

[X] Public — [] Internal Use — [] Confidential — [] Strictest Confidence

VOLUME TERMINOLOGY

The Volume describes functional requirements applicable to **Card transactions** which result in the provision of the **Card Services** to the **Cardholder** and **Acceptor**. The Card Services described in the Volume are grouped as follows:

- Payment Services:
 - Payment
 - Refund
 - Cancellation
 - Pre-Authorisation Services
 - Deferred Payment
 - No-Show
 - Instalment Payment
 - Recurring Payment
 - Quasi-Cash Payment
- Cash Services:
 - ATM Cash Withdrawal
 - Cash Advance
- Card Inquiry Services:
 - Card Validity Check
 - Balance Inquiry
- Card Electronic Transfer
 - Card Funds Transfer
 - Original Credit
 - Prepaid Card - Loading & Unloading

Card transactions are performed based on Card Data which either is retrieved from the Cardholder's **Physical Card, Virtual Card** or **Consumer Device** during the Card transaction or is **Stored Card Data** which has previously been stored by the Acceptor.

The Volume uses the term **Cardholder Environment** to denote the source from where Card Data is retrieved when performing a Card transaction, i.e. Physical Card, Virtual Card and Consumer Device. The source of and method by which Card Data is obtained is referred to as **Acceptance Technology**. Refer to Table 3 in Book 2 of the Volume for a list of Acceptance Technologies and the Cardholder Environment(s) they are applicable to.

The environment where a Card transaction is conducted in the Acceptor's domain is called **Acceptance Environment**. The Volume describes two Acceptance Environments:

- **Physical POI**
- **Remote POI**

The POI (Point of Interaction) is the initial point where Card Data enters the Acceptor's domain. It consists of hardware and software.

A Physical POI (also referred to as a Physical/EMV Terminal) may be **Attended** (including Semi-Attended) or **Unattended**. A Physical POI is used to perform so called **Local Card transactions** at the card Acceptor's premises. The term "Local" was introduced to denote the complement of "Remote".

So, Local Card transactions are normally initiated by the Cardholder using a Physical Card (Contact or Contactless) or a Mobile Contactless Payment Application on a Mobile Device.

So, Local Card transactions are normally **Cardholder Present** and **Card Present** transaction, that is, during the transaction, the Cardholder is present at the card Acceptor's premises or at an Unattended Terminal, and the Physical Card or Mobile Device is physically presented to the Acceptor.

But Local Card transactions are not only Cardholder Present and Card Present transactions. For Pre-Authorisation Services, No Show, subsequent transactions of Instalment Payments and Recurring Payments, Local Card transactions may be **Cardholder Not Present** and **Card Not Present** transactions initiated on the Physical POI at the card Acceptor's premises by the Acceptor based on Stored Card Data.

A Virtual POI is used to perform Remote Card transactions. A **Remote Card transaction** is a Card transaction which is **e-commerce**, **m-commerce** or **MOTO**:

- e- and m-commerce transactions are normally initiated by the Cardholder using a Consumer Device and conducted via a Virtual POI to buy products and services over the internet.

If the Consumer Device is an **Electronic Device**, this is referred to as an e-commerce transaction.

If the Consumer Device is a Mobile Device, this is referred to as an m-commerce transaction.

- MOTO Transactions are conducted in the Acceptor's environment and initiated by the Acceptor, normally using Manual Entry with the Cardholder interacting remotely for MOTO.

A Physical POI, configured to handle Card Not Present transactions or a Virtual Terminal may be used to process the Card Data.

For some Card Services, Remote Transactions may be initiated by the Acceptor based on Stored Card Data, e.g., No Show, subsequent transactions of Instalment Payments and Recurring Payments.

A Virtual POI includes a Payment Page which may be presented to the Cardholder from either a Payment Gateway or the Acceptor's website. The Virtual POI may also facilitate (redirection) services to support Authentication of the Cardholder by the Card Issuer for e-and m-Commerce.

A **POI Application** is an application consisting of software and data used to perform Card Services. Depending on the architecture of the POI (Physical or Remote), the POI Application may be implemented on one component or distributed on several components. The POI Application may be integrated with a sale system or may be standalone.

According to the Volume, POI Application implements **Functions** which are executed to process Card Services. Examples of these Functions are **Selection of the Application, Card Authentication, Cardholder Verification**.

Card Authentication Methods are used to perform the Card Authentication Function. Examples of Card Authentication Methods are **Combined DDA/Application Cryptogram Generation (CDA)** (for Local and Remote Card Transactions), Dynamic Authentication - One Time Password (OTP)* (for Remote Card Transactions).

Cardholder Verification Methods are used to perform the Cardholder Verification Function. Examples of Cardholder Verification Methods are **Online PIN** (for Local Card Transactions), **Biometrics on Consumer Device** (for Local and Remote Card Transactions), **Online Personal Code** (for Remote Card Transactions).

¹ This Card Authentication Method is used for e- and m-commerce and may use EMV authentication methods.