CDAC Card Operating System (CDAC-COS)

Introduction

Smartcard offers a secure and convenient platform for carrying digital information and credentials for identification and authentication of an individual. It also facilitates the storage of physical credentials like fingerprint, etc. on the same card. The card can be used for multitude of applications like access control, attendance, digitally signing documents, encryption of confidential information, storage of user specific information e.g., medical records, canteen bills, library usage, financial transactions , etc.

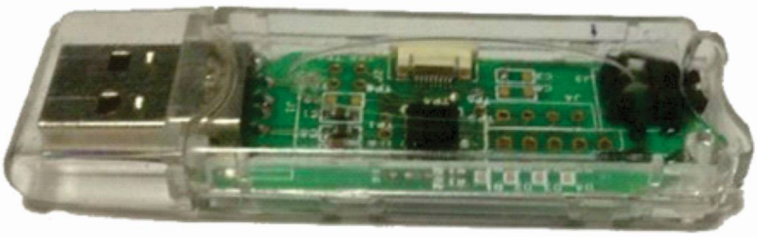
SmartCard Operating System (CDAC-COS CL and CDAC-COS PKI).

Smart card operating system developed by CDAC – CDAC-COS is compliant to SCOSTA-CL standard and Public Key Infrastructure (PKI). The Operating System provides a mechanism for the exchange of information between the smart card and reader and interpretation of commands and data. It facilitates security using symmetric and asymmetric key cryptography using Triple-DES (3DES) and RSA respectively. It can communicate with contact as well as contactless interfaces using ISO 7816 and ISO 14443 protocols. It supports the following operations performed using public key cryptography.

- Authentication
- Authentication and Session Key Establishment
- Computation of Digital Signature
- Encryption and Decryption
- Certificate Verification
- Key Generation

PKI based Crypto Token

The USB based Crypto Token is a compact and portable plug-n-play device which runs SCOSTA PKI operating system. This token securely generates asymmetric key pair for RSA and secures the private keys inside. It ensures that only authorized users can perform various operations using cryptographic functions. It is designed to support a wide range of desktop applications



प्रगत संगणन विकास केन्द्र

Centre for Development of Advanced Computing (C-DAC)

www.cdac.in