In this Document:

Contact Chip – General
Frequently Asked Questions (FAQ)

1. **What is the relationship between the EMV Chip Specifications and ISO/IEC 7816 standards? What differences are there, and why do they exist?**

   The EMV Chip Specifications are based on, and are a subset of, the requirements in the ISO/IEC 7816 series of standards. However, ISO/IEC 7816 is a series of standards rather than an implementation oriented specification such as EMV, and a terminal supporting all of its requirements would be quite complex. The EMV Chip Specifications should be read in conjunction with the ISO/IEC 7816 standards. However, if any of the provisions or definitions in the EMV Specifications differ from the ISO/IEC standards, the EMV Specifications shall take precedence. More specifically, ISO/IEC 7816-3 specifies the card/terminal interface, whereas EMV specifies the card and terminal requirements separately - this makes a direct comparison of the two documents difficult and not always meaningful. From a terminal manufacturer's point of view, a comparison of the requirements in EMV Book 1 with the ISO/IEC 7816-3 standard should reveal the differences that need to be taken into account. EMVCo does not have such a comparison available. With regards to ISO/IEC 7816-4, which specifies the organization, security and commands for interchange, the EMV Specifications use some of the commands specified, but not all options are necessarily supported. In addition to the ISO/IEC 7816-4 defined commands, EMV has also defined additional commands that must be supported by cards and terminals.

2. **What is the purpose of the EMV Specifications?**

   The purpose of the EMV Specifications are to facilitate the worldwide interoperability and acceptance of secure payment transactions. The EMV Chip Specification describes mandatory and optional terminal behaviour and the interface between the terminal and card. Card functionality beyond this card to terminal interface is not described. Supplemental specifications from the Payment Systems (or from EMVCo for Common Payment Application cards) provide requirements for internal card processing of the transaction. These card specifications and additional vendor requirements are required along with the EMV Chip Specification to build a complete

card. Additional terminal specifications are also needed for a complete terminal design to cover areas that are unrelated to the card-terminal interface such as the terminal to host interface.

3. **How do the EMV Specifications fit in with other international standards?**

   The EMV Specifications are based on various standards (such as ISO 7816, ISO 14443, and ISO 8583) and define the physical, electrical, data and application levels for financial payment transactions. Through payment systems representatives, EMVCo promotes and complements the ongoing standardisation efforts by vigorously contributing to the ISO standards drafting process in order to ensure continued compatibility between the ISO standards and the EMV Specifications. On this website, EMVCo makes available to the public many online resources such as final and published versions of EMV Specifications, bulletins and application notes, type approval-process documents, and approval lists. Through payment systems representatives, EMVCo promotes and endeavours to harmonise the standardisation work by actively contributing to the ISO standards drafting process in order to ensure ongoing compatibility between the ISO standards and the EMV specifications.

EMVCo & Biometrics
Frequently Asked Questions (FAQ)

Background: In 2016 EMVCo worked to integrate biometrics as a cardholder verification method (CVM), allowing various biometric verification methods to be integrated into the EMV contact payment flow with limited impact on the acceptance infrastructure. The work supports EMVCo's goal of interoperability by optimising the existing EMV Integrated Circuit Card Specification for Payment Systems (EMV Chip Specifications) to reduce the impact of implementation.

1. **Why is EMVCo involved in this biometric activity?**

   The payments community has been exploring how it can support biometric verification methods, such as fingerprint, voice recognition and facial recognition, to meet this growing market requirement

   EMVCo also recognises that regulatory activities, such as the European Directive on Payment Services 2 (PSD2), calls for strong authentication methods in payments and biometric verification is one means of achieving this.

   While there are already many implementations using biometric verification, to date they have not been globally interoperable. The payment industry recognises that if

the biometric is captured on the merchant POS terminal or ATM and is to be matched with data on the consumer's chip card or server, the transmission of the biometric templates must leverage a universally accessible approach to reach interoperability needs. This transmission must also be done in a secure manner.

Terminal and ATM manufacturers, alongside others within the payment community, acknowledged that updating existing EMV Chip Specifications would help to offer a global framework with minimum impact on the current contact payment flow.

2. At a high level, what is EMVCo doing in this area?

Firstly, it is important to note that the scope of EMVCo in this area is focused specifically on updating the EMV Contact Chip Specifications to allow the use of existing biometric methods as an EMV cardholder verification method (CVM).

The EMV 4.3 Contact Chip Specification supports the acceptance of four cardholder verification methods (CVM): offline PIN, online PIN, signature and no CVM. The specification has been modified to now also support both match-on-card and match-on-server solutions by re-using the EMV concepts and logic of offline (enciphered) PIN and online PIN verification.

The enhancements provide an interoperable mechanism to pass the biometric data from the reader on the POS terminal / ATM to the card in a secure manner, and for the card to return the 'match' result to the terminal in a secure manner. Similar to online PIN verification, the verification of the biometric template can also happen on a remote server. Note that this is an implementation option and EMVCo does not define the mechanism of the biometric verification (or matching). That is outside of EMVCo's scope.

This work also includes the definition of an EMVCo process to establish a Biometric Solution ID and will define the associated registration process. This is a unique number which identifies the solution supported on a card and enables the ATM / POS to recognise that it also supports the same solution.

3. What does this mean in reality?

The updates to EMV 4.3 Contact Chip Specification enable the payment community to add a biometric verification option into the current EMV contact flow with limited impact. This means that when the cardholder inserts their EMV chip card into the terminal, only in the case where both the terminal and the card are enabled to support the biometric CVM and have compatible biometric modalities, would a biometric capture be attempted. In this instance, the terminal would prompt the cardholder to offer a form of biometric for verification, for example, request a fingerprint image on the POS terminal.

4. **What aspects of the EMV 4.3 Contact Chip Specification have been updated?**

   In order to achieve interoperability, EMVCo defines the new CVM for biometrics and a new variant of the 'verify' command which includes how the template is secured, and the coding of the biometric-related values of terminal verification results. The updated EMV Specification also supports the use of issuer script commands to load, change, or unblock the templates after card issuance.

   The updates relate to EMV Book 2 – Security and Key Management, Book 3 – Application Specification and Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements.

5. **Do all existing POS terminals and ATMs need to be updated to align with the specification update?**

   No. The specification has been developed for full backwards compatibility and optional support of biometric-based verification. For example, if a card supporting a biometric CVM is inserted into a terminal that does not support this functionality, the transaction will be performed using another verification method. This ensures the co-existence of both cards and terminals with and without biometric CVM capability, with minimal risk of interoperability issues.

6. **Will EMVCo's work be focused on one particular biometric modality such as fingerprint?**

   No. The EMV 4.3 Contact Chip Specification supports several types of biometric CVM: palm, voice, fingerprint, facial and iris.

7. **When do you expect this functionality to be available for implementation?**

   The draft specification bulletin was published in November 2016 on the EMVCo website. Following market input, EMVCo aims to release the final specification updates in Q2 2017.

8. **Is this the only biometric activity that EMVCo is working on?**

   No. EMVCo is working with the FIDO Alliance to determine how EMV payment use cases can be incorporated into FIDO Alliance's technical standards. The focus of this partnership is related to shared cardholder device CVM, for example, using the same biometric method to both 'open' a smartphone and verify a payment made with it.