



Contactless Smart microSD Card

India

July 2019

Introduction

- Our product is a contactless smart microSD card (LGM Card) - a product for banks, transit providers, Government, service providers, wallet providers, TSM
- Our product is used while inserted in SD slot of a mobile phone. It enables to store sensitive data on a secure chip and to use this data for mobile contactless payments, transit access, in m-commerce, secure access and other use-cases
- We believe our partner may consider our product mainly because it:
 - has potential to simplify and securely move current financial services into mobile phones
 - addresses currently not-addressed base (not-connected and feature phone users)
 - enables seamless and secure authentication of the mobile phone user
 - can securely store Aadhaar or Virtual ID and thus enable KYC process inline with India Government requirements
 - can open new business streams – in co-operation with government, transit, smart cities
- Implementation of LGM Card enables to use existing card issuance processes, payments processing and merchant acceptance networks

Certified by NPCI as RuPay dual interface card

Product

LGM Card

- Our product is a standard microSD memory card used while inserted in SD slot of user's mobile phone serving him as:
- a memory card with 4 or 16 GB
- a multiple smart card and hardware token - as it has embedded one or two secure chips
- a contactless enabler - as it has embedded miniature NFC antenna
- It can be used in smartphones with OS Android and Windows, in Java devices and also in feature phones. As the miniature NFC antenna works also under batteries and metal back covers customer is not limited by the phones' design
- Service provider (SP) can decide to use LGM Card for own services and within his own partnerships
- The secure chips of LGM Card can be personalized via a standard ISO7816 contacts placed on the surface of the LGM Card. This enables to use current personalization machines

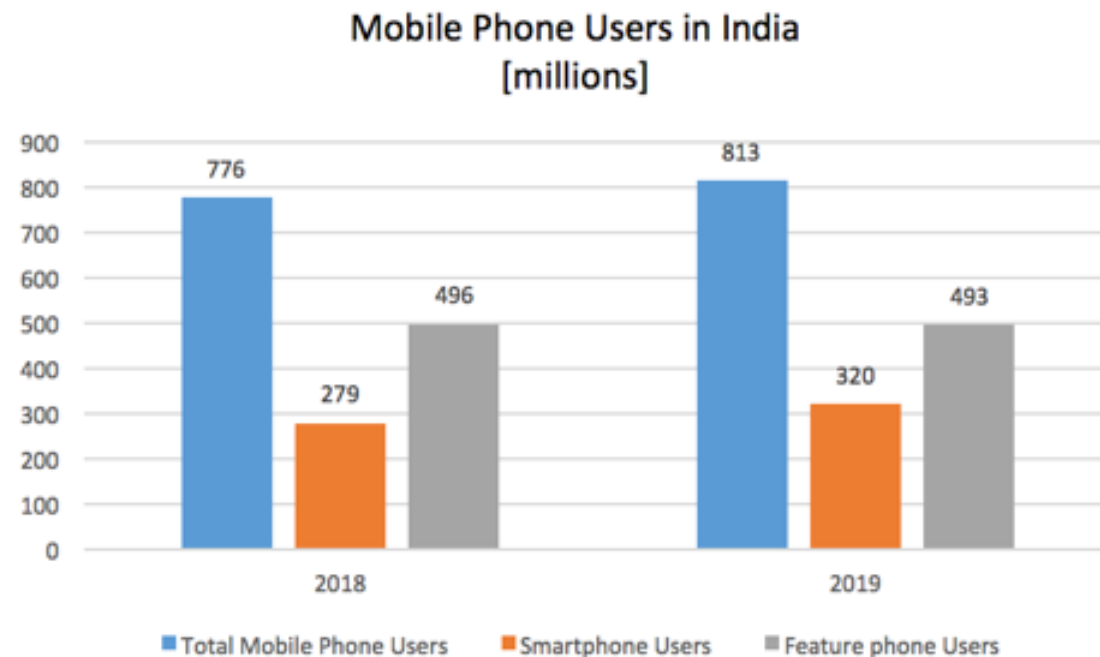


Opportunities

- Address nearly all India citizens, targeting also not-connected and feature phone users - providing them various secure and simple mobile solutions
- Mirror (store) any plastic contactless chip card on the secure chip of the LGM Card - currently 5-7 cards can be stored on one chip of LGM Card
- Store client certificate for a simple both-side authentication (registration and check-in processes) of the user - without entering login credentials or password
- Enable to link Aadhaar number or Virtual ID of the individual user (his device) and simplify KYC process
- Use the sensitive data stored on secure chip of LGM Card for contactless offline and online mobile payments, transit payments and access, m-commerce, as mobile ID card, for access to governmental servers and many other use-cases
- Increase number of secure m-commerce purchases as customer will need not to retype cards data on the phone's screen during payment
- Reuse current infrastructures for cards personalization, issuance and distribution and keep current relations with merchants and other payment industry players
- Remain a full control of your brand, secure data and big data
- Be ahead of competition – providing highly secure, convenient and multi-purpose services from a mobile phone

Addressing huge Base in India

- From approximately 800 million phone users in India – approximately 300 millions use smartphones and 500 millions use feature phones
- Globally 82% of all smartphones and nearly 100% of feature phones have SD slot ². Our microSD card suits both smartphones and feature phones ³



- 1) 2018, based on Indian local vendors information: 67% = feature phones, 34% = smartphones.
- 2) By SD association 2017 and by SLC internal inputs from discussions with Indian phone vendors
- 3) video <https://youtu.be/ybvlayTTxDc>

Addressing Unaddressed mobile Users

- From approximately 800 million mobile users **in India** – approximately 100 million are actual mobile Internet users (usually also smartphone users) and thus potential users for mobile banking / wallets and payments through apps. **Currently all providers focus on this segment only**
- **LGM Card can serve both smartphones and non smartphones and it enables contactless services also for not-connected phones**
- For connected customers (100 million) LGM Card can extend security of current online services and enable contactless services. For not-connected customers (713 million) LGM Card can provide contactless services, e.g. enter transit gate or pay on contactless merchant's POS by a tap of the phone

All SP focus here only

Country	Total Mobile User Base	Smart Phone Penetration	Smart Phone Users	Non Smart Phone Users	Actual Mobile Internet Users	Non Mobile Internet Users
	[Mil.]	[Mil.]	[Mil.]	[Mil.]	[Mil.]	[Mil.]
India	813	35%	285	528	100	713
Sri Lanka	24	20%	4,8	19,2	0,4	23,6
Pakistan	120	20%	24	96	11	109
Bangladesh	130	18%	23,4	106,6	7	123
Indonesia	190	55%	104,5	85,5	36	154

LGM Card can serve all

Based on various public data, 2016-2018

Bank Cards

stored on LGM Card's Secure chip(s)

- Bank can store any type of chip bank card on Secure element (SE) of LGM Card, e.g.:

- EMVCo – VISA, MasterCard, RuPay
- Metro and other transit cards
- Pre-paid, loyalty, QR cards etc.
- Card(s) of 3rd parties – employee cards etc.

LGM Card (Gen1) can physically store 5-7 cards on each SE



- Customers can use these cards from their mobile phones:
 - to purchase by a tap of the phone at any merchants' standard contactless POS
 - to enter and pay for a metro by a tap of the phone (using EMVCo card or Stored value card)
 - for m-commerce using bank card without a need to retype card data during payment
 - to top-up pre-paid cards stored on SE from other card – all from a smartphone
- Cards stored on LGM Card can be personalized in a contact way or Over the Internet (OTI)
- Transactions can be processed via existing infrastructures with agreed Interchange fees (IF)

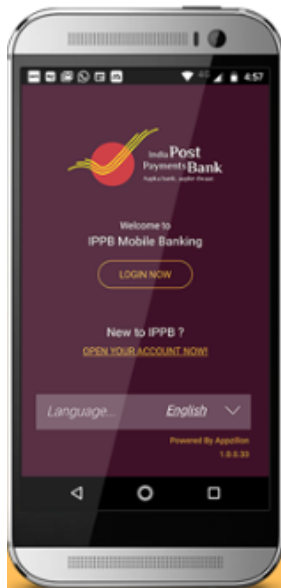


LGM Card

for not connected customers

- Not connected customers usually do not use smartphones. Usually banks provide mobile services to these customers using SMS banking - yet with a limited number of services
- LGM Card will add NFC capability also to basic and feature phones. Bank can offer not connected customers contactless purchases and contactless metro access - by a tap of their phone

Tap & pay on contactless POS
Tap & go on metro
Store Aadhaar on SE



- SE of LGM Card can store Aadhaar number and that can be displayed on a the phone's screen during Aadhaar based purchases
- Tap & pay function can be integrated in Bank's mobile application or it can be enabled from the phone's menu
- Connected customers using Bank's mobile application can benefit in more areas – see next slides

Mobile Transit

- NCMC is EMVCo type of plastic contactless chip card (Q-Sparc, RuPay) that stores credentials on Secure chip and that can be used also for contactless offline transactions and transit gates access in India Smart cities
- LGM Card is ideal mobile alternative for NCMC plastic cards as it:
 - Contains SE – so NCMC card is securely stored / personalized on SE and protecting pre-paid credentials
 - Contains NFC antenna that enables access to metro gates and to pay on contactless POS
 - Enables credentials usage also while the phone is w/o data connectivity (online & offline transactions on POS or transport gate)
 - Does not change eco-system used for plastic version of NCMC
 - Similar usage to plastic NCMC – simple tap (of the phone)
- LGM Card can also store Stored Value Card (SVC) on its SE
- Many top-up options, including that from a mobile phone using other bank card stored on LGM Card. Transit operator can save costs for top-up at kiosks

Plastic NCMC – can be mirrored on SE of microSD and used via NFC antenna of the microSD from a mobile phone



LGM Card

used in m-Commerce

With LGM Card inserted in a mobile phone payments in m-commerce can be easy and secure

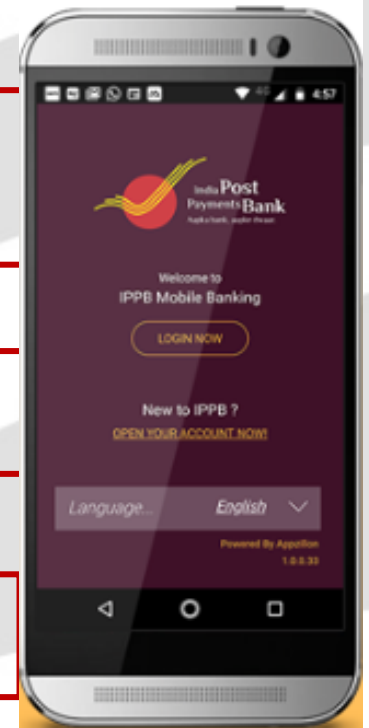
- **Payment with a bank card** that is stored on SE of LGM Card (a standard way using CVV/CVC code)
 - On supported payment gates payment card data can be read from the SE, encrypted and send to the merchant – without a need for customer to retype this data on mobile phone's screen
- **Payment from a bank account**
 - As a result of both-side authentication* – the customer has seamless access to his bank account without entering Account number, Customer ID (CIF) or registered mobile number. No need to use OTP
- **Payment from a wallet / using tokens**
 - As a result of both-side authentication* – the customer can use a simple MPIN to enter his wallet application and use all current services available from Mobile application without changes
 - To raise the security - cards on file (virtual cards) and tokens can be stored on SE of LGM Card

Raised volumes of m-commerce purchases with LGM Card

Use only MPIN to access Mobile application / Wallet

Seamless access to bank account

No need to enter card data during payment



* See details of both-side authentication with LGM Card on next slides

Strong Authentication with LGM Card

- SE of LGM Card can:
 - Generate and store digital certificates (key, client certificate, ID, token, PKI certificate)
 - Store biometrics data at client's side
- With LGM Card the service provider (SP) can launch both-side authentication based on secure keys that are generated, encrypted and stored inside a tamper-proof HW SE and to use this SE also to store biometrics data at client's side (not server side). This has more benefits over password/OTP methods:
 - **Higher security.** Public key authentication provides cryptographic strength that even extremely long passwords can not offer ¹⁾ and client certificates never leave tamper-proof HW SE thus offering a layer of security that API keys cannot provide. The private key of the client certificate is used to create a digital signature in every connection, and so even if the certificate is sniffed mid-connection, new requests can't be instantiated with it ²⁾
 - **Higher comfort.** It frees the users from remembering complicated passwords (or worse yet, writing them down). Public key authentication also allows automated, password less login ¹⁾.
 - It **allows users to implement single sign-on** across the servers they connect to ¹⁾
 - Public key **cryptography is included**
- Service provider has to set up PKI (Public Key Infrastructure) enabling remote management OTI (Over the Internet)

1) By SSH.com. <https://www.ssh.com>

2) By Dani Grant - *Introducing TLS with client authentication*, May 2017

Strong Authentication

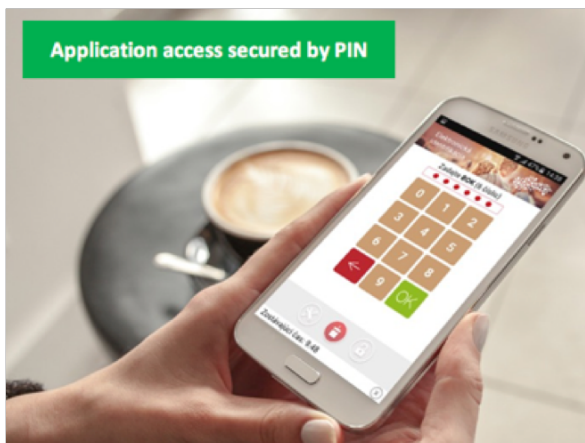
Benefits for users and SP

- LGM Card storing SP's key in the SE will **enable SP to control attempt of any user (his device) accessing SP's database with an option for blocking access to not authorized users**
- It will also enable **seamless process for customer** – automated, password less registration and login and **single sign-on across various SP's servers / services**
- Example of a use case:
 - Customer will enter Mobile application of the particular SP that can be protected by his password
 - The Mobile application of the SP will read data from the SE of LGM Card via the SP's API and send it to SP's server to confirm that LGM Card was issued by the SP to the particular customer
 - To use the service customer will only select the service on the device screen. The customer needs not to provide any additional data – e.g. password or e-mail and no need for confirmation SMS or OTP
- Once the SE of LGM Card stores individual customer's sensitive data, e.g. biometrics, bank card data or a token the **SP will need not to collect databases of sensitive data** or databases pairing PINs, e-mails and customer accounts
- These can **eliminate risk of violating customer's account by cracking his password or stealing databases comprising sensitive data**



Mobile ID Card

- **One SE of LGM Card can store ID card / Aadhaar including biometrics.** This will enable citizen to use ID card from his mobile phone – securely and under full control of Government
- **ID card can be issued in the same way like plastic chip ID cards.** Government can personalize secure chip of LGM Card in their current secure infrastructures. Each LGM Card can be personalized as ID card for a particular customer - under control of Government
- **Government can offer verification services**
 - Verify eID data stored on secure chip (on-spot and remotely)
 - Identify each customer (his mobile phone device) who is accessing governmental servers
 - Store and use electronic signature from a mobile device
 - Offer Governmental verification services to commercial entities
- **Payments for governmental services** - with bank card stored on SE of LGM Card
- **LGM Card can add security to Governmental Cloud based solutions**



Aadhaar seeding with LGM Card

- Usually customer can link his Aadhaar number to his existing bank account or other service by himself via multiple channels including - Internet Banking or mobile apps
- With LGM Card customer can input his Aadhaar number into LGM Card by himself via existing processes while securely storing Aadhaar data on the SE of the LGM Card. This will enable:
 - Aadhaar seeding with customer bank account or other SP service
 - Use Aadhaar number or Virtual ID without collecting databases of Aadhaar by SP
 - Seamless access to Aadhaar based SP services from a mobile phone
- Customers with no data connectivity usually using basic or feature phones can be served at SP branches providing them LGM Card and storing Aadhaar number and SP bank card on SE at the SP's branch
- Not-connected customers who will store their Aadhaar number on the SE of LGM Card can use their mobile phone to display the Aadhaar number on the screen of their mobile phone – and show it during Aadhaar based payments to a merchant

Secure Access with LGM Card

- LGM Card can be used by employees as a chip contactless employee card used from mobile phones
 - To access employee premises equipped with NFC readers
 - To access employee Intranet and bank systems
- The employee will tap his mobile phone to enter the door while this function can be integrated in Mobile application or it can be enabled as a shortcut from the phone's menu
- SE of LGM Card can generate OTP that the employee will have to enter into his company's PC to be able to login to Intranet and bank systems



Merchant App with LGM Card

- **Merchant App** is usually a cashless payment solution enabling merchant to accept payments for goods/services using various payment options, for example:
 - Transactions initiated by customer i.e. scanning a QR code and making payments in a push transaction mode
 - Transactions initiated by merchant i.e. accepting payments from the customer via Account Number + OTP, scanning customer QR card + OTP, Aadhaar Number + OTP
- LGM Card can be **used as Merchant card for the merchant's authentication**. SE can store digital certificate of approved merchant and enable him seamless authentication into Acquiring bank systems and simple access to his merchant bank account
- LGM Card (inserted inside a customer smartphone) can also **store Merchant Loyalty card including loyalty points and financial credential – securely on SE** and that can be used during purchases with registered merchants



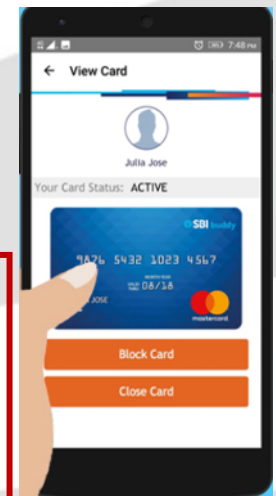
Mobile Wallet

with LGM Card

- Mobile Wallet is usually a pre-paid wallet or virtual card wallet (open or closed loop) and that enables many use-cases
- With LGM Card in his phone Mobile Wallet user can benefit from:
 - Make Sign Up and Sign In processes simple, secure and unified (same access to any SP online service)
 - Simplified top-up options inbuilt in the Mobile Wallet app:
 - from bank account – due to seamless access to SP’s Internet Banking without entering Internet Banking login credentials
 - from debit card (stored on SE of LGM Card) – due to no need to retype card data during recharge
 - Use Mobile Wallet also for contactless retail purchases
 - Simplify m-commerce with virtual card (stored on the SE of LGM Card)
 - Storing Virtual card data (number and CVV) on SE enables m-purchases without a need to retype card data on supported payment gates
 - SP will need not to manage SP database of any sensitive customers data




LGM Card can be a differentiator - enabling SP customers more convenience & security



Back-up Slides

Basic technical Features

- A standard microSD memory card with 4GB or 16 GB flash memory
- One or two Secure elements (SE)
- Embedded miniature NFC antenna (patented) and that works also under batteries and metal back covers
- ISO7816 contacts on the surface enabling contact personalization of the SE(s)
- Support for OS Android, JavaME, Windows Mobile
- Gen2 of the product supports also feature phones
- Certified by  as RuPay dual interface card, in July 2019




Form Factor	SDHC microSD card, Speed Class 10 (UHS-I)
Flash Memory	4GB (pilots), 16 GB (stock), 8GB or 16GB mass produced
Gen1 – Secure chips	<u>SE#1</u> : NXP J5C145, JCOP 2.4.2 R1, 145 KB EEPROM, MIFARE Flex® (4K) <u>SE#2</u> : NXP J5D081, JCOP 2.4.2 R2, 80 KB EEPROM, MIFARE® DESFire® EV1 8K
Gen2 – Secure chip	SE#1: e.g. IDEMIA, Pearl v5 (availability based on binding PO)
NFC Antenna	ISO 14443A, ISO 18092, Compliant with MIFARE®
Interfaces	Standard microSD interface, ISO 14443A, ISO 7816

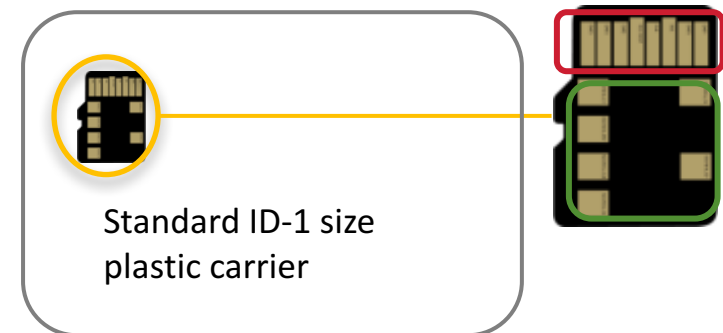
Personalization Options

- LGM Card has patented design of ISO7816 contacts placed on its surface
- Personalization can be done optionally as
 - **Contact personalization** (microSD card is embedded on ID-1 plastic carrier)
 - On Datacard machines
 - On a contact reader connected to PC (for instant issuing)
 - **OTI personalization** (microSD is inserted in a mobile phone)
 - Using TSM
 - **Contactless personalization** (microSD is inserted in a mobile phone)
 - Using contactless reader connected to PC (for instant issuing)

- Contact personalization according to

 specification

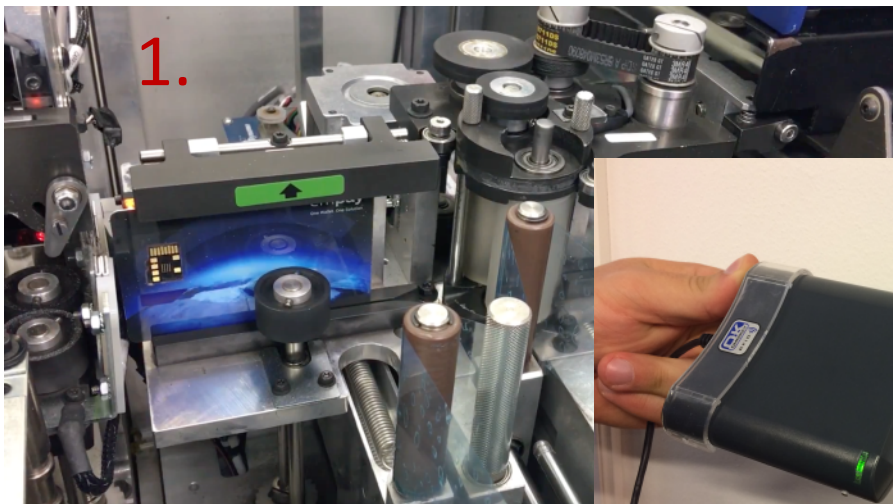
- Uses ISO 7816 contacts placed on the surface of the LGM Card card (marked in a green oval)
- Does not use the 8-pin normal microSD card contacts that connect the microSD card to a mobile phone (market in red oval)



Contact personalization can be a condition for SECURE loading of sensitive data on the SE, for example ID card or AADHAAR number

Personalization Examples

- LGM Card enables various forms of personalization:
 - **Contact personalization** using standard ISO 7816 contacts; using:
 1. **standard personalization machines** (e.g. Datacard) – video available at <https://www.youtube.com/watch?v=79cvXtx2uvc>
 2. **standard contact reader connected to PC**
 - **Contactless personalization** using:
 3. **standard contactless reader connected to PC** and while the microSD card is placed inside a mobile phone's sd slot



LGM Card Activation - Example

LGM Card is customer's device. We provide SecKeys and API to the Issuer /SP

1. Issuer personalizes microSD card's smart chip and distributes microSD cards to cardholders in plastic carrier in the same way like current bank cards
2. User takes microSD card out of the plastic carrier and inserts it into his phone
3. User downloads User interface application (UIA) over the air. [He can be navigated for card personalization and activation]. Now he is ready to use his phone for various services supported



4. **User can add 3rd party services gradually, as they are available.** User will download 3rd party application into his mobile phone and activate the service by a tap to 3rd party contactless acceptance device or Over-the-Internet (OTI) using TSM services

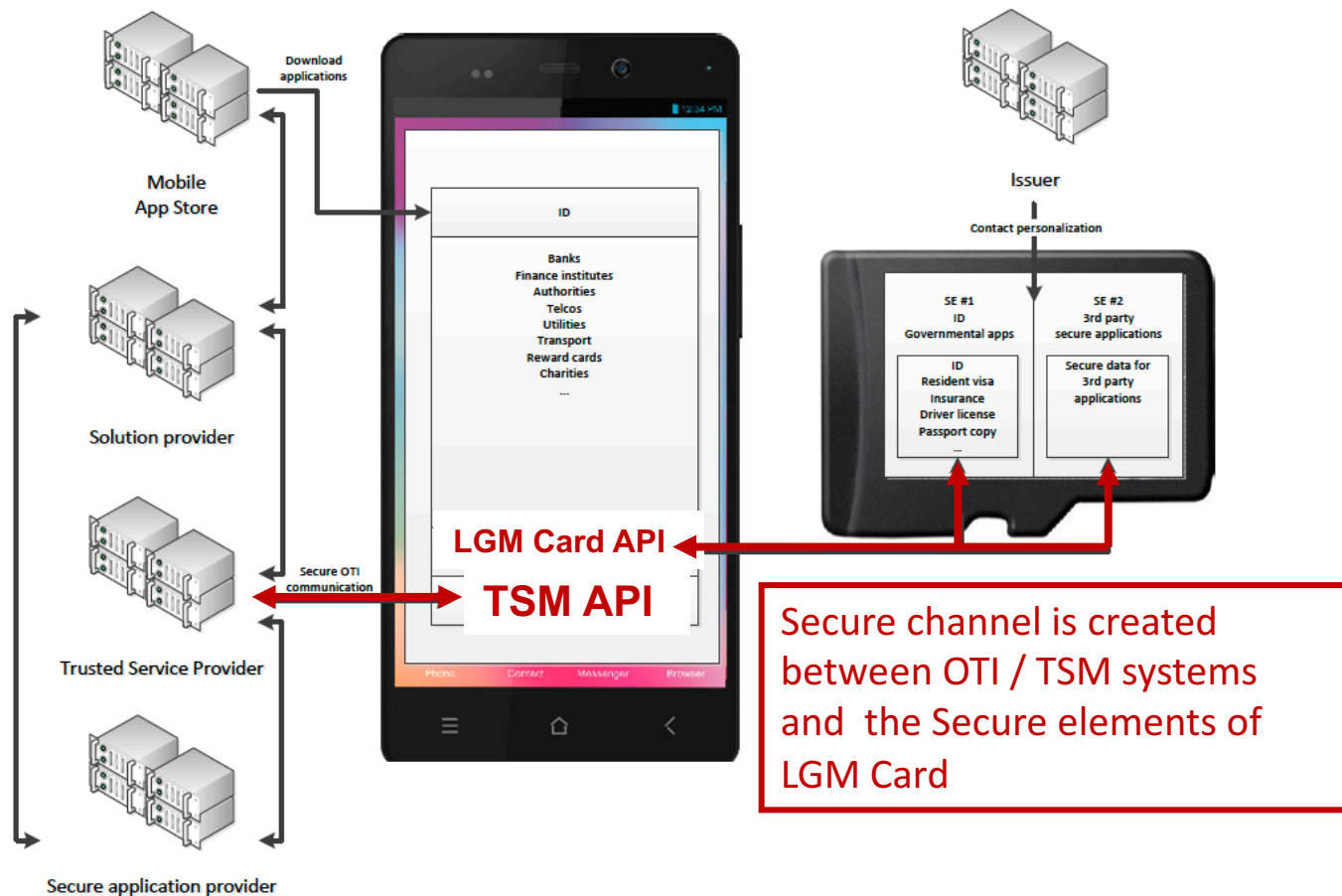
Basic Integration Requirements

- LGM Card requires basic integration with Card management system (CMS) and development or update of current Mobile application by adding options:
 - Using microSD card
 - Interface for tap&pay / tap&go use-cases
 - Interface for m-commerce payments
 - Top-up
- Optional can be a support for unified verification/authentication/authorization processes for various services (PKI, Clients certificates)
- For seamless purchases in m-commerce using bank card or token stored on SE – the online merchants or payment gateway have to support such payments with LGM Card
- No changes are required:
 - On contactless POS machines and POS acceptance network that currently accept c'less chip bank cards
 - For personalisation machines (e.g. DataCard) and in contact EMVCo personalisation processes
- SP can optionally develop and offer API to 3rd parties to integrate their services
- SP can potentially become TSM

OTI & TSM - Example

used for LGM Card life-cycle management

- Over the internet (OTI) systems enables remote life-cycle management of LGM Card with huge flexibility of adding new applications and serving many partnering solutions
- In the case that **SE is used to store EMVCo type of bank cards** a TSM system has to be deployed



Benefits for Banks

- Issuing bank can personalize secure chip of LGM Card as a normal EMV bank card. All transactions processed through the existing payment industry infrastructure and standard interchange fees will apply in a wide range of card-present transactions, including:
 - Contactless payments on a standard contactless POS
 - Card-based internet payments (using CVC, CVV code)
- Revenue streams that may cover the costs of issuing contactless smart microSD:
 - Typical revenue derived from serving as a deposit account
 - Interchange fees and IF revenue can be used to build a cash-back value proposition to the customer - driving sales
 - Increased usage of bank cards (No. of transactions) on contactless POS – using mobile phone typically for micro purchases
 - Online payment scenarios where it can be used for card-present transactions and for 3D secure using http(s) as an alternative to potentially costly SMS
- Secure access to Direct banking services
 - Internet banking. LGM Card can generate One –time password (OTP) and display it on mobile phone screen. Client rewrites OTP value manually
 - Mobile banking. LGM Card can be used as a secure storage of clients' certificates and enable automate, password less access to Mobile banking

Benefits for Token Solutions

- Although tokens brought high security to HCE the SE of LGM Card can add significant value
- Tokens and Vault servers are great target for hackers as:
 - tokens in most of current HCE solutions are delivered to the mobile phone and protected only by a software (tokens are stored in part of mobile phone's common memory – Trusted Execution Environment, TEE). TEE security has to be proven
 - to get the tokens it is necessary to connect to Vault server. Using the application is the weakest link that contains the information to authenticate to the back-end and to access to local tokens
 - Vault servers store huge amount of data that can be stolen. If bank cards data / tokens are stored on SE of individual users – no central database will have to be created
- LGM Card can be valuable for HCE and tokenization as it:
 - Provide non-repudiation and protection for identity theft and tokens (Store client certificate & tokens on SE)
 - Provide a hardware root of trust that could be preconfigured for the service
 - Ensure strong authentication to the HCE server, for example by using PKI and multi-factor authentication. Controlled access can raise protection against stolen databases of passwords from servers and eliminating risk of violating a customer's account
 - Ensure a great user experience

Control sensitive and big Data

- In current mobile solutions Card manager CM keys (enabling access to SE) are not provided to the Service Provider. In Apple Pay and Samsung Pay – phone vendors have control of SE. TEE (Trusted Execution Environment) is used by the device vendor to install his “network accessing” secure key management and other OS related security
- Using LGM Card the Service provider has full control of the hardware SE and NFC antenna capability. Card manager (CM) Keys enables him to control SE and to:
 - Store Private/ Public keys in SE
 - Store PKI certificate issued by selected CA (Certificate Authority) in SE
 - Verify / authenticate / authorize the user before allowing him for particular mobile service
 - Load sensitive data into the SE - also in the most secure, contact way
 - Collect data about customers shopping habits

Inline with security Standards

- EMV chip technology used in a secure infrastructure can significantly reduce fraud. EMV system has proved to be highly effective
- Since software/cloud has certain security risks, moving the SE into hardware provides more security
- In HCE (Host card emulation) mobile payments card data are placed in the cloud and HCE is an enabler that makes it possible for application residing in a mobile device to work in card-emulation mode. Tokenization adds security to HCE; but HCE and TEE security has to be proven
- LGM Card has embedded one or two Secure chips that meets Global Platform (GP) specifications. Presence of HW Secure chip enables the strongest HW authentication ¹ for
 - Physical storage of full card data on Secure element
 - Storage of Clients certificates enabling more secure access to Governmental Cloud, HCE or wallet servers and to store tokens
- LGM Card is inline with Government of India – Use of Aadhaar e-KYC service of UIDAI ²⁾

1) *Inline with PCI DSS Requirement 8.3, February 2017 and Gov. of India, Ministry of Electronics & Information Technology, ORDER No 2(94)/2017 – Cert-In-Pt.I, date:12.08.2017*

2) *Government of India Ministry of Communications Department of Telecommunications, File No.:800-29/2010-VAS (Vol.1), dated 12th June, 2018*