA2, EA and RA etc.) as requested for.

- *Authority Card Issuance:* The SKMA nodal officer should collect the Authority cards only after producing a verifiable employee ID card or other satisfactory identity document and furnishing an acknowledgement for the receipt of the Authority cards.

- *Authority Card Issuance:* The SKMA nodal officer should send by a courier service/Fax/e-mail his/ her confirmation to the CKGA nodal officer about his/ her having brought the Authority cards safely to SKMA.

- *Authority Card Issuance:* After collecting the Authority cards from the CKGA nodal officer, SKMA nodal officer should be responsible for managing the distribution of the same to different trusted agents in the state.

- *Authority Card Issuance:* The SKMA nodal officer should inform the RKMA nodal officer within 1 working day by registered post/Fax/e-mail and ask him/her to collect Authority cards and their respective PIN's from the SKMA.

- *Authority Card Issuance:* The SKMA nodal officer should match the acknowledgement along with the signatures received from the RKMA nodal officer with the records.

- *Authority Card Issuance:* The SKMA nodal officer should maintain an RTO-wise distribution list for the Authority cards, containing the Authority card details and the details of the RTO/ RKMA nodal officer to whom the Authority cards and PIN's have been issued. (Refer Form RTSK3)

- *Authority Card Issuance:* SKMA Nodal Officer should update the Authority card distribution list every time an RKMA Nodal Officer under it informs of a change of ownership of the Authority card(s) or other particulars of the existing Authority card(s).

- *Security Audit:* The SKMA nodal officer should ensure that an annual independent security audit of the physical and IT infrastructure of each RTO within its jurisdiction to the extent used for the issuance of DL cards, location of SKMA system and safe keeping of the Authority cards, is carried out by a technical audit team deputed by NIC, initially and later by a responsible and reputed third party.

- *Security Audit:* In addition to the above, the SKMA nodal officer should also visit the respective RTO from time to time, to inspect and ensure that the DL/RC card issuance process, Authority card management procedures and the database management procedures are being strictly followed.

- *Safe Storage:* The SKMA Nodal Officer should store the active and backup SKMA cards and their PIN's in a Thick Steel Safe having two lockers and in a manner such that:

  Locker 1 has,
  - the active SKMA card,
  - PIN for the backup SKMA card and,

  Locker 2 has,

- backup SKMA card,

- *Physical keys to the lockers*: As mentioned above, each of the two lockers/ locker chambers will require a pair of keys to unlock. One key from every pair of keys should be in the custody of the SKMA nodal officer. The other key should be in the custody of another officer to be designated by SKMA Nodal Officer.

- *Safe Storage:* The SKMA nodal officer should be physically present every time the two safes housing the backup SKMA card and its PIN are accessed.

- *Usage Counter:* The SKMA nodal officer should reset the Issuer Authority Cards (DLIA1, DLIA2, RCIA1 and RCIA2) usage counter within 1 working day after receiving request from the RTO nodal officer.

- *Master key Compromise:* On receiving request from the RKMA Nodal Officer for arranging the generation of another set of backup Authority cards within the period of 5 working days after being informed about Authority card compromise, the SKMA nodal officer should forward the request to the CKGA nodal officer.

- *Master key Compromise:* The SKMA nodal officer should maintain an issuing authority-wise list of damaged/ lost/ compromised Authority cards, which he would update every time a Authority card damage/ compromise is reported by any of the issuing authority.

- *Master Key Destruction:* The SKMA Nodal Officer should ensure that the compromised, damaged, faulty, Authority card are destroyed –physically and logically- in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key.

- *Master Key Destruction:* The SKMA nodal officer should be responsible for logging the Authority card destruction activities,

including the number and serial numbers of Authority cards, the date and time, names and designations of trusted agents/ officials present. The above log should be securely archived for a period of not less than 5 years.

- *Master Key Destruction:* The SKMA nodal officer should also inform the CKGA nodal officer about the destruction of the Authority cards along with the details.

- The SKMA Nodal Officer shall be responsible for managing the distribution of the PIN's of the Authority cards to the RKMA Nodal Officers in the state only after the SKMA nodal officer has handed over the Authority cards to them.

- At the time of initial establishment of the Symmetric Key Infrastructure, concerned State Government should appoint/designate the SKMA nodal officer for the state and send by registered post, the SKMA nodal officer's name, and designation and identification details to the CKGA Nodal Officer.

- On being informed of the SKMA key card compromise, the SKMA Nodal Officer should ascertain that the SKMA card has actually been compromised before authorizing and approving the recovery of the backup SKMA Master Key card.

RTO Key Management Authority

Each RTO shall have a designated RTO Key Management Authority (RKMA) nodal officer and his name, designation and identification details shall be communicated to SKMA NodalOfficer by the RTO.

- The RKMA nodal officer should be responsible for appointing minimum two trusted agents/ officials – Issuing Authorities (IA) each for issuance of DL and RC cards.

- The RKMA nodal officer should record the name, designation, signature and photograph and other details of all IA's/ EA's/ RA's and other trusted agents within the jurisdiction of the RTO.

- *Authority Card Issuance:* The RKMA nodal officer should send the request for required number and Type of Authority Cards to SKMA Nodal Officer (Refer Form RTSK2)

- *Safe Storage:* The RKMA nodal officer should be responsible for safe storage of the active and backup IA, RA and EA cards in a Thick Steel Safe having Three lockers and in a manner such that:

  Safe 1 has,
  - Active IA1 cards,
  - Initial PIN for active IA2 cards,
  - Backup IA2 cards,
  - PIN's for backup RA cards,

  Safe 2 has
  - Active IA 2 cards,
  - Initial PIN for active IA1 cards,
  - Backup IA1 cards,
  - PIN's for backup EA cards and,

  Safe 3 has,
  - PIN's of the back up of IA1 and IA2 cards and,
  - Backup EA cards,
  - Backup RA cards,

- *Safe Storage:* Active IA1, IA2 cards must be stored in these safes as per the procedure mentioned above at the end of each working day and taken out at the start of next working day.

- *Safe Storage:* IA1 and IA2 cards should never be kept out of the safe, whenever they are not in use.

- *Physical keys to the safe*: For the three safes mentioned above, each of the three safe/ safe chambers will require a pair of keys to unlock. One key from every pair of keys should be in the custody of the RKMA nodal officer. The other key should be in the custody of the issuing authority.

- *Security Audit:* The RTO nodal officer should ensure that the KMS software, made available by NIC on behalf of Ministry of Road Transport and Highways, Government of India is used for all DL related activities at the RTO.

- *Master Key Issuance:* The RKMA nodal officer should collect the Authority cards from SKMA nodal officer by producing a valid employee Id.

- *Master Key Issuance:* The RKMA nodal officer should also collect the PIN's for the Authority cards from SKMA Nodal Officer by producing a valid employee Id.

- *Master Key Issuance:* The RKMA nodal officer should furnish an acknowledgement for the receipt of Authority cards and PIN's to the SKMA nodal officer.

- *Master Key Issuance:* It is the responsibility of the RKMA nodal officer to manage the distribution of the master key cards to the IA's/ EA's and RA's in the RTO region. He should inform the IA/ EA and RA officials to collect their respective master key cards by registered post within one working day.

- *Master Key Issuance:* The RKMA nodal officer should ensure that IA's/ EA's/ RA's change their initial PIN's immediately after receiving their Authority cards.

- *Master Key Issuance:* The RKMA nodal officer should receive an acknowledgement from the IA's/ EA's/ RA's after issuing them the master key cards and their initial PIN's.

- *Master Key Issuance:* The RKMA nodal officer should be responsible for ensuring that two IA's (who will issue DL/RC

cards in tandem) are provided with IA Authority cards which is a unique pair.

- *Master Key Issuance:* The RKMA nodal officer, after duly recording the Authority card owner details, should send the acknowledgement back to the SKMA office where the acknowledgement number and other particulars pertaining to the Authority card owner should be recorded by SKMA Nodal Officer.

- *Backup:* The RKMA nodal officer should be physically present every time the three safes housing the IA, EA and RA and their backup master key cards and their PIN's are accessed.

- *Usage Counter:* The RKMA nodal officer should forward the request for resetting of IA usage counter received from the two IA's to SKMA Nodal Officer.

- *PIN Management:* The RKMA nodal officer should ensure that in the event of suspected PIN compromise, new PIN's are generated by all IA's/ EA's/ RA's for their respective master key cards in the presence of the RKMA Nodal Officer.

- *Master Key Compromise:* The RKMA Nodal Officer should be responsible for accessing the backup EA and RA Master Key Cards along with their PIN's from the secure safes. These should be handed over to EA/ RA only after the receipt of a '*Backup Key Acknowledgement'* form duly signed by the EA/ RA. The said form should be archived for future records for a period of not less than, when the next audit is conducted.

- *Master Key Recovery:* The RKMA Nodal Officer should request the SKMA nodal officer to arrange for generation of another set of backup master keys cards within the expiry of 5 working days after being informed about master key card damage/ loss/ compromise.

- *Master Key Destruction:* The RKMA Nodal Officer should be responsible to ensure that all damaged Authority cards are

returned under sealed cover to the SKMA nodal officer. This should also be included by a *'Card Destruction Request'* which should clearly state the number and class of master key cards to be destroyed and the names and designations of officers who were the custodians of the said cards.

- *Master Key Destruction:* The RKMA nodal officer along with the IA's should be responsible for securely destroying- physically and logically- the damaged, redundant DL/RC cards as per requirement, in a manner that key reconstruction is rendered impossible.

- *Master Key Destruction:* The RKMA nodal officer should be responsible for maintaining the smart card destruction log, containing details like the number of DL/RC's, their serial number, names and designations of the IA's/ nodal officer present. This log should be securely archived until the technical audit takes place.

- In case of unavailability of either of the IA's, the RKMA nodal officer should immediately take possession of the key to the secure safe of that IA. He/ she should designate a new trusted official/ agent as the new user of the IA card and hand over the keys of the secure safe containing the IA card to him/her with instructions to change the PIN for the IA card immediately.

- *IA Card Issuance:* The IA should furnish an acknowledgement on receipt of the master key cards and their PIN's to the RKMA nodal officer.

- *Key Security:* The two IA's should not carry their respective IA cards outside the office premises and securely store them in two separate secure safes inside the RKMA after the working hours.

- *Safe Storage:* The IA's should ensure that the DL/RC cards after being generated are housed in either of the secure safes used for storing the active set of IA cards.

- *Usage Counter:* Both the IA's should send a request, in writing, to RKMA to arrange for replenishment of the usage counter.

- *PIN Management:* The two IA's should not disclose the PIN's of their IA cards to anybody within or outside RTO. Even the two IA's should not share their PIN information with each other.

- *DL/RC Issuance:* It is the responsibility of both the IA's to be present at the time of DL/RC key generation. They should ensure that all the keys for the DL/RC card are generated and stored in the DL/RC card such that the DL/RC card is completely functional.

- *DL/RC Issuance:* The IA's should be responsible for verifying, physically and with the RTO database, the correctness of applicant information in the DL/RC card, after receiving the printed card from the card personalizer.

- *DL/RC Issuance:* It should be the responsibility of the IA's to securely archive the DL/RC acknowledgement forms received from the DL/RC distributing officer for a period of not less than 5 years.

- It is the responsibility of each IA to immediately inform the RKMA nodal officer in case of their unavailability/ incapacity to perform his/ her duties.

- *Key Compromise:* If the IA believes there has been a compromise of/ damage to his/ her Authority card, he must promptly notify the RKMA nodal officer.

- *Key Compromise:* The IA should send a request, in writing, to the RKMA nodal officer to access the backup master key cards and their PIN's in an event of loss/ damage/ compromise of the master cards.

- *DL/RC Destruction:* In case of damage of/ modification to the DL/RC card, the IA should be responsible for completely

destroying the received DL/RC by invoking the *'Comprehensive DL/RC Card Destruction'* procedure.

- *DL/RC Destruction:* The IA's along with the RKMA nodal officer should be responsible for securely destroying- physically and logically- the damaged/useless DL/RC cards once a week, in a manner that key reconstruction is rendered impossible.

Annexure V

Technology Risk Factors and Presumptions in implementing the Symmetric Key Infrastructure

1. The Secret Key stored in Smart Card is never exposed to outside word by any means.
2. No reverse engineering / brute force attack methodologies will be successful in decrypting encryptions based on 128 bit 3DES algorithm.
3. The KMS applications are executed in a controlled environment with adequate controls to mitigate the risk of Key Compromise. The requirements for the controlled environment are listed in detail in the earlier Annexure.
4. Database security and its integrity for Back End operations (VAHAN and SARATHY) have been fully ensured.
5. The operators and Trusted agents working on the KMS operations are bound by contract not to disclose the details of Application Software to un-authorized persons or entities. And each of such persons have signed the Non Disclosure Agreement with the SKMA of the State.

Annexure VI

S.No	Application/ Module Name	Version / Date	Application Exe	Hash Value
	SKMA			
1	Personalization of Issuing Authority Pair (DL)		DLIAPerso.exe	
2	Personalization of Endorsement, Review and Verifying authority		DL-OthersPerso.exe	
3	Personalization of Issuing Authority Pair (RC)		RC-IAPerso.exe	
4	Personalization of Other RC Authority Cards		RC-OtherPerso.exe	
5	DL SKMA Pin Change		DLSKMAPINChange.exe	
6	DL Authority Cards Pin Change		DLAuthPINChange.exe	
7	DL Authority Cards Pin Unblock		DLAuthUnblockPINs.exe	
8	RC SKMA Pin Change		RCSKMAPINChange.exe	
9	RC Authority Cards Pin Change		RCAuthPINChange.exe	
10	RC Authority Cards Pin Unblock		RCAuthUnblockPINs.exe	
11	SKMA		SKMA.exe	
	RKMA			
1	DL Validation		DLValidation.exe	
2	RC Issue		RCIssue.exe	