Services Rendered by Smart Card Technologies Division, NIC for Pan India Projects Since 2002

Background:

A vehicle owner or a driving licence holder used to carry paper documents for Registration certificate (RC) and Driving Licence (DL). These documents were not legible, often in torn condition and were difficult to manage at times. In the year 2000, Ministry of Road Transport and Highways, decided that in view of non-uniformity of documents (DL/RC), heterogeneity of data formats, it was important to evolve and implement standards uniformly across India

A need was felt to develop a Smart Card Operating System that is secure and tamper proof. The SCOSTA (Smart Card Operating System for Transport Application) Operating System for Smart Cards was developed in a dedicated and collaborative effort of NIC, academia and the Smart Card industry. It is based on ISO-7816 standards and therefore, complies with any international requirements. The Testing and Certification for the SCOSTA compliance for the Smart Card industry is done by a committee headed by DG (NIC) involving members from NIC, STQC and CCA.

The SCOSTA project was initiated with the following principal objectives:-

i. **Standardization of Information**

The card layout, data fields and other relevant information stored on the card and the back-end should be standardized to ensure that information on all cards (issued wherever in India) is uniform.

ii. **Inter-operability**

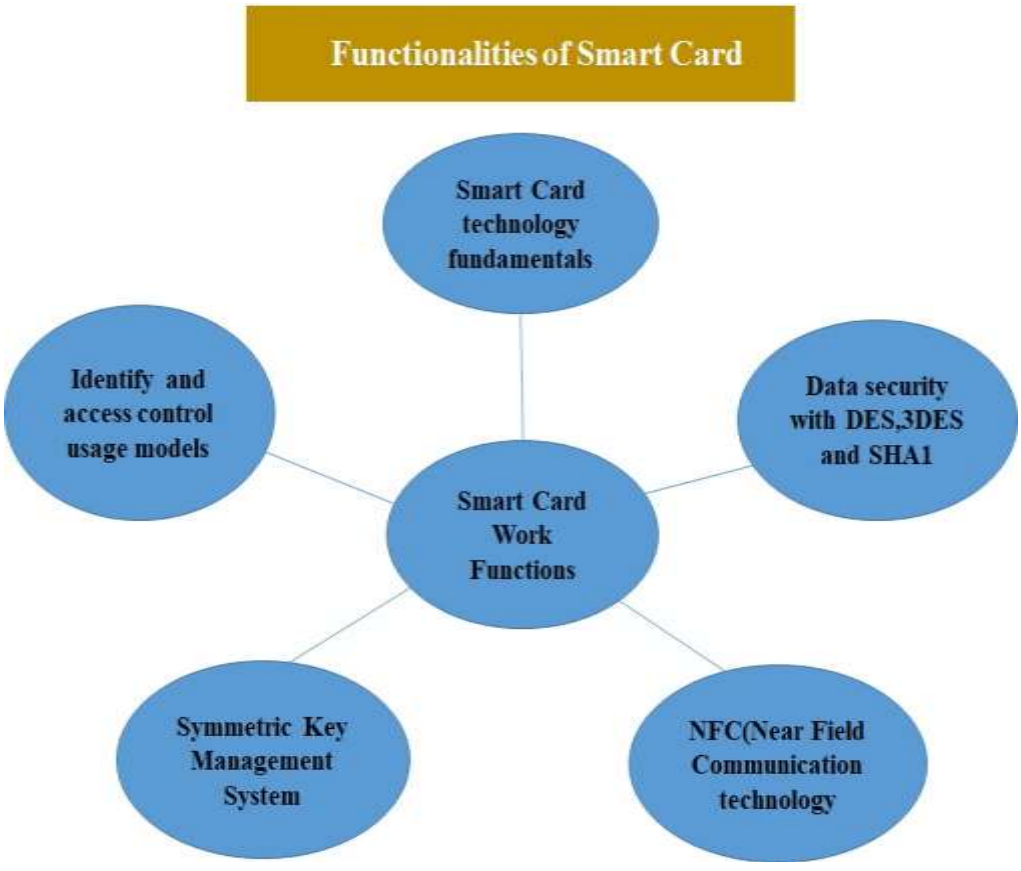
Since the Smart Card Indian applications are to be deployed nationwide, it is essential for the standards to be interoperable and therefore, SCOSTA specifications deal fully with this aspect.

iii. **Multi-Vendor Support / Non-Proprietary**

Keeping in view the need for future up-gradation, multi-vendor support and the critical requirement of the specifications and product to be non-proprietary, it is essential to have the operating system specification to be open and standard.

iv. **Security and Integrity of Data**

A microprocessor based smart card can ensure that only authorized persons can read or write the application data stored in the card. SCOSTA supports both password based and key based authentication of users. The application specifications include secure key management systems that ensure that only officials authorized to change the card data can do so and that it is not possible to create forged identity.



Smart Card Features That Protects Privacy

Secure data storage

Smart cards provide a way to securely store data on the card. This data can only be accessed through the smart-card operating system by those with proper access rights. This feature can be utilized by a system to enhance privacy by storing personal user data on the card rather than in a central database

Encryption

Smart cards provide a robust set of encryption capabilities, including key generation, secure key storage, hashing, and digital signing. These capabilities can be used to protect privacy in many ways. This protects the message from being tampered with, and also provides the recipient with assurance about origination.

Strong device security

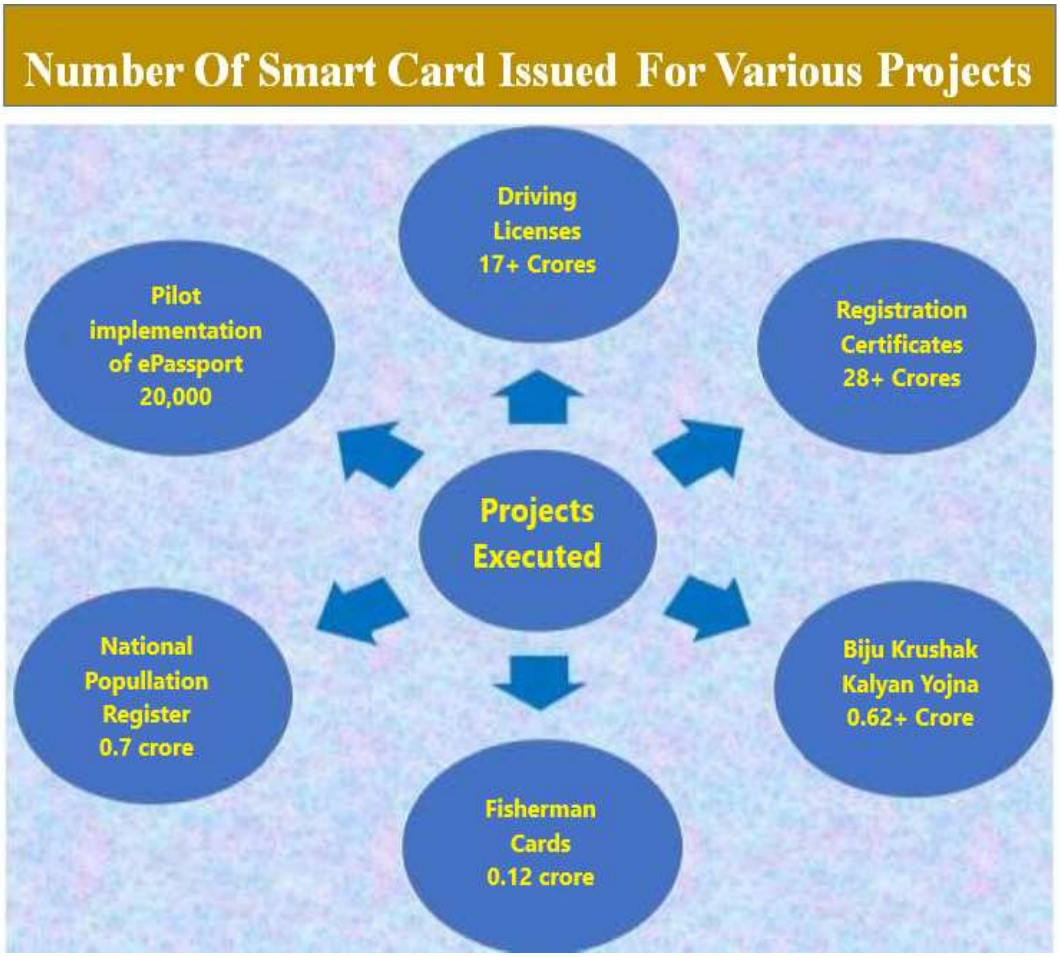
Smart-card technology is extremely difficult to duplicate or forge, and has built-in tamper resistance. Smart-card chips include a variety of hardware and software capabilities that detect and react to tampering attempts, and help counter possible attacks.

Secure communications

Smart cards provide secure communication between the card and reader. Similar to security protocols used in many networks, this feature allows smart cards to send and receive data in a secure, private manner.

Smart Card based PAN India Projects designed, developed and implemented by Smart Card Technologies Division, NIC

MEA	• Electronic Passport for Indian Diplomats & Govt. officials as a proof of concept
MoRTH	• DL & RC cards issuance using Client - Server based applications. • Web Based DL/RC KMS Applications • NFC enabled mobile application for reading for DL/RC Cards
RGI	• Coastal Residence Identity Card
Department of Fisheries	• ID card for Marine Fishermen
Govt. of Odisha	• Biju Krushak Kalyan Yojana(BKKY) Card for Farmers
OTHERS	• National Population Register(NPR) , Rashtriya Swasthya Bima Yojana(RSBY), Public Distribution System(PDS)

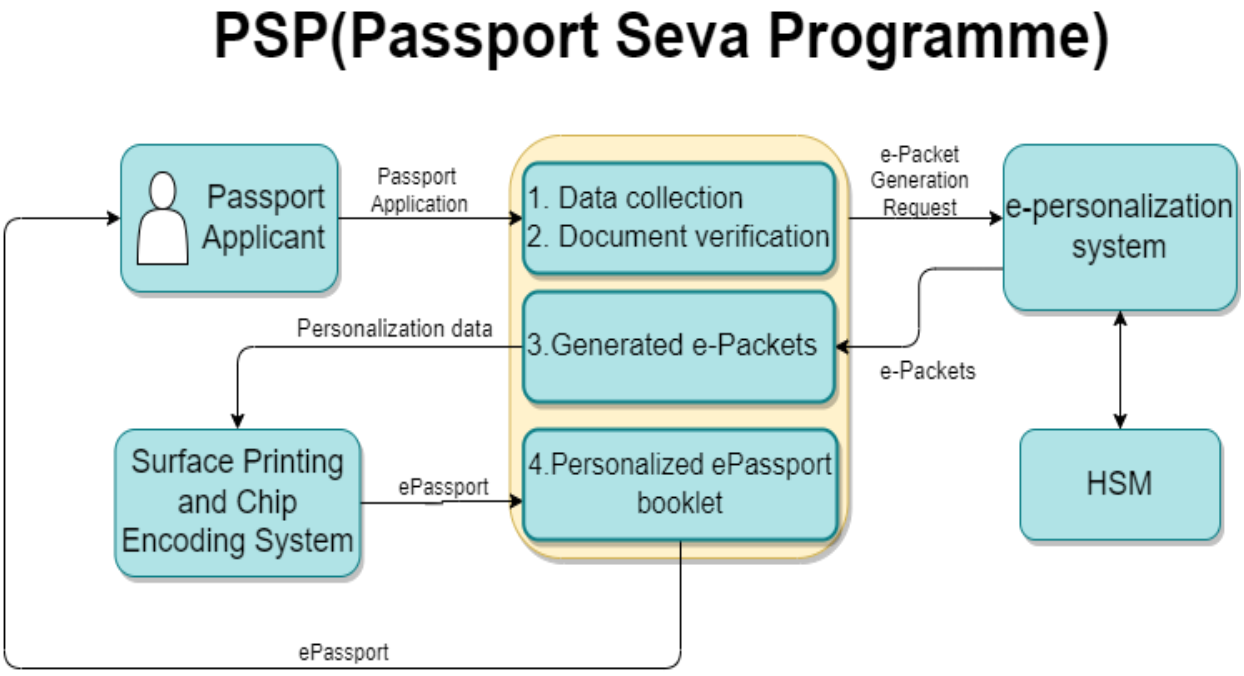


Ministry of External Affairs: e-Passport Project

NIC has been entrusted by MEA to design, develop and execute the issuance of ePassport for Indian citizens, diplomats and officials. NIC has earlier successfully executed a pilot project for issuance of 20,000 ePassports for diplomats and officials.

The ePassport shall secure the identification of the passport holder and will eliminate forgery of biometric information stored in the ePassport. Hence it shall provide enhanced privacy and protection against identity theft. Another benefit of ePassports shall be smoother transit through immigration check posts and Border Control across the world.

All the ePassports that are biometric, need to have a symbol on the front page as depicted below:



Issuance process for ePassport

1. The enrolment data of the end user resides the database maintained by MEA. Data is de-duplicated and the granting officer approves the data for centralizing printing.
2. The process of ePacket generation is completed in advance (in the night) before the start of personalization every day using ePacket Data Preparation Manager (DPM). The data transferred to ePacket DPM will include mandatory Demographic data for Data Group DG1 in xml format, mandatory Photo image for DG2 in XML format, data for other optional DG's and database containing passport number, passports chip serial number and OEM code.
3. Now with these data, DPM system will generate electrical data file called as ePacket to be written in the chip. It includes BAC keys, DG1 (Machine Readable Zone data), DG2 (Photo data). This ePacket is returned to the print queue.
4. Now before writing the ePacket data in to passport chip, chip authentication is done by the printing machine.
5. Once the chip authentication is successfully completed then the printer software writes ePacket personalization file in the blank passport and also prints graphical data on data page of the passport booklet.

Verification process of ePassports

The privacy of the Passports holder, data on the chips is generally protected by an access control mechanism. The access control mechanism denies access to the chip contents unless the inspection system can prove that it is authorized to access the chip. This "proof of authorization" is acquired by reading information found on the data page of the ePassport booklet. The assumption is that if the traveller has willingly handed their ePassport to anybody to open and read.

1. The reader derives access keys based on the data in the machine readable zone.
2. The chip and reader mutually authenticate each other
3. The chip starts secure messaging and grants access to data

Currently ePassports shall use **Basic Access Control (BAC)** for reading data in the chip. In this the inspection system derives the access key by reading the Machine Readable Zone (MRZ) on the data page of the ePassport. The keys used in BAC shall be symmetric.

Once the ePassport chip has been accessed, ePassport validation shall begin, which shall be done by **Passive authentication** method. Passive authentication is the process of

authenticating the digital signature to confirm that the information stored on the chip was saved by the authorised person (i.e. the issuing State) and has not been tampered with.

Ministry of Road Transport and Highways: DL & RC Project

As an e-governance initiative, Ministry of Road Transport and Highways initiated the project of computerization of all RTOs and issuance of Smart card based DL and RC. The Application for issuance of smart card based DL and RC is a first effort of its kind in the country with defined national standards.

The primary objective for introducing smart cards in e-Transport project was to provide security against issuance of fake DL/RC. This resulted in better enforcement of traffic rules & regulations as per Central Motor Vehicle Act. The Driving License (DL) and Vehicle Registration Certificates (RC) are the subjects handled by individual States in the federal fabric of the country, under, constituted and monitored by the Ministry of Road Transport and Highways.

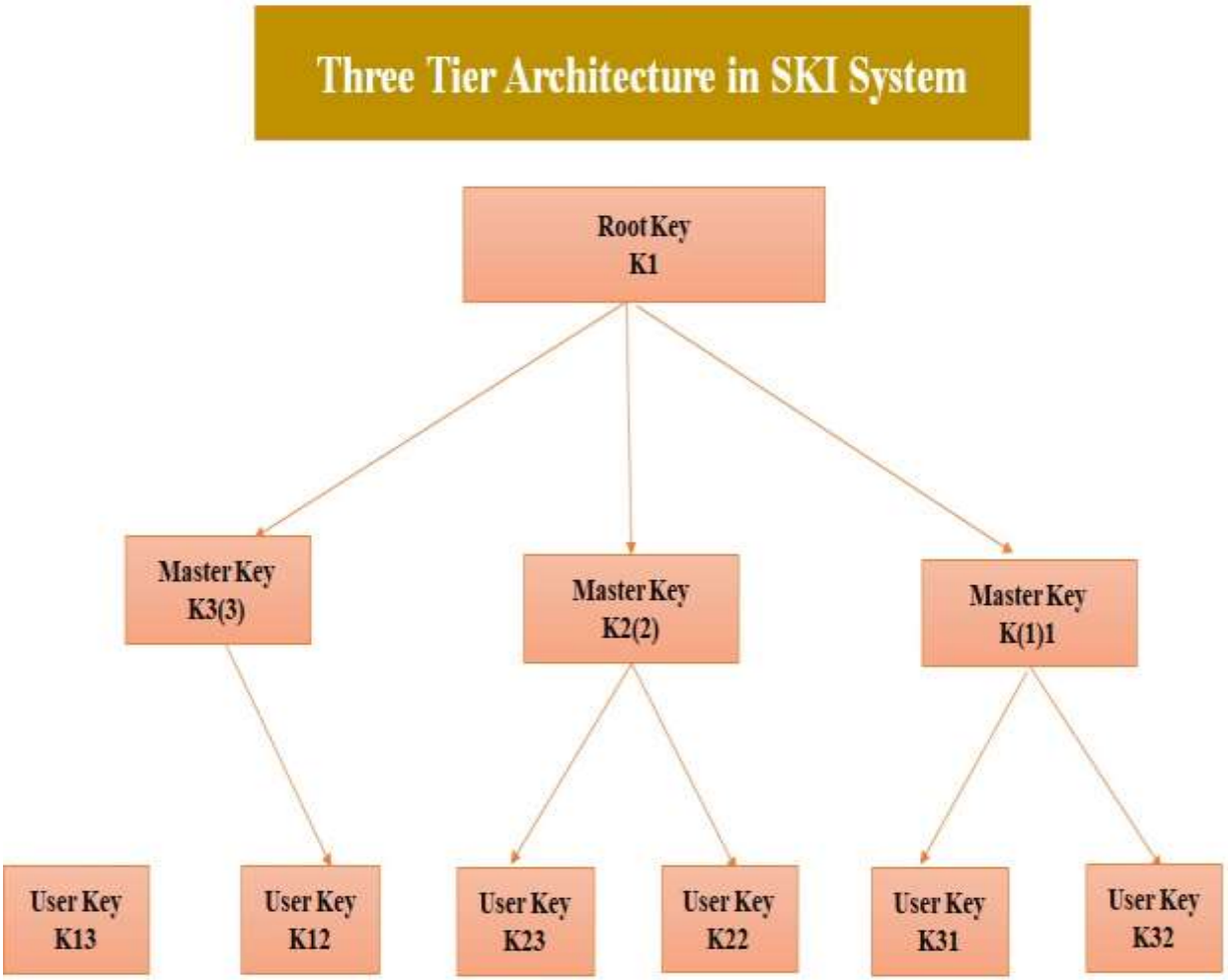
Sample DL and RC Cards

Need for Key Management System (KMS)

KMS refers to the management of cryptographic keys in a cryptosystem that deals with the generation, Exchange, storage, use, destruction and replacement of keys that are used for various operations on smart card. KMS enhances the security of the smart cards and is required for building up a security infrastructure around the basic application of the Smart Card.

NIC has developed expertise in KMS and has implemented KMS for various PAN India projects like e-Transport DL/RC Smart Card Project, National Population Register (NPR), Biju Krushak Kalyan Yojana (BKKY) etc.

The setup which takes care of production, issue and maintenance of authority cards is named as Symmetric Key Infrastructure (SKI) or Key Management System (KMS). Since the processes involved in the whole operations are highly sensitive in nature, the infrastructure required must be established in a highly secured environment.



Web based KMS for the Issuance of RC and DL Cards at RTO's

Need For Web Based KMS

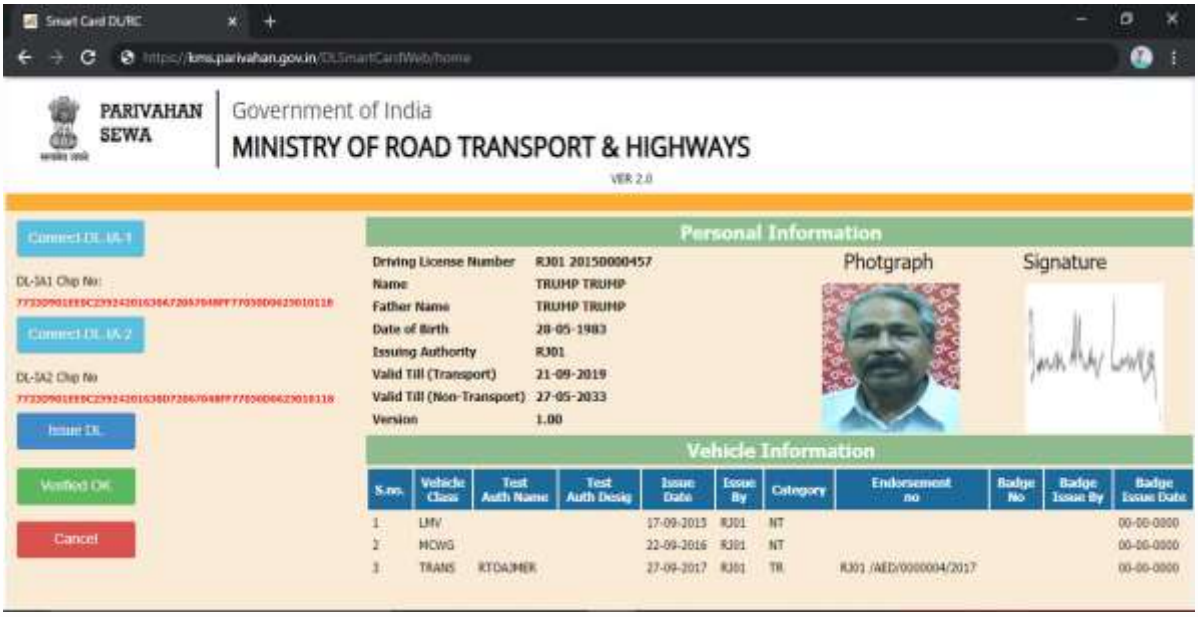
There are approximately 1100 RTOs across the country. At least one database server is required to be in place for individual RTOs. If KMS application needs to be updated, it requires multiple set-ups to be created and installed for individual RTOs. Therefore, the need for web based Smart Card-KMS system was considered prudent to be developed for the implementation of specifications notified by Transport Ministry as per gazette notification of 1st March 2019 for Smart card based DL and RC. The new web based KMS system is designed, developed and implemented by Smart Card Technology Group of NIC. This has resulted in better management of software and hardware resources.

Benefits of Web Based KMS Applications:-

- A web based KMS system facilitates to install the application and its supporting software automatically by using a single url without any additional efforts.
- With the introduction of web based system, the interaction of application with local database could get eliminated making the system work faster and eliminating the data redundancy.
- The web KMS system could result in saving considerable infrastructure cost at local level (RTO).
- The Web based KMS system also results in automatic Updation of application software if required at the client end (RTO's).
- The project could help in saving the time and ease of use by RTO's officials for the issuance of DL/RC Smart cards
- All the benefits stated above could result in making the entire project cost effective as the cost of manpower, hardware requirement and software minimized considerably.

Development of Mobile app for DL & RC

A mobile app was developed for reading personalization data from smart card based DL and RC using NFC. After reading, all the data is displayed on the screen.



Client screen shot for DL KMS

Services provided by Smart Card Technologies Division, NIC

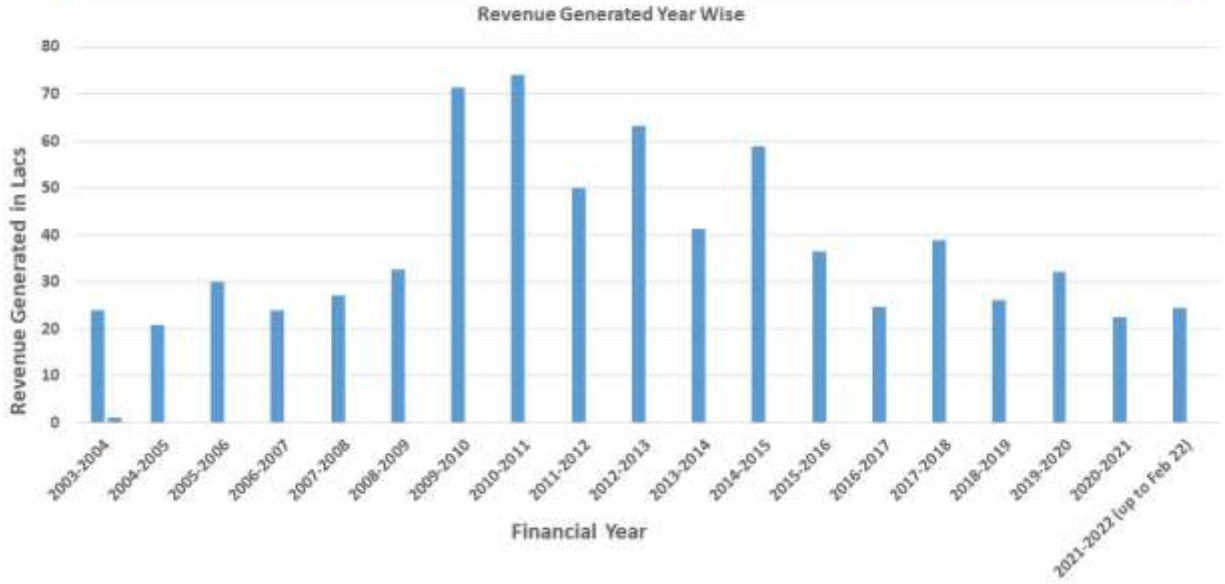
Testing and certification by SCOSTA Compliance Certification Committee for eGovernance Smart Card projects.

The scheme envisages demonstrating conformance to SCOSTA/SCOSTA-CL requirements. The scope of certification is limited to the Smart Card Compliance Certificate of SCOSTA / SCOSTA-CL standard. This scheme is intended to provide by means of system assessment, testing, and subsequent surveillance, an adequate level of confidence that the products (Smart card / Microcontroller module / Inlay) conform to the specified requirements of appropriate standards. SCOSTA/SCOSTA-CL compliance testing is done to verify the compliance of the OS provided by the vendors as per SCOSTA specifications. SCOSTA/SCOSTA-CL certification is required for various smart card-based Id projects for the supply of smart cards.

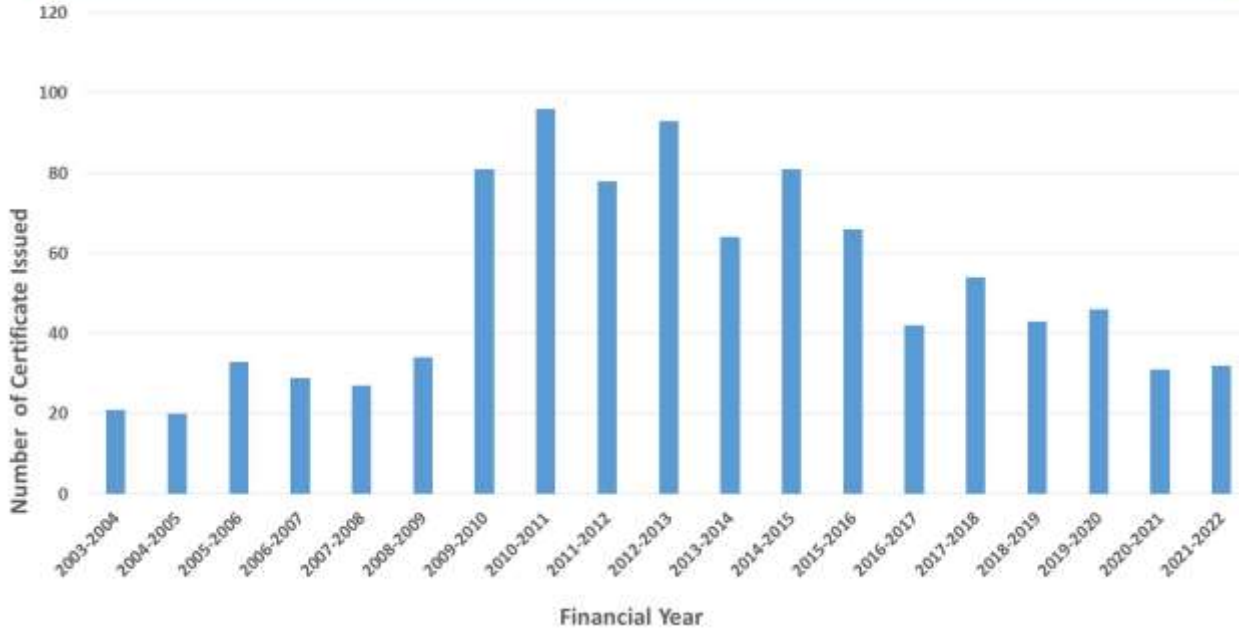
The SCOSTA/SCOSTA-CL Compliance Certification Committee is constituted and headed by DG NIC. This committee comprises members from STQC, CCA and NIC.

As on date, more than thirty major national and international industry players have adopted these standards into their Smart Card products and are being used in the national and international market.

Revenue Generated from 2002 till date from SCOSTA Compliance Certification



Certificates Issued from 2003 till date from SCOSTA Compliance Certification



Milestones Achieved by Smart Card Technologies Division

2001-2002	• SCOSTA Operating System Launched • Initiation of Smart Card Technologies Division
2003-2004	• Designed Key Management System of eTransport application for MoRTH • Designed and developed DL & RC applications for MoRTH
2005-2006	• Implemented eTransport Applications in various States for issuance of DL & RC Smart Cards
2007-2008	• SCOSTA-CL Operating System Launched • Designed and developed Multi National Identity Card (MNIC) for Indian Citizens (Registrar General of India)
2008-2009	• Designed , developed and implemented e-Passport project (PoC) for Ministry of External Affairs • Designed , developed and implemented Smart Card based PDS System in Chandigarh,Haryana and Chattisgarh
2009-2012	Designed , developed and implemented Rashtriya Swasthya Bima Yojana(RSBY) project, a cashless health insurance for Ministry of Labour & Employment.
2013	• Introduction of 64Kb Smart Cards for DL/RC in 27 states • Design, developed and implemented Biju Krishak Kalyan Yojna (BKKY) for the State of Odisha for Farmers
2014	Design, developed and implemented KMS, Handheld Terminal Application and Application Software for Resident Identity Card and Marine Fisherman Identity Card.

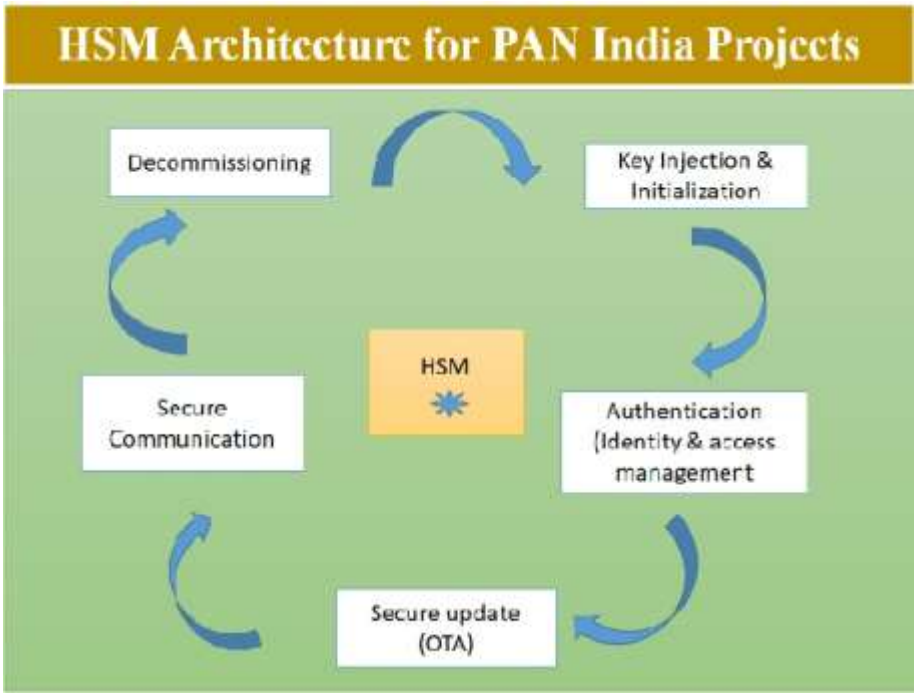
Milestones Achieved by Smart Card Technologies Division

2015-2016	• Change of platform to .NET with introduction of centralized database in Smart Card based DL/RC • Design, developed and implemented Smart Card based National Population Register pilot project for Indian citizens living in coastal areas.
2017	Web services incorporated in DL/RC applications for accessing data from Central Database
2018	Migration of website www.scosta.gov.in to NIC cloud.
2019	Proposal for Creation of Test bed and Interoperability of ePassport at NIC for MEA
2020	New web based KMS application developed for issuance of DL and RC Smart Cards as per new Gazetted notification issued by MoRTH.
2021	• Implementation of new web based application for DL & RC in Punjab and Andaman &Nicobar Islands. • Developed e-Personalization i.e. chip encoding software for DL and RC Smart Cards. • Finalized ePassport data elements in consultation with MEA.
2022	• Testing of ePassport samples for SCOSTA Compliance • Development of ePassport reading Software for ePassport in process • Implementation of web based KMS for DL & RC in States of Bihar and GOA. Other States like Maharashtra, Uttar Pradesh and Tamil Nadu are in the process of implementation.

Future Roadmap

Usage of Hardware Security Module (HSM) in PAN India Smart Card Projects:

A Hardware Security Module (HSM) provides secure key storage, fast access of master keys and cryptographic Operations within a tamper-resistant hardware device**.** NIC has expertise in developing smart card applications using HSM. HSM was earlier used in NPR (National Population Register) and MFID (Marine Fisheries Identity Card) project for securely storing of Authority keys. HSM is used for issuance of user NPR and MFID cards.

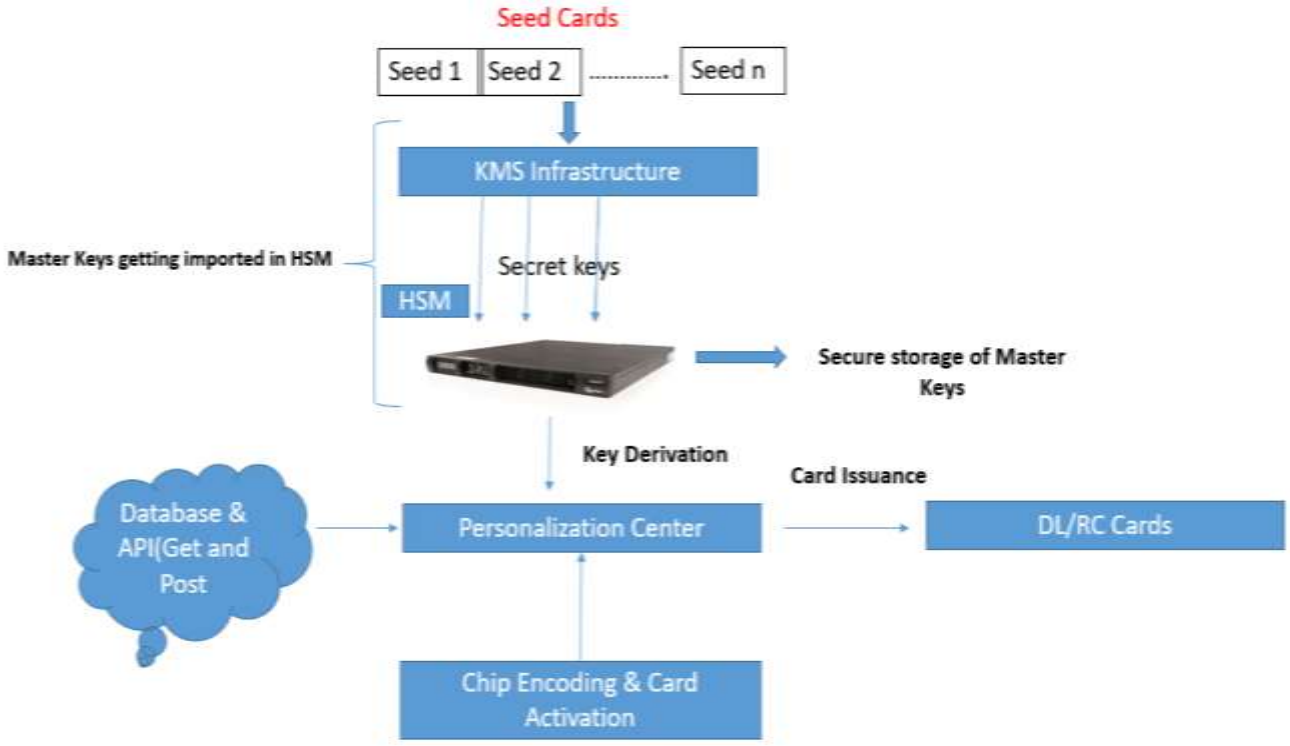


Proposed solution for centralized Card Issuance management system with HSM

a) HSM Based DL/RC Issuance in e-Transport

To enhance the security of online web services for the issuances of DL/RC Cards, it is proposed to use Hardware Security Module (HSM) to secure the key storage. It also provides cryptographic operation within a tamper-resistant hardware device**.** HSM has dedicated and powerful crypto processors which can simultaneously carry out thousands of crypto operations thereby making the KMS work fast and helping in bulk issuance. NIC has developed a smart card application using HSM in National Population Register (NPR), Fisheries etc**.** HSM shall be used for secure storage and fast access of master keys for various projects. HSM provides enhanced security and flexibility in KMS operations. Every KMS system will act as a client and

will be connected to HSM through a secure network. KMS of personalized DL and RC cards will be done on KMS client systems by invoking centralized Vahan/Sarathi KMS application. The application will use authority keys from HSM.



Centralized Card Issuance management system with HSM

b) HSM based chip authentication and issuance of ePassport

HSM in ePassport project shall store secure cryptographic keys and shall perform following cryptographic operations

a. Generation of Secure Data Object(SOD)
b. Chip Authentication

c) Mobile app for reading ePassport

- A mobile app shall be developed for reading ePassport.
- User can download the app from Play Store in NFC enabled mobile.
- Through app, user can connect ePassport using NFC and read the information from the ePassport for its correctness.

d) Reading and verification app for ePassport in KIOSK at every Passport Seva Kendra(PSK).

- A KIOSK shall be installed at every PSK.
- An app shall be developed for reading and verification of ePassport and shall be installed in every KIOSK.
- The user can read and verify his/her ePassport at KIOSK for its correctness.

Currently Used SCOSTA OS (CL) in PAN India Projects

At present SCOSTA Operating System has the following features:-

- The Operating System is a fully open source and interoperable.
- It incorporates security measures using symmetric key cryptography using DES and Triple-DES (3DES) algorithm.
- It has the ability to communicate with contact as well as contactless interfaces using ISO 7816 and ISO 14443 protocols.
- There is no Asymmetric key support.
- No future upgrade beyond PA/BAC is possible for the ePassport.

Smart Card O/S (SCOSTA-CL) to support PKI for enhanced security

Smart Card operating system if incorporates the PKI features like digital signatures, origin integrity, certificate verification, etc. it shall enhance the reliability and security against unauthorized access. It shall also enable the tamperproof storage of biographical and biometric information. PKI features enhance the reliability and security against unauthorized access.

Encryption algorithms like AES, ECC, and RSA can be integrated in existing Operating System also hashing algorithm like SHA 256bits or 512bits can be introduced. This will be still based on International standards (ISO 7816, ISO 14443, ICAO and MRTD) so that interoperability required in product can be achieved. The O/S should support backward compatibility with respect to SCOSTA and SCOSTA-CL specifications.

Under Atma Nirbhar Bharat Abhiyan, an Indian designed and developed chip with home grown OS will enhance the security of the smart card and will also save considerable foreign exchange.

Access Control System

On the request from MHA, a PoC was done for Access control system using SCOSTA complaint smart cards. Based on successful authentication and authorization with the smart card the entities shall have access to the building.

Access Control System

There are around 65 buildings under MHA control in Delhi. The Parliament House, PMO, Rashtrapati Bhavan have different access control cards with a different operating system. The access control cards issued are not interoperable. So the need of the hour is to have an interoperable access control card for accessing all the buildings. Smart card-based Access Control for government employees shall be used for accessing different buildings which are under MHA supervision. The smart card will securely store the demographic and biometric (Photo) information of its holders and provide access only to authorized entity. This authorization will be facilitated by the robust Key Management System (KMS) to be developed around it by NIC.