Introduction to EMV

EMV (named after Europay, MasterCard, and Visa) is a payment technology and global standard for secured payment processing using smart/chip cards. The user payment application resides on an embedded computer chip that can store secret information securely and can perform cryptographic processing. The EMV specification aims at ensuring worldwide interoperability and mitigating the risk to frauds by describing terminal behavior and communication protocols between the terminal and ICC. Presently the EMV specifications are maintained by EMVCo for EMV Contact, EMV Contactless, EMV Tokenization, EMV Card Personalization Specification etc.

There are two types of EMV transactions, mainly contact and contactless and the type is determined by how the chip connects with the acceptance terminal. In contact chip the chip must come in physical connection with the chip reader, so the chip is inserted by the customer to the POS terminal. In case of contactless EMV, the user either needs to tap the card or must bring the card within sufficient proximity of the card reader. The information then flows between the chip and terminal via NFC (Near Field Communication). In either case the terminal provides power to the chip to enable its functionality.

1. EMV Transaction Flow

A EMV transaction may differ for contact and contactless ICC. This section provides more information about the various steps taking place in both cases:

1.1 Contact ICC Transaction Flow

A traditional EMV ICC transaction consist of the following steps each explained in more detail as under:[1]

1. **Application Selection:** There can be more than one application residing on the chip and the terminal makes use of SELECT Command to select an PSE, DDF or ADF corresponding to the file name or AID. The application compatible with both card and terminal with highest priority is chosen. If no common application is present, the transaction is declined.

2. **Initiate Application processing:** This is done via the GET PROCESSING OPTIONS Select/Response APDU (Application protocol data unit) command. The ICC responds with AIP (Application Interchange Profile) & AFL (Application File Locator). AIP specifies the application functions that are supported by the application in the ICC & AFL consists of the list of files and related records for the currently selected application.

3. **Read Application Data:** The READ Record Command is used to read necessary data from chip (PAN, Application Expiry date etc.).

4. **Card Authentication Method (CAM):** There are 3 types of offline Data Authentication methods-SDA, DDA & CDA that can be performed, but the method used depends on the abilities of the terminal and card. Online-only terminals are not needed to support offline data authentication. All other terminals must support both SDA and DDA and may also support CDA. SDA - Static Data Authentication of the card data to verify that it has not been modified. DDA - Dynamic Data Authentication of card and terminal data to verify that the card application and data are genuine. CDA - Combined DDA and Application Cryptogram Generation. The results of CAM are recorded in TVR & TSI.

5. **Processing Restrictions:** The Processing Restrictions comprises the following compatibility checks:

   (a) **Application Version Number:** The application within the terminal and ICC shall maintain same Application Version Number assigned by the payment system.

   (b) **Application Usage Control:** The Application Usage Control indicates restrictions limiting the application geographically or to certain types of transactions.
6. **Cardholder Verification Method (CVM):** ICC has a CVM list that includes CV rules under which that CVM should be applied. The various types of CVM method supported for contact EMV card are: Offline PIN, Online PIN, Signature, No CVM & other.

7. **Terminal Risk Management:** The terminal ensures that transactions are periodically send for online authorization to protect against frauds that are not identified in an offline environment. In doing so the terminal makes the following checks:

   (a) **Floor Limit checking:** The total amount authorized by the terminal for a PAN is checked against the terminal floor limit and if the amount exceeds the terminal floor limit, the transaction is send online for Authorization.

   (b) **Random Transaction Selection:** Selects random transactions for online processing. It include a bias for higher amounts transactions to go online more often.

   (c) **Velocity Checking:** The terminal checks counter values (Lower Consecutive offline limit, Upper consecutive offline limit) in the ICC to decide whether to go online.

8. **Terminal Action Analysis:** The terminal will analyse the results of the previous authentication and risk steps stored in the Terminal Verification Results (TVR) data element & the issuer action code. The terminal will then request an Application Cryptogram (AC) using GENERATE AC Command to the ICC. The following Cryptogram can be requested by the terminal:

   (a) **Application Authentication Cryptogram (AAC):** Transaction should be declined offline

   (b) **Authorization Request Cryptogram (ARQC):** Transaction should go for online processing.

   (c) **Transaction Certificate (TC):** Transaction should be approved offline.

9. **Card Action Analysis:** The card performs risk management of its own based on issuer rules and decide to complete a transaction online or offline or reject the transaction in response to GENERATE AC Command by returning a ARQC, an TC, or an AAC respectively to the terminal.

10. **Online processing:** Once the card issues an ARQC, an online authorization request transaction is forwarded to the acquirer with original Data elements and application selected. The acquirer then forwards the transaction to the issuer after pre-validation steps. The issuer will then validate the cryptogram and chip data received and will generate an ARPC (Authorization Response Cryptogram) either to approve or decline the transaction.

11. **Second Terminal Action Analysis:** If no valid response is received from the host during online pro-
As Issuers have now migrated from Magnetic stripe to EMV, supporting both contact and contactless payments, they want to support NFC-enabled mobile payments solutions. The major benefits for issuers to adopt contactless chip are:

**Improved customer experience:** For Contactless transactions, customers don’t need to leave their cards inserted for long times during the entire time of approval nor is there a possibility that the card is removed at a wrong time thus making the payment process simpler and quicker for users. Also as users are getting accustomed to Mobile payments such as ApplePay, there is a possibility that the users would like to use their cards for contactless payments too. [4]

**Increased Revenue & Utilization:** The Contactless payments are targeted towards low-value transactions that are cash transactions today. Infact studies have found that contactless payments may help drive top-of wallet behaviour with more spending being recorded with a contactless card. They also give way to new opportunities in the open bankcard payment systems that are now for example used in transit payment systems. For example, in the metropolitan area in Utah, bus riders use their Visa, MasterCard or American Express branded contactless bankcards to “tap on” when they board and “tap off” when they leave their buses [5].

**Security:** Contactless payments maintain the same security features as contact payments. Also if EMV is combined with tokenization like in case of ApplePay, cross-channel frauds could be prevented even in case of data breach.

**Straightforward dual-interface Card Deployment:** It is relatively easier for the issuers to make dual-interface cards as both contact and contactless cards share the same Payment Applications and Key Management for Cryptography making them much more affordable.

**Global Interoperability:** The earlier implementation of contactless cards in U.S. were not interoperable globally. But the NFC enabled EMV transactions are globally accepted and a frequent traveler will benefit and not face issues using these dual-interface cards.

### 3. Contactless ICC: Key Concerns

#### 3.1 POS terminal manufacturers considerations

When the POS terminal manufacturers migrated to POS equipment supporting EMV, most of them added the ability to perform contactless EMV transactions too in their device.[6] POS terminal providers noted that many of the newer terminals are upgradable with software to enable NFC payment acceptance, but most of the older terminals are not software upgradeable. Having said that the migration from contact to contactless will be impacting the POS terminal manufacturers as listed below:

**Advancement in POS terminal:** POS terminal must be upgraded to accommodate NFC Enabled EMV transactions. POS application providers need to integrate the contactless reader application software into their merchant POS software and configure the contactless reader and POS software with the...
specific device and payment networks’ functional requirements. If the POS terminal manufacturer are producing magnetic stripe POS devices, then the entire device would require an upgrade – both hardware & software upgrades.

**Device Testing & Certification:** Additional hardware and software testing and certification of the POS equipment may be required to ensure the devices are compliant with EMV, NFC and PCI DSS standards.

**CVM Method Support for Mobile Payment (Optional):** If the POS terminal should accept mobile transaction then maybe they will require a kernel update to support CDCVM.

**Terminal Capabilities Settings:** Contactless terminals have capability settings maintained through configuration files. It is necessary that these settings reflect only the capabilities for which the terminal is certified or approved. For example, if the application is approved for MSD contactless but not EMV contactless, the capability settings should reflect that restriction. If a merchant updates the terminal to include a certified EMV contactless application, the terminal capability settings should also be updated.

### 3.2 Issuers considerations

Issuers considering to support contactless chip transactions will examine the following implementation considerations:

**Issuance & personalization:** Issuers must provide or procure dual-interface EMV cards by consulting their card providers. If the issuer supports contact EMV, then no major updates to the personalization equipment are required except for including additional contactless parameters.

**Issuer processor Contactless support:** The issuer may want to check that their switching issuer processor platform supports contactless EMV properly. The issuer may also need to update authorization processing and risk management rules to accept EMV contactless transactions.

**Educating the Cardholder:** The cardholder must be educated that their new card has dual functionality and must be given enough information about how to use it at the POS machines. They must also be highlighted with the benefits of contactless payments.

**Testing & Certification:** Issuers may want to conduct rigorous testing and set evaluation criterias for these dual-interface cards so that they comply with EMVCo, ISO 14443 standards to ensure that card hardware and software operate as specified and intended.

### 4. Conclusion

This memo describes the adoption of EMV ICC payment technology worldwide benefiting the consumers, merchants, and issuers in combating frauds and providing flexibility and risk management capabilities to the issuers throughout the transaction lifecycle. Contact ICC have been widely adopted but the implementation of contactless/dual-interface cards have always been in question due to the challenges contactless cards may provide to the merchants, acquirers & issuers. But as customers are moving towards NFC-enabled mobile payments, there is an increasing demand from customers towards faster, simple and convenient forms of payment methods.

Issuers and mobile wallet providers-Apple and Samsung have already taken the first step toward driving broader contactless acceptance. However, due to the scarcity of contactless POS terminals, there may not be enough merchant acceptance to justify issuing dual-interface cards. The memo therefore aims at specifying the benefits and concerns of issuers & POS terminal manufacturers in supporting the next generation contactless payment technology. By addressing these implementation concerns, it will benefit everyone by enabling greater checkout speed for merchants and by providing a top of wallet advantage for issuers.

### References


