Multicard Contactless Smartcard Development and Storage

NXP Key Generation Services

Multicard offers key generation and application development services to ID Card End-Users. Under this program, our Customers own their keys and manage applications. The End-User then controls their own card platform and authorizes which vendors can have space on their card.

Our services include the following NXP chipsets:

- MIFARE Classic®
- MIFARE Plus®
- MIFARE® DESFire® (EV1/EV2/EV3)

Services include:

- Development of Proximity Integrated Circuit Card (PICC) key. i.e., the Master Key.
- Development of Physical Access Control System (PACS) Application using NXP Mutual Authentication Mode Setting specifications:
    - Utilizing AES Encryption
    - Enabling AES Key Diversification
    - Defining the Application ID number
    - Formatting for PACS system
- Custom Applications: Multicard will look at developing customer card applications such as Transit, Logical Access (LACS), Payment, etc. Normally, these are provided by the related system vendor, in which case Multicard will work with the 3rd Party vendor to ensure proper encoding of the card either utilizing the customer IDMS system or pre-encoding process at the time of card manufacturing.

multicard

Key and Application Storage & Management Services

Multicard offers secure storage and management services, which includes a secure key ceremony process to share Customer keys with Customer authorized 3rd Party vendors and stakeholders.

Storage

- Encryption Keys and Applications are stored:
  - On a hardware device. Not in the 'cloud' on a network.
  - Behind a card-access controlled door in a secure, physical room.
  - In a locked storage device within the secure room.
- Disaster recovery:
  - Primary key/application hardware devices are stored in Phoenix, AZ
  - Backup hardware devices are stored at a 3rd Party, trusted location in Orange County, CA.
    - Backup files are stored in a locked safe within a secure office.

Management/Key Ceremony

- All key and application files are also password protected at the file level.
- Multicard used PGP encryption to encrypt all key and application files prior to transfer or transmission.
- When keys need to be shared with 3rd Party vendors and stakeholders the following method is used:
  - Intended recipient of the files sends Multicard a PGP public key.
  - File is re-encrypted using the public key.
  - Encrypted file is sent to recipient via Multicard email account.
  - The file level password is encrypted using the PGP key and similarly sent to the recipient.
- Agreements and Authorizations
  - Key and Application Owner (the Customer) signs an NDA and Intellectual Property Agreement with Multicard and any intended recipient.
  - Customer sends Multicard a written document authorizing Multicard to shares its keys and applications with the intended recipient.
  - Deletion: Upon written notification from the Customer, Multicard and our 3rd Party backup partner will delete all files related to Customer owned keys.