QR Code Specification
Consumer-Presented
Version V1. 1

October 2021

Confidential and Trade Secret Materials

This document contains sensitive, confidential and trade secret information and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.
The policies, procedures, and rules in this specification are subject to change from time to time by American Express Global Network Services.

Table of Contents

List of Figures

List of Tables

1 Revision History

Version	Date	Changes
1.0	February 2019	Initial publication
1.1	DecemberOctoberOctober 20210	• Moved EMV Data Field Application Interchange Profile (AIP) from section 4.7 to section 4.5(Tag 82), updated the presence requirement from conditional to mandatory and updated the value to a fixed value • Moved Terminal Verification Results (TVR) from section 4.7 to section 4.5, updated the presence requirement from conditional to mandatory, and added timestamp requirement for value requirement • Adjusted the presence requirement for the data elements listed in section 4.7, same in section 5.2.5 • contains a specific known value for CPQR transactions - The specific default value added is 'FFFF' for AIP in 4.7.1 • Adjusted default value for Amount, Other in from section 4.7.3 • Adjusted default value for Terminal Country code from section 4.7in 4.7.4 • Added timestamp requirements for Terminal Verification results in 4.7.5 • Adjusted default value for Transaction Currency Code in from section 4.74.7.6 • Repurposed TVR use for CPQR Code Timestamp Setup in 5.2.5.3, and renamed instances of CPQR Code Expiry Timestamp to CPQR Code Timestamp • Updated EMV Cryptogram input data table in 5.2.5.4 with new AIP and TVR value notes • Updated Consumer Presented QR data format table in 5.3 with new AIP and TVR value details • Adjusted and new default values added to QR Data to Bit 55 Authorisation message mapping in table 5.4 • Update the description of Unpredictable Number in section 2.6 and section 4.5 • Minor editorial corrections

2 Introduction

A QR Code® is a type of matrix bar Code containing data that can be optically machine read.

This specification includes:

- The data format and contents of the Consumer-Presented QR Code
- Cardholder Verification Method (CVM) requirements for American Express QR payments
- Generation of the QR Code for QR source devices
- Performance and Security requirements for the QR source device
- Capture and processing of the QR Code for QR reading devices
- Performance and Security requirements for the QR reading device

2.1 Scope

The *American Express Global Network QR Code Specification – Consumer-Presented* ***should*** be read in conjunction with the EMV® QR Code Specification for Payment Systems - Consumer-Presented Mode [EMV-QRCPS].

The primary objective of this document is to describe the ***mandatory*** and ***optional*** functionality required when implementing a QR Code payment product.

EMV publications may be obtained from the EMVCo website at www.emvco.com.

2.2 Audience

This document is primarily intended for use by payment application developers for Cardholder devices (Mobile developers) and Merchant devices (Terminal developers).

It may also be used by testing facilities, Issuers of American Express payment products, Acquirers, American Express personnel and mobile wallet and system developers seeking a technical understanding of the range and detail of functions available on systems supporting QR Codes.

2.3 Reference Material

Reference citations in this guide are shown as labels within square brackets.

Full details of the reference documents used in this guide are given in the table below:

Table 2-1: Reference Documents

Term	Description
[EMV-QRCPS]	EMV® QR Code Specification for Payment Systems - Consumer-Presented Mode, Version 1.0, July 2017
[AEBOP]	American Express Business and Operational Policies
[AEHCESC]	American Express HCE Security Considerations
[ISO/IEC 18004]	Information technology—Automatic identification and data capture techniques - QR Code bar code symbology specification
[ISO 18245]	Retail financial services—Merchant category codes
[ISO/IEC 13239]	Information technology—Telecommunications and information exchange between systems—High-level data link control (HDLC) procedures
[ISO 3166-1 alpha 2]	Codes for the representation of names of countries and their subdivisions—Part 1: Country codes, using two-letter country codes.
[ISO 4217]	Codes for the representation of currencies and funds
[ISO/IEC 7816-4]	Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange
[ISO 639]	Codes for the representation of names of languages—Part 1: Alpha - 2 Code
[EMV Book 4]	EMV Integrated Circuit Card Specifications for Payment Systems - Book 4 Cardholder, Attendant, and Acquirer Interface Requirements
[Unicode]	Unicode Standard, specifically the UTF-8 encoding form. For more information, please check: http://www.unicode.org/versions/latest
[RFC 4648]	Base-N Data Encoding standard

2.4 Notation

The following notation is used throughout this document.

Table 2-2: Notation Table

Term	Description
"00"	When referencing characters to be included in the Consumer-Presented QR Code, the characters will be enclosed in double quotes.
'0' to '9' and 'A' to 'F'	Hexadecimal Notation. Values expressed in hexadecimal form are enclosed in single quotes ''. Spaces may be inserted into hex values, to add clarity and make longer values more readable, for example '00 01 02 03',
Mandatory requirements	Highlighted through the use of the words ***must, shall, mandatory,*** or ***mandate(s)***
Options	Highlighted through the use of the words ***Optional*** or ***may***
Recommendations	Highlighted through the use of the words ***should*** or ***recommend(s)***

2.5 Use of Terms

In this document the term "Reading device" refers to a Merchant device such as a Point of Sale (POS) Terminal or mobile phone operating as a QR Code reader.

This may be a camera equipped mobile phone for capturing optical QR codes but does not exclude other methods of transferring the data contained in QR codes.

The term "QR reading application", refers to a software application running on the reading device to provide the functionality of a Global Network QR payment product.

The term "QR Source" refers to a method of displaying a QR Code; it may be a Cardholder's device such as a mobile phone hosting a payment application capable of displaying a QR Code.

The term "QR source application", refers to a software application running on the source device of a Cardholder.

2.6 Acronyms and Abbreviations

Table 2-3: Acronyms and Abbreviations

Term	Meaning
AC	Application Cryptogram. A secure data element generated by the Card across a defined set of Transaction data to enable the Issuer to verify the authenticity of an Authorization or settlement request.
Acquirer	An American Express Entity which has, or any other Person Authorized by an American Express Entity which has, a contract with an S/E pursuant to which: A Cardholder/Cardmember is entitled to charge purchases of goods or services at such S/E by means of a Card, and the S/E agrees to transfer such charges to the Acquirer.
AID	Application Identifier. A value defined by [ISO 7816-5] and used to identify the application to the Terminal.
AIP	Application Interchange Profile
an	Alphanumeric
ans	Alphanumeric Special
Application Selection	A Terminal deciding the application payload from the QR it will use for payment processing.
Application Specific	Payment data not interpreted or used by the POI directly
ATC	Application Transaction Counter. A counter maintained by a payment device that is incremented by one every time that device performs a Transaction.
ARQC	A type of Cryptogram indicating that the device wishes the Transaction to go Online. (*Mandatory*)
ATC	Application Transaction Counter
Authorization/Authorized	A Merchant obtaining an Approval for a Transaction or an Issuer's approval of a Transaction to a Card Account number range assigned to the Issuer
Authorised Processor	A third-party company that has been certified by AEGNS to perform processing services on an Acquirer's behalf.
C	Conditional
CA	Certificate Authority
CDCVM	Consumer Device Cardholder Verification Method. The process by which a payment device verifies the Cardholder/ Cardmember.

Term	Meaning
Cardholder Verification	An EMV defined term. The process by which a payment device or a payment device and a Terminal verify the Cardholder/Cardmember.
Cardmember	A Person who has entered into an agreement and established a Card Account with any Issuer, or whose name appears on a card. Also known as Cardholder.
Contactless	A term used to describe a Transaction environment in which the Card is enabled with a radio frequency chip to communicate with a Radio Frequency (RF)-enabled POS device to initiate a Transaction.
Cryptogram	Security data created by the payment device or Issuer systems and used to validate a Transaction or Authorization response.
EMV	A set of payments technology specifications.
EMVCo	EMVCo LLC, the organization that manages the EMV specifications and the approval process for payment devices and Terminals. See emvco.com.
Expresspay	Expresspay is a program within American Express for facilitating Contactless Transactions between a payment device containing an Expresspay application and an Expresspay-enabled POS device.
HCE	Host Card Emulation
IAC	Issuer Action Code
ID	Identification
ISO	International Standards Organization
Issuer	Any entity (including, without limitation, American Express and American Express Entities) Authorized by American Express or an American Express Entity to issue a payment device and to engage in the card issuing business
Implementers	The collective term for: Terminal Vendors; Merchants; Acquirers or Authorized Processors charged with Implementing American Express Contactless NFC acceptance at the POS
LUPC	Limited Use Payment Credentials
MAC	Message Authentication Code
Cardholder Verification	An EMV defined term. The process by which a payment device or a payment device and a Terminal verify the Cardholder/Cardmember.
Merchant	A Merchant (also known as “Service Establishment”). Any Person that has entered into a contract with an Acquirer wherein such entity agrees to: i. Permit any Cardholder to charge purchases of Goods and Services at or from such entity by means of the Card and ii. Transfer such Charges to an Acquirer

Term	Meaning
mPOS	Mobile Point of Sale
M	Mandatory
n	Numeric e.g. n 2 means two numerical digits
O	Optional
Offline	When a Transaction is performed without the Terminal connecting to the Acquirer
Online	A Transaction that is sent to the Acquirer prior to Transaction completion
PAN	Primary Account Number
PAR	Payment Account Reference
Payment System	A party operating a payment card network
POI	Point of Interaction
POS	Point of Sale, also see Terminal
POS Application	Software residing in the Terminal or POS which implements the business requirements and functionality beyond the scope of the Payment System specifications. This will include local market requirements and host communications protocols
POS Data Code	Point of Service Data Code. A series of codes that identify the Terminal capability, security data, and specific conditions present at the time a Transaction took place at the point of service
Private Key	A cryptographic key used in asymmetric cryptography. In order to verify the authenticity of a communication that one party has generated with a Private Key, the second party needs only have the first party's Public Key. Private Keys ***must*** be stored securely
Processor	A party that processes American Express Transactions on behalf of Merchants, Acquirers, or Issuers
Public Key	A cryptographic key used in asymmetric cryptography. In order to verify the authenticity of a communication that one party has generated with a Private Key, the second party needs only have the first party's Public Key. Public Keys may be freely distributed
Public Key Certificate	This is a Public Key, signed with the Private Key of a third party. This enables anyone who has the Public Key of that third party to be able to verify and trust the Public Key held in the certificate
QR Code	Quick Response Code

Term	Meaning
RFU	Reserved for Future Use
Secret Key	A Cryptographic key used in symmetric cryptography. In order to communicate securely using symmetric cryptography two parties ***must*** both share the same Secret Key. Secret Keys ***must*** be stored securely
S	String
Terminal	A payment device capable of accepting American Express Card products for payment for goods or services
Transaction	A Charge, Credit, Cash Advance (or other cash access), or ATM Transaction completed by the means of a Card
TRID	Token Requestor ID
Unpredictable Number	A randomised number generated and used by the QR Source Application device and used by the card in AC generation
var.	Variable

3 Overview

The Consumer-Presented QR Code product consists of a mobile payment application on a consumer's Mobile Device, such as a phone or wearable.

When the consumer wishes to pay a Merchant, a QR Code is generated on the consumer's Mobile Device.

This is scanned at the Merchant Point of Interaction (POI) by traditional Point of Sale (POS) equipment or the Merchant's Mobile Device (mPOS).

The generation of the data contained in the consumer- presented QR Code, is based on existing Host Card Emulation (HCE) techniques.

The QR Code contains standard EMV data elements, along with additional data. The EMV data, transferred to the Merchant during the scan, is submitted for Authorization and Settlement using existing EMV fields within the ISO messages supported by American Express Global Network Services.

The EMV data within the QR Code contains a cryptogram to authenticate and protect the Transaction.

The methods used to generate the cryptogram are based on existing HCE methods. A set of Limited Use Payment Credentials (LUPCs) are downloaded to the consumer's device containing keys that are unique to each Transaction. The use of LUPCs allow Transactions to be secure and does not rely upon Online connectivity if no data connection is available on the consumer's device.

The main stages of a consumer- presented QRC Transaction are:

- LUPC Replenishment (Mandatory)
  - Before any QR Transactions can take place, the LUPC ***must*** be downloaded to the consumer's Mobile Device to be used in parallel with other device payment credentials (i.e. Card data). The LUPCs are individual payment keys, unique to each Transaction. See Section Limited-Use Payment Credentials (LUPCs).

- Cardholder Verification (Mandatory)
  - Cardholder Verification is ***mandatory***. This may take the form of the consumer unlocking their device by password/passcode or biometric (Consumer Device Cardholder Verification Method (CDCVM)).
  - Cardholder Verification may also be done by the consumer entering a password/passcode directly into the Consumer-Presented QR Application (Cardholder Verification Method (CVM).

- Merchant Initiation (Mandatory)
  - The Merchant will enter Transaction details and initiate the QR payment Transaction at the POI. Transaction data is displayed, such as the amount to pay.
  - The QR scanner will be started, ready to capture the consumers QR Code.

- Data Entry (***Optional***)
  - Although the consumer is not required to enter any data before paying with a QR Code, this is an ***optional*** feature allowing the Consumer to input some Transaction specific data.
  - For example, a greater amount to pay could be entered for tip or convenience reasons.

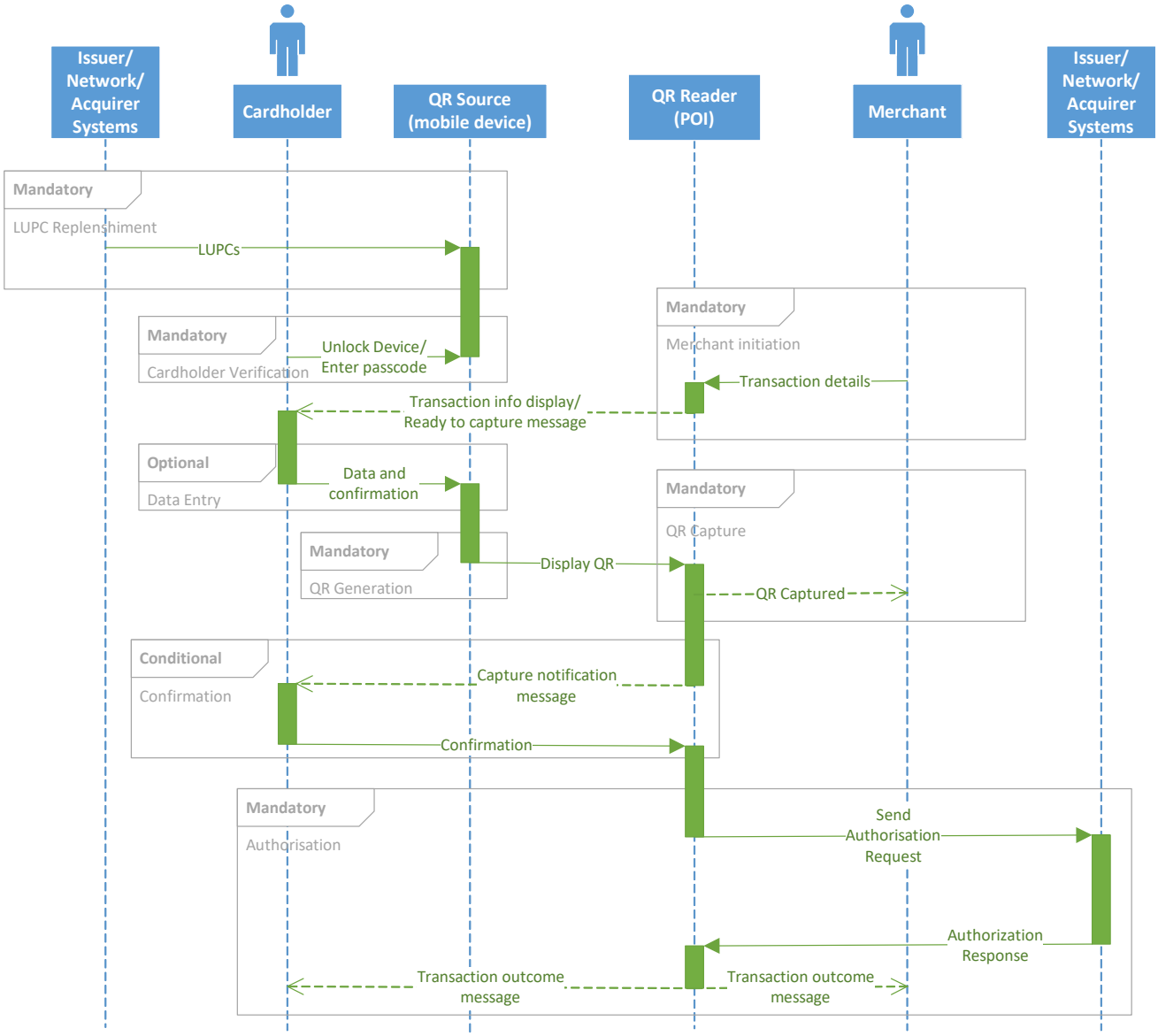
- QR Generation (Mandatory)
  - The QR generating application will generate a QR Code, after all conditional and ***optional*** processes have been performed by the consumer.
  - Before presentment, the consumer ***should*** be satisfied with the Transaction details.

- QR Capture (Mandatory)
  - The Merchant POI captures and parses the consumer's QR Code, ready for Authorization.

- Confirmation (Conditional)
  - Some implementations may require a consumer confirmation stage prior to the Merchant submitting the Transaction for Authorization.
  - This may consist of the Merchant displaying the Transaction details to the consumer and asking for confirmation.

- Authorization (Mandatory)
  - After the consumers QR is captured and parsed, and any necessary confirmations have been made, the Merchant system sends an Authorization request to the payment network.
  - Once the Authorization response is received, the Merchant and consumer are informed of the Transaction outcome by the Merchant system, and the Transaction is complete.

3.1 Use Case Flow



3.2 Use Case Blocks

The individual descriptions and requirements for the use case blocks (Shown in 3.1 Use Case Flow) are contained in the following Sections.

3.2.1 LUPC Replenishment (Mandatory)

An Issuer ***must*** issue LUPC to a Consumer-Presented QR Code Application to minimize risk and enable Transactions.

Subject to Issuer choice on the cryptogram version and functionality to be used, the QR Code Application ***must*** be issued with LUPCs that contain single-use Session Keys (SKs).

The LUPCs used in QR Code applications are only valid for a limited time for each single Transaction.

Therefore, the QR Code Application ***must*** require frequent updates of valid LUPCs from the Issuer system. A ***recommended*** maximum of 8 LUPCs can be downloaded and held by the QR Code Application.

Prior to downloading, the consumers QR Code Application ***shall*** be securely enrolled with the issuance system. American Express can provide On-Behalf-Of (OBO) services to fulfil these requirements.

3.2.2 Cardholder Verification (Mandatory)

Cardholder verification is required by policy (refer to [AEBOP]). This can take the form of a CDCVM or a CVM.

The definition of a CDCVM, is using the device owner's authentication credentials, normally used to unlock the device, to provide proof of identity to the QR generating application.

This may take the form of either a Device Password based credential or a Device Biometric credential.

The following list contains CDCVMs that may be used at the Issuers' discretion:

- Device Password (Alphanumeric)
- Device Passcode (Numeric)
- Device Fingerprint [1]

A CDCVM is authenticated by the device not the QR generating application. A message is then sent from the device to the application to indicate that CDCVM has been performed successfully. This process relies on a high level of trust of the device by the QR generating application.

A CVM is a means by which the Cardholder provides an authentication credential to the QR generating application to prove their entitlement to perform a Transaction.

In this case, a passcode and passphrase can be entered on the device and passed to the QR generating application. The application then performs the authentication of the credential.

If a passcode is used, it ***shall*** not be set by default to any PINs of related cards or accounts.

Issuers may select methods of Cardholder verification depending on their needs and regional regulations.

[1] Other biometric authentication may be used at the Issuer's discretion.

3.2.3 Merchant Initiation (Mandatory)

The Merchant enters the details of the Transaction into the POI system (e.g. the Amount). This initiates the Transaction and ***must*** display the Transaction details to the consumer.

Transaction details may be displayed later during the Confirmation stage of the Transaction, depending on implementation needs and local requirements.

The initiation stage ***shall*** activate the QR reader on the POI and wait for the consumer's QR Code to be presented. The POI ***shall*** also indicate to the consumer, that it is ready to capture the QR.

3.2.4 Data Entry (*Optional*)

Once the consumer is ready to generate the QR Code, the Issuer may wish for the consumer to be able to enter data which can be communicated to the Merchant in the QR Code, but this is not recommended.

This data may be contained in the Merchant POI data, or the Application Specific data that is to be passed to the Issuer via the network.

3.2.5 QR Generation (Mandatory)

The QR generating application takes a default set of data as defined in Section 4.1 POI and Application Specific Data, plus any additional data entered in the ***optional*** Data Entry stage and formats it into POI data and Application Specific data.

Within the Application Specific data there is a cryptogram generated using a unique Transaction session key, default data and variable data such as Unpredictable Number, the Application Transaction Counter, and Issuer Application data.

The application ***shall*** convert the data into a QR Code as defined by [EMV-QRCPS].

The QR Code ***shall*** be displayed on the display of the Mobile Device, ready to be scanned by the Merchant.

3.2.6 QR Capture (Mandatory)

Once the consumer's QR Code is presented, the POI ***shall*** scan the QR and convert to a data string, followed by parsing and format checking as defined by [EMV-QRCPS].

3.2.7 Confirmation (Conditional)

Confirmation may be required by some implementations. Once the QR Code has been scanned by the POI, Transaction details may be displayed on the POI for the consumer to confirm before the Transaction is sent for Authorization.

This may take the form of a message stating the Transaction amount requiring an "OK" or "Cancel" confirmation from either the consumer or the Merchant.

3.2.8 Authorization (Mandatory)

The data extracted from the POI part of the QR Code is used to select the American Express QR processing function within the Merchant Terminal.

Values extracted from the Application Specific data are added to a list of default data, modifying the default values where necessary.

This data is then submitted in a standard POS Authorization Request (1100) message.

The Issuer will process the request and respond with an Approval or Decline message which ***shall*** be communicated to the Merchant (and may be communicated to the consumer) via the point-of-sale system.

4 Data Objects

The following Section defines the Data Objects and contents required within the QR Code. It describes the minimum set of ***mandatory*** data objects that ***must*** be present in the QR Code.

Subsequent paragraphs describe additional data that may be conditional or ***optional***.

4.1 POI and Application Specific Data

The data encapsulated in the QR Code is categorized as Point of Interaction (POI) data or Application Specific Data.

POI data is used by the QR Code reading device, POS Terminal, or Merchant Mobile Device), for identification of the payment scheme, processing, and routing of the Transaction.

Application Specific Data is not interpreted or used by the POI directly, instead the POI is required to take this data and place it in a network message, to be processed by the Issuer.

4.2 Structure of individual data objects

Each data object is coded as per [EMV-QRCPS] using the BER-TLV format.

Where:

- T is BER-TLV encoded Tag
- L is BER-TLV encoded Length
- V is the data element

The cumulative size of the data objects in the QR Code ***shall*** be a maximum of 512 bytes as per [EMV_QRCPS].

4.3 Data Objects Definitions

The definitions used in the tables describing the data objects are as follows:

Name – The descriptive name of the primitive or template data object. This does not appear in the QR Code.

Tag – A Code representing the primitive or template data object within the QR Code, as defined in [EMV-QRCPS].

Type/Position – This describes if the data object is present in the root of the QR Code or if it exists within a template. Data is also marked as POI or AS (Application Specific), see 4.1 POI and Application Specific Data definitions.

Additional information is given if there are any restrictions as to where the data object ***should*** occur with the QR Code. The rules concerned with the hierarchy of data objects are defined in [EMV-QRCPS].

Format – This describes the range of characters that can be used within the value of the data object. They are as follows, and full definitions can be found in [EMV-QRCPS];

- String (S)

  Any [Unicode] character

- Alphanumeric Special (ans)

  The 96 characters described in the Common Character Set define in [EMV Book 4]

- Alphanumeric (an)

  Any ASCII encoded alpha numeric character

- Binary (b)

  Any binary values. i.e. raw data with a byte value of '00' to 'FF' and consisting of one or more bytes as specified

- Numeric (n)

  The ten characters representing the digits "0" to "9"

- Compressed Numeric (cn)

  Up to two numeric digits represented in the upper and lower nibbles of a single byte. Where one digit is needed, padding of 'F' ***shall*** be used in the remaining nibble

Length – This shows the fixed or variable length limits of the value associated with the data object.

Presence – This can be one of the following;

- Mandatory (M)

  The data object ***shall*** be present in all QR Codes.

- Conditional (C)

  The data object ***shall*** be present if the state condition statement is true.

- ***Optional*** (O)

  The data object may be present at the choice and discretion of American Express, the Issuer, or the regional payment body.

Requirements – This describes the requirements and/or processing rules for the given data object.

4.4 Minimum POI Data Object set

The following Data Objects ***shall*** be present in the Consumer's QR Code and ***shall*** be parsed by the QR Code reading application at the POI.

4.4.1 Payload Format Indicator		
Tag: '85'	Format: an	Length: 5
Type/Position: Root – POI – ***Shall*** be the first tag present		
Presence: M		
Requirements: ***Shall*** have a value of "CPV01"		

4.4.2 Application Template		
Tag: '61'	Format: b	Length: Var.
Type/Position: Root – POI – Template container within root		
Presence: M		
Requirements: ***Shall*** contain, at a minimum, all ***mandatory*** data for American Express Transactions		

4.4.3 ADF Name (AID)		
Tag: '4F'	Format: b	Length: 5 - 16
Type/Position: POI – Within '61' Application Template		
Presence: M		
Requirements: ***Shall*** contain the application ADF Name (AID) of A000000025011001		

4.4.4 Primary Account Number (PAN)		
Tag: '5A'	Format: cn	Length: var. up to 19 digits (10 bytes)
Type/Position: POI – Within '61' Application Template		
Presence: C		
Requirements: ***Shall*** be present if Track 2 Equivalent Data is not present. ***Shall*** contain the PAN.		

4.4.5 Application Expiration Date		
Tag: '5F24'	Format: n 6	Length: 3
Type/Position: POI –Within '61' Application Template		
Presence: C		
Requirements: ***Shall*** be present if Track 2 Equivalent Data is not present. The value ***shall*** be in the format YYMMDD.		

4.4.6 Track 2 Equivalent Data		
Tag: '57'	Format: b	Length: var. up to 19 bytes
Type/Position: POI – Within '61' Application Template		
Presence: C		
Requirements: Either this data or Primary Account Number (PAN) Tag: '5A' ***shall*** be present.		

4.4.7 Application Version Number		
Tag: '9F08'	Format: b	Length: 2
Type/Position: POI –Within '61' Application Template		
Presence: M		
Requirements: ***Shall*** contain the Application Version Number '00 10' for this version of the specification.		

4.5 Minimum Application Specific Data Object set

The following Data Objects ***shall*** be present in the Consumer's QR Code and ***shall*** be parsed by the QR reading device.

This minimum data is based on an EMV cryptogram using cryptogram version number '11'.

4.5.1 Application Specific Transparent Data		
Tag: '63'	Format: b	Length: Var.
Type/Position: AS – Within '61' Application Template		
Presence: M		
Requirements: ***Shall*** contain ***mandatory*** and ***optional*** American Express specific data to be passed to the Issuer for authentication for a given Transaction.		

4.5.2 Application Cryptogram		
Tag: '9F26'	Format: b	Length: 8
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: ***Shall*** contain the Application Cryptogram calculated for the given Transaction.		

4.5.3 Application Transaction Counter (ATC)		
Tag: '9F36'	Format: b	Length: 2
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: ***Shall*** contain the ATC for the given Transaction. The ATC is obtained from the LUPC used for the Transaction.		

4.5.4 PAN Sequence Number		
Tag: '5F34'	Format: n 2	Length: 1
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements:		

4.5.5 Unpredictable Number (UN)		
Tag: '9F37'	Format: b	Length: 4
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: Device-based random number generators ***must*** have sufficient entropy for the required security level of the function for which they are used within the Mobile Application.by the QR Source Application in AC generation.		

4.5.6 Issuer Application data (IAD)		
Tag: '9F10'	Format: b	Length: Up to 32
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: The CVR within the IAD is used during the generation of the EMV Cryptogram.		

4.5.7 Application Interchange Profile		
Tag: '82'	Format: b	Length: 2
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: The value of 'FFFF' is used for cryptogram generation and Authorization. This value is unique for CPQR transaction, no other value is allowed.		

4.5.8 Terminal Verification Results		
Tag: '95'	Format: n 10	Length: 5
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: M		
Requirements: This data element shall be used to hold a QR Code Timestamp. It is part of the payload for cryptogram generation and is validated during Authorization. The format of QR Code Timestamp is numeric (Unix Epoch time - seconds since 1970), right-justified with leading zeroes as necessary.		

4.6 Additional POI Data Object Set

There are ***optional*** and conditional data objects that may be present in the QR Code to add extra functionality and flexibility to the payment. The following Section describes the additional POI data objects.

4.6.1 Application Label		
Tag: '50'	Format: ans	Length: 1 - 16
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: May be printed on the POI receipt. Special characters defined within the 'ans' format is limited to the space character only.		

4.6.2 Language Preferences		
Tag: '5F2D'	Format: an	Length: 2 - 8
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: The POI ***shall*** use the first mutually supported language (when reading the Language Preferences from left to right) to display messages to the Cardholder.		

4.6.3 Issuer URL		
Tag: '5F50'	Format: an	Length: Var.
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: The POI may read the customer information within the Issuer URL in order to provide an electronic receipt to the customer. The Issuer URL may contain the customer's phone number or an email address.		

4.6.4 Token Requestor ID (TRID)		
Tag: '9F19'	Format: n 11	Length: 6
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: The use of this data element is subject to the availability of Network capabilities.		

4.6.5 Payment Account Reference (PAR)		
Tag: '9F24'	Format: ans	Length: 29
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: The use of this data element is subject to the availability of Network capabilities.		

4.6.6 Last 4 digits of PAN		
Tag: '9F25'	Format: cn	Length: 2
Type/Position: POI –Within '61' Application Template		
Presence: O		
Requirements: The use of this data element is subject to the availability of Network capabilities. If the POI prints the Last 4 digits of PAN on the receipt, it ***shall*** use the value contained within this tag.		

4.7 Additional Application Specific Data Object Set

There are ***optional*** and conditional data objects that may be present in the QR Code to add extra functionality and flexibility to the payment. Some of the data objects have default values.

These defaults are used during the cryptogram calculation and are not placed in the QR Code.

Alternatively, if values other than the defaults are used, the replacement value ***shall*** be placed in the QR Code.

The following Section describes the additional Application Specific data objects.

4.7.1 Application Interchange Profile		
Tag: '82'	Format: b	Length: 2
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence:		
Requirements: If not present, a default value of '0000' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		
4.7.134.7.1 Amount, Authorized		
Tag: '9F02'	Format: n 12	Length: 6
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		
Requirements: If not present, a default value of '000000000000' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		

4.7.144.7.2 Amount, Other		
Tag: '9F03'	Format: n 12	Length: 6
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		
Requirements: If not present, a default value of '919191919191' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		

4.7.154.7.3 Terminal Country Code		
Tag: '9F1A'	Format: n 3	Length: 2
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		

Requirements: If not present, a default value of '9999' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.

4.7.164.7.4 Transaction Currency Code		
Tag: '5F2A'	Format: n 3	Length: 2
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		
Requirements: If not present, a default value of '9999' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		

4.7.174.7.5 Transaction date		
Tag: '9A'	Format: n 6 (YYMMDD)	Length: 3
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		
Requirements: If not present, a default value of '140101' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		

4.7.184.7.6 Transaction Type		
Tag: '9C'	Format: n 2	Length: 1
Type/Position: AS – Within '63' Application Specific Transparent Data Template		
Presence: C		
Requirements: If not present, a default value of '00' is used for cryptogram generation and Authorization. Or if a non-default value is required, it ***shall*** be used for cryptogram generation, sent in the QR Code and ***shall*** be sent in the Authorization message.		

This specification does not preclude the use of other implementation specific data, which may be present in the Application Specific data portion of the QR Code.

5 System requirements

5.1 Issuance System Requirements

The Issuance System is responsible for Issuing the Payment account data and LUPCs to the Consumer-Presented QR (CPQR) Application. The issuance of CPQR Accounts differ from normal Expresspay Cards in several ways including:

- Instant issuance of CPQR Accounts
- Use of Card data (PAN and Exp Date) for CPQR transactions
- Frequent issuance of LUPCs
- CPQR Account Card Life Cycle Management.

American Express can provide On-Behalf-Of (OBO) services to fulfil these requirements.

5.2 Mobile Device Requirements

5.2.1 Security

Since the QR generating application requires cryptographic key storage and cryptogram computation, it is imperative that the software, keys, and payment credentials are secured using established security techniques. Please refer to [AEHCESC].

5.2.2 Card data, LUPC Storage and Replenishment

An Issuer ***must*** create Card data and issue with valid LUPCs to a CPQR Application to minimize risk and enable Transactions.

Card data requirements are detailed in the Business and Operating Policy [AEBOP]

Subject to Issuer choice on the cryptogram version and functionality to be used, the CPQR Application can be issued with LUPCs that contain single-use Session Keys (SKs).

The LUPCs are only valid for a limited time for each single Transaction. Therefore, the CPQR Application ***must*** receive frequent updates of valid LUPCs from the Issuer system.

Card data and LUPCs may be used for NFC and QR implementations depending on the type of Issuer implementation. It is ***recommended*** that LUPCs are refreshed as a background process whenever the CPQR Application has data connectivity. This ensures that the CPQR Application is always ready to be used for payment, with or without data connectivity.

The CPQR Application ***must*** use a Local Master Key (LMK) to encrypt security critical data for storage. The application developer is free to use any security mechanisms provided by the Mobile Platform/Operating System, such as Key Storage, Key Chains, and Trusted Execution Environments etc. Security requirements are detailed in the security requirements [AEHCESC].

5.2.3 Cardholder Verification Methods

Cardholder Verification is required before generating and displaying a QR Code on the Cardholder's device.

This may take the form of a CDCVM, where the action of unlocking the Mobile Device with a passcode or fingerprint, provides Cardholder verification that can be used during the Transaction.

After CDCVM is performed, the following data ***shall*** be used during the generation of the QR Code.

- CVR = '03A00100' for a non-biometric CDCVM such as Device Passcode

Or

- CVR = '03A20100' for a biometric CDCVM such as Device Fingerprint

If the Issuer Application Data Format is '01' – HCE Issuer Application data format, set the Issuer Application Data Mobile CVM Method ID as follows.

IAD CVM Method ID = $\begin{pmatrix} \text{'01' for Device Passcode} \\ \text{'03' for Device Password} \\ \text{'05' for Device Fingerprint}^2 \end{pmatrix}$

CVR and IAD data ***shall*** be computed before the cryptogram is generated

5.2.4 Cardholder Data Input

The Cardholder is not required to enter any data prior to the application generating a QR Code. However, ***optionally*** data can be entered (for example an amount), secured by the cryptogram and transmitted to the Issuer Authentication Service via the QR Code.

A set of ***mandatory*** AS data and a set of default values are used to generate the Application Cryptogram. The ***mandatory*** data must be present in the QR Code, but the default data does not. If however, any of the default values are changed by either the Consumer-Presented QR Application or by user data input, the new value rather than the default value ***shall*** be used in the cryptogram and ***shall*** be placed in the QR Code.

5.2.5 QR generation

The QR Code data consists of the POI data and AS data. The ***mandatory*** minimum set of POI data described in Section 4.4 - Minimum POI Data Object set, ***shall*** be contained within the QR Code. The ***optional*** POI data described in Section 4.6 - Additional POI Data Object Set, can be included if required by the implementation.

The ***mandatory*** minimum set of AS data described in Section 4.5 - Minimum Application Specific Data Object set, ***shall*** be contained within the QR Code.

The ***optional conditional*** AS data described in Section 4.7 - Additional Application Specific Data Object Set, can be included if required by the implementation.

5.2.5.1 Application Transaction Counter

For card based EMV Transactions the Application Transaction Counter (ATC) is incremented for each Transaction, but when the payment method is based on LUPCs, which is the case for Consumer-Presented QR payments, the ATC ***shall*** be obtained from the LUPC used for the Transaction.

5.2.5.2 Unpredictable Number generation

The QR generating application ***shall*** generate or derive a four-byte Unpredictable Number (UN) prior to the display of each QR Code.

The UN ***shall*** be securely generated and be sufficiently random to provide the correct degree of unpredictability during the Cryptogram generation.

[2] Other biometric authentication may be used at the Issuer's discretion.

5.2.5.3 QR Code Timestamp setup

Terminal Verification Results (TVR, tag '95') is re-used to store a QR Code Timestamp for this CPQR specification only. The format shall be a numeric (BCD) representation of Unix Epoch time (seconds since 1970), right justified with leading zeroes.

Depending on the implementation, the value of the QR Code Timestamp could be set to:

- QR Code Generation Timestamp or
- QR Code Expiry Timestamp

If it's a QR Code Generation Timestamp, the current time value shall be derived from a trusted time source, where possible.

If it's a QR Code Expiry Timestamp, it shall be the current time value (shall also be derived from a trusted time source where possible) plus an issuer-defined period. (For example, thirty seconds or two minutes.) The QR Payload data shall be held by the CPQR application until expired or used in a transaction.

5.2.5.35.2.5.4 EMV Cryptogram input

The CPQR Application ***shall*** use the data from Table 5-1: Cryptogram Input Data, to calculate the Application Cryptogram '9F26' based on the Cryptogram Version being implemented and using a unique session key from the next available LUPC. See Section 6 Cryptographic Requirements.

Where the default data has been modified, either by implementation specific user input or by an implementation specifying non-default values, these modified values ***shall*** be used during cryptogram generation rather than the default values.

If modified values are used, they ***must*** be placed in the QR Code data. (Default values need not be placed in the QR Code data).

Table 5-1: Cryptogram Input Data

Name	Tag	Length (bytes)	Value
Amount, Authorized	'9F02'	6	Default = '000000000000'
Amount, Other	'9F03'	6	Default = '919191919191'
Terminal Country Code	'9F1A'	2 (n 3)	Default = '9999'
Terminal Verification Results	'95'	5 (n 10)	QR Code Timestamp value right justified with leading zeroesDefault = '8000000000'
Transaction Currency Code	'5F2A'	2 (n 3)	Default = '9999'
Transaction Date	'9A'	3 (n 6 YYMMDD)	Default = '140101'
Transaction Type	'9C'	1 (n 2)	Default = '00'
Unpredictable Number	'9F37'	4	Random number from the QR source application
Application Interchange Profile	'82'	2	Always Default = 'FFFF0000'
Application Transaction Counter	'9F36'	2	Unique counter value obtained from the LUPC per Transaction
Card Verification Results	In IAD '9F10'	4	The computed value from Section 5.2.3

5.3 Consumer-Presented QR data format

The requirements for the structure of the Consumer-Presented QR Code are as follows;

- The Payload Format indicator ***shall*** be the first tag.
- The minimum POI data ***shall*** be present in the Application Template tag '61' in the root after the first tag.
- The minimum Application Specific Data ***shall*** be present in the Application Specific Transparent Data tag '63' within Application template tag '61'
- All tags present in template '61' and '63' may be presented in any order.

The following table shows the format and structure of the contents of a Consumer-Presented QR Code.

Table 5-2: Consumer-Presented QR data format

Tag			Length	Name	Value/Notes	Presence
'85'			5	Payload Format Indicator	"CPV01"	M
'61'			var.	Application Template		M
	'4F'		5 - 16	ADF Name (AID)	A000000025011001	M
	'50'		1 - 16	Application name		O
	'5A'		≤10	PAN	Up to 19 digits	C – If '57' not present
	'5F24'		3	Expiry Date		C – if '5A' present
	'57'		≤19	Track 2 Equivalent Data		C – if '5A' not present
	'5F2D'		2 - 8	Language Preferences		O
	'5F50'		var.	Issuer URL		O
	'9F08'		2	Application version number	'00 10'	M
	'9F19'		6	Token Requestor ID (TRID)		O
	'9F24'		29	Payment Account Reference (PAR)		O
	'9F25'		2	Last 4 Digits of PAN		O
	'63'		var.	Application specific transparent data		M
		'9F26'	8	Application Cryptogram	As generated using the data from Table 5-1: Cryptogram Input Data	M
		'9F36'	2	Application Transaction Counter (ATC)	Unique counter value obtained from the LUPC per Transaction	M
		'9F37'	4	Unpredictable number (UN)	Random number from the QR source application	M
		'9F10'	up to 32	Issuer Application Data (IAD)	The CVR within the IAD is used during cryptogram generation. See Table 5-3	M
		'5F34'	1	Application PAN Sequence number		M
		'82'	2	Application Interchange Profile (AIP)	T'FF FF'If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Dataakes mandatory value 'FFFF', either present or set as default value. See	CM C

					Table 5-1: Cryptogram Input Data	
		'9F02'	6	Amount, Authorized	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C
		'9F03'	6	Amount, Other	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C
		'9F1A'	2	Terminal Country Code	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C
		'95'	5	Terminal Verification ResultsFormat	Value as used in AC generation. See Table 5 1: Cryptogram Input DataIf not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	MC
		'5F2A'	2	Transaction Currency Code	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C
		'9A'	3	Transaction date	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C
		'9C'	1	Transaction Type	If not present, default value used. If present, actual value used. See Table 5-1: Cryptogram Input Data	C

5.3.1 Issuer Application Data format

The following table shows the structure of the Issuer Application Data. The CVR portion of the data is used by the QR source device to generate the cryptogram.

Table 5-3: Issuer Application Data format

Name	Length	Value/Notes	Presence
Length	1		M
Derivation Key Index (DKI)	1		M
Cryptogram Version Number (CVN)	1	'11' for restricted EMV 2TDEA	M
Cardholder Verification Results (CVR)	4		M
IAD Format (See note)	1	'01' = HCE format '02' = Issuer discretionary Data	M
IAD Session Key Information			
Length	1	16 for restricted session keys 0 for non-restricted session keys	C Present if format '01'

	Restricted start date	3	YY MM DD	C Present for restricted session keys
	Restricted start time	3	HH MM SS	C Present for restricted session keys
	Restricted end date	3	YY MM DD	C Present for restricted session keys
	Restricted end time	3	HH MM SS	C Present for restricted session keys
	MAC	4	Left 4 bytes of MAC	C Present for restricted session keys
IAD CVM info				
	Length	1	'01'	C Present if format '01'
	Mobile CVM Method ID	1	'00' No Mobile CVM Performed '01' Device Passcode '03' Device Password '05' Device Fingerprint [3] All other values RFU	C Present if format '01'
Device info		Up to 20 keeping total IAD length ≤32		C Present if format '01'

Note: Since CVN '11' is a restricted session key cryptogram, the IAD format ***should*** be '01' and the IAD ***should*** contain the session key information.

If it is not possible to use IAD format '01' because of implementation restrictions, a database of session key restrictions (i.e. time and date) will have to be made available to the Authorization system.

5.3.2 QR display

The Consumer-Presented QR Application ***shall*** display the QR Code for a maximum of one minute, after which time it ***shall*** be hidden.

The Consumer-Presented QR Application may provide a facility to show the same QR again after the display timeout, e.g. an "I need more time" button.

It is not recommended to display a new QR Code after timeout, as this will use up LUPCs stored on the device.

It is ***recommended*** that the QR be no smaller than 25mm x 25mm, and that the Consumer-Presented QR Application increases the screen brightness if below 50%, where possible on the Mobile Device.

5.3.3 Performance

The Consumer-Presented QR Application ***shall*** be capable of creating and displaying a QR Code within one second of the user selecting an option to pay by QR Code.

[3] Other biometric authentication may be used at the Issuer's discretion.

5.4 POI/Terminal Requirements

5.4.1 Network support

This specification is based on [EMV-QRCPS]. Therefore, a payment cryptogram is generated by the QR source device and submitted for Authorization by the Merchant through an EMV capable network.

This requires that data is submitted in Bit position 55.

5.4.2 Transaction initiation and QR Capture

The Merchant may enter the Transaction amount or use some other method to initiate a QR payment at the point-of-sale Terminal.

The Terminal can prompt for the card member to present multiple payment methods but ***shall*** activate its QR scanner as well as other supported interfaces, such as Contactless.

Some implementations ***may*** specify a limit for the maximum QR Transaction amount that can be made. The limit ***may*** be enforced by the Terminal or the Issuer.

If the maximum QR Transaction amount limit is breached, the Transaction can be declined by the Terminal, or submitted for Authorization for the issuer to make the decision.

The QR capture device will be enabled and the payer notified to present their QR Code.

Once the QR Code is read successfully, the data is converted from Base64 [RFC 4648] to binary, ready for processing by the POI application, see [EMV-QRCPS] for details. If the QR read fails, the Merchant ***shall*** be notified.

5.4.3 QR Parsing

The format of the QR data ***shall*** be as detailed in Section 5.3 - Consumer-Presented QR data format.

If the QR data is in a prescribed format with the minimum ***mandatory*** data present with acceptable values, the POI application ***shall*** search each Application Template (tag '61') and examine the ADF Name (tag '4F') until the American Express QR AID is found.

Once the parsing is complete, as described in [EMV-QRCPS] Section 5, two sets of data are available to the POI application; POI data and Transparent Data.

The POI data is used by the POI for operations such as determining what language to display messages, or to print information on a receipt etc.

The Transparent data is used to submit the Transaction for Online Authorization.

5.4.4 Authorisation

Once the POI application has parsed the QR data, the Merchant's Terminal sends the data to the Acquirer for construction of an Authorisation Request (1100) message for submission to the Issuer host for ***mandatory*** Online approval.

There ***may*** be an additional step where the payer can confirm their willingness to proceed prior to the Merchant submitting the authorisation request.

All data in the 1100 message, other than Bit position 22 (Point of Service (POS) Data Code) and Bit position 55 (ICC System Related Data) ***shall*** be completed as a standard Card Present transaction.

The majority of ICC related data for Bit position 55 comes from the contents of the QR Code.

Table 5-4: QR Data to Bit 55 Authorisation message mapping, shows how either data from the QR Code, or default data are mapped to data required for Bit 55 of the authorisation message.

For the Issuer to identify a QR Transaction, The POS Data Code which is mapped to Bit position 22 (POS Data Code) ***shall*** be encoded as follows;

- Position **6** (Card Present) = **1** (Card present)
- Position **7** (Card Data Input Mode) = **3** (Bar Code)

Note: Please refer to other American Express supported local market ISO specifications for further information on CPQR Transaction identification codes.

Once the Authorisation Request has been submitted, the Issuer performs a risk analysis on the Transaction data and CVM status, and an Authorisation Response is sent back to the Merchant.

If an Authorisation Response Code of '00', '08', '10, or '11' is received, the Terminals ***shall*** treat these codes as meaning an Issuer approval for the Transaction.

All other codes, or no response, ***shall*** be treated as an Issuer decline for this Transaction. In either case, the Terminal ***shall*** notify the Merchant of the Issuers decision.

If approved, the Transaction is completed, goods can be exchanged, and receipts generated.

Table 5-4: QR Data to Bit 55 Authorisation message mapping

Field Name	Length	Source	Default
Application Cryptogram	8	From QR Code	
Issuer Application Data (IAD)	33	From QR Code	
Unpredictable Number	4	From QR Code	
Application Transaction Counter (ATC)	2	From QR Code	
Terminal Verification Results (TVR)	5	From QR Code if present	'8000000000' if not present
Transaction Date	3	From QR Code if present	'140101' if not present
Transaction Type	1	From QR Code if present	'00' if not present
Amount, Authorized	6	From QR Code if present	'000000000000' if not present
Transaction Currency Code	2	From QR Code if present	'9999' if not present
Terminal Country Code	2	From QR Code if present	'9999' if not present
Application Interchange Profile (AIP)	2	From QR Code if presentAny	'FFFF0000' if not present
Amount, Other	6	From QR Code if present	'919191919191' if not present
Application PAN Sequence Number	1	From QR Code	
Cryptogram Information Data	1	Terminal	'80' (ARQC)
Issuer Action Code – Default [4]	5	Terminal	'8000000000'
Issuer Action Code – Online [5]	5	Terminal	'8000000000'
Issuer Action Code – Denial [6]	5	Terminal	'0000000000'

[4] 'Issuer Action Code – Default' may not be required by all authorisations message formats.

[5] 'Issuer Action Code – Online' may not be required by all authorisations message formats.

[6] 'Issuer Action Code – Denial' may not be required by all authorisations message formats.

6 Cryptographic Requirements

This chapter describes the cryptographic security requirements for payment Transactions, as outlined in these specifications.

6.1 Limited-Use Payment Credentials (LUPCs)

An American Express CPQR Application uses Session Keys (SKs) to generate cryptograms for Issuer Authorization. The SKs are provided to the CPQR Application by the Issuer or 3rd party within the LUPCs.

The SKs are provided with additional data, which describe the following:

- Restrictions on key usages
- Data to be provided in the Application Cryptogram response
- The QR payment account identifier

6.1.1 Session Key (SK) Management

The CPQR Application is responsible for SK management. SKs ***must*** be generated by the Issuer and sent securely to the CPQR Application as part of the LUPC data set (see Figure 6-1 Cryptogram Generation and Table 6-1 LUPC Data Details,for more information).

The SKs ***must*** be protected by a Transport Key (TPK), and transmitted over a mutually authenticated secure channel, which is secured using industry best practices.

The CPQR Application ***must*** store these LUPCs securely for subsequent use. The CPQR Application ***must*** ensure during a SK update, the Issuer and Consumer-Presented QR Application SKs are kept in synchronization.

When a CPQR Application uses a SK during a Transaction, it ***must*** be removed securely from the CPQR Application's SK store. SKs with a lower Application Transaction Counter (ATC) than the SK used for the Transaction ***must*** also be removed securely.

The SKs have a validity period after which the CPQR Application ***must*** remove the SK from the SK store.

The CPQR Application ***must*** monitor the SK store and request new SKs when required. The CPQR Application ***must*** ensure that requests for new SKs are scheduled so the CPQR Application has sufficient opportunity to collect new SKs before all of its SKs expire.

Table 6-1 LUPC Data Details

Data Element	Format	Length	Presence	Description
Application Cryptogram Session Key	b	16	M	The triple DEA or AES Session Key.
Derivation Key Index	b	1	M	The AC Derivation Key Index, returned to Issuer in the IAD.
ATC	b	2	M	The ATC used to generate the Session Key.
Cryptogram Version Number - EMV Mode	b	1	M	The Cryptogram Version Number (CVN) that describes how the Session Key is generated and how the cryptogram ***must*** be generated.

Cryptogram Version Number - Magnetic Stripe Mode	b	1	Not supported	The Cryptogram Version Number (CVN) that describes how the Session Key is generated and how the cryptogram ***must*** be generated.
Card Identifier	var	var	M	Each Session Key is generated for a particular Expresspay Mobile QR payment account (card). This Card ID provides the Consumer-Presented QR Application an identifier for that QR payment account. This format of this field is at Issuer discretion.
Combined Passcode Derived Key CVM SK (Combined PDK CVM SK)	b	16	Not supported	The Session Key used in Issuer verified CVM processing, encrypted under a Passcode Derived Key.
Mobile CVM Derivation Key Index	b	1	Not supported	Mobile CVM Derivation Key Index.
IAD Session Key Info	see Table 5-3: Issuer Application Data format	Jan-16	M	Details of restricted use Session Key derivation.

6.2 Cryptogram Version Number (CVN) Requirements

The CVN describes the mechanism to be used by both the CPQR Application and Authorization System to derive the cryptogram. An EMV mode cryptogram ***shall*** be generated using the SKs.

The Cryptogram version number ***shall*** be '11' when implemented.

Table 6-2 lists the CVNs supported by the CPQR Application.

Table 6-2 Supported CVNs

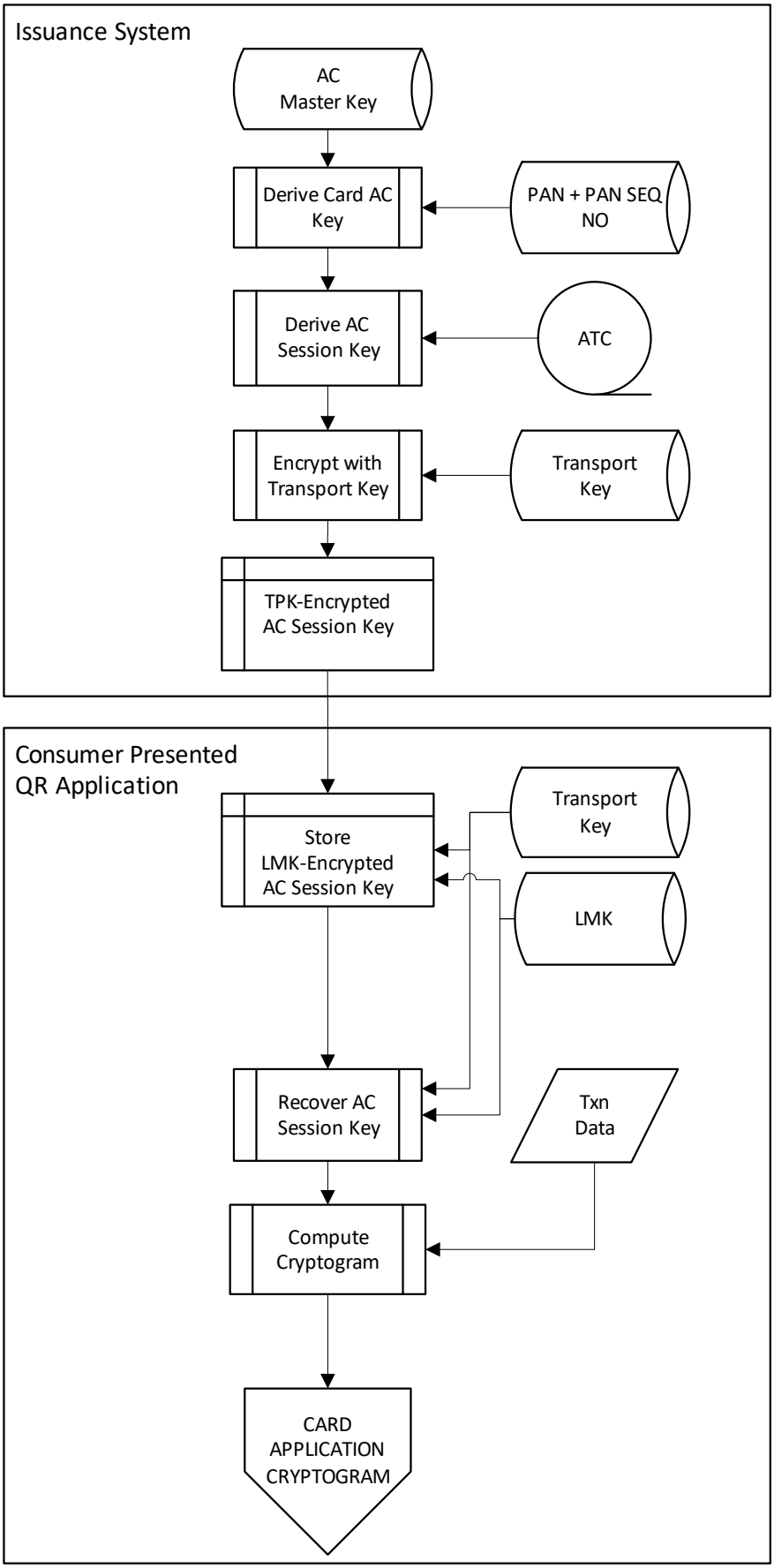
CVN	Description
'11'	EMV Mode with 2TDEA restricted session key.

The next Sections in this chapter describe CVNs in detail, including the cryptographic operations required to support them.

6.3 Cryptogram Generation Requirements

The CPQR Application ***must*** generate application cryptograms, using Application Cryptogram (AC) SKs generated by the Issuer, as shown in Figure 6-1 Cryptogram Generation.

Figure 6-1 Cryptogram Generation



6.3.1 Cryptogram Generation Process

The complete cryptogram generation process includes the following steps:

6.3.1.1 Card Key Derivation.

Card Key Derivation derives a Card Key from an Issuer Master Key (IMK). IMKs are securely stored by the Issuer and indexed via the Derivation Key Index (DKI).

Issuer Master Keys are indexed via the Derivation Key Index. The Derivation Key Index (DKI) is present in the LUPC and is sent to the Authorization System in the Issuer Application Data.

The Card Key ***must*** be derived by the Issuer from the appropriate Issuer Master Key using the Card's PAN and PAN sequence number.

The Issuer ***must*** securely store the Card Keys in the Issuance System and ***must*** *not* deliver these keys to the Consumer-Presented QR Application.

6.3.1.2 Session Key Derivation.

Session Key Derivation is the derivation of a Transaction specific key from a Card Key. This derivation typically uses the Application Transaction Counter (ATC) as input to ensure that different Transactions use different SKs.

For QR Mobile Devices, the Issuer derives the SK, which is delivered to the Mobile Device, along with its ATC. A restricted SK is the term used in this document for SKs derived from both an ATC and other Transactional data.

The inclusion of other Transactional data means that the SK can be restricted to Transactions where that particular Transaction data is used. A restricted SK is derived by the Issuer, and the restricted SK, ATC, and other data specifying the restriction are delivered to the QR source device.

6.3.1.3 Cryptogram Generation.

Cryptogram Generation is the process of creating a cryptogram from a SK that uses Transaction and device data.

The purpose of generating cryptograms is to create cryptographic data that can be used by the Authorization system as evidence that the Transaction was conducted with the QR source device, using a particular set of Transaction data.

6.3.2 Application Cryptogram Card Keys

Issuers ***must*** use one of the following options for deriving the Application Cryptogram Card Keys:

- **2TDEA - EMV Option A:** Card Key Derivation Option A is detailed in EMV Book 2, Section A1.4.1. In addition to the requirements of EMV, there is a requirement that the parity of each byte of a DES key is odd. Thus, after a new key is derived, for each byte of the key, the least significant bit ***must*** be flipped if the parity is not odd.
- **AES - EMV Option C:** Card Key Derivation Option C is detailed in EMV Book 2, Section A1.4.3.

6.3.3 Derivation of Restricted AC Session Keys

For CVN '11', restricted Session Keys are used. To issue a restricted Session Key, an Issuer ***must*** decide on a validity period for the Session Key.

Derivation of restricted Session Keys requires an additional, dedicated master key to calculate a MAC value to be included in the diversification value. For CVN '11' this will be a 2TDEA MAC key.

This master key is used to create a Derived MAC Key using the same methods as used for Application Cryptogram Card Keys, as defined in Section 6.3.2.

A Validity Period restriction, formatted as:

- A Start Date in format YYMMDD
- A Start Time in format HHMMSS
- An End Date in format YYMMDD
- An End Time in format HHMMSS

For CVN '11', the Application Cryptogram Session Key is a double-length (16-byte) TDES key.

The Session Key is derived by enciphering a diversification value with the Card Key to produce a 16-byte Session Key (SK) using 2TDEA in CBC mode, using restricting details as described above.

1. First, the MAC Data is assembled as follows:
   - ✓ *MAC Data* = ATC || '80' || '00' || StartDate || StartTime || EndDate || EndTime
2. Next, compute an 8-Byte MAC by performing a 2TDEA operation in CBC mode using 2TDEA Derived MAC Key (MK):
   - ✓ *MAC = 2TDEA(MK)[MAC Data] Initialization Vector = 8 bytes of '00'*
3. Append the MAC to the end of the MAC Data to form the 24-Byte diversification value (R):
   - ✓ *R* = MAC Data || MAC
   - ✓ Divide R into 8-byte blocks R1, R2, R3.
4. Compute the Session Key by encrypting R with the Card Key (CK) in CBC mode:
   - ✓ *A* = 2TDEA(CK)[R1] Initialization Vector = 8 bytes of '00'
   - ✓ SK_a = 2TDEA(CK)[R2] Initialization Vector = *A*
   - ✓ SK_b = 2TDEA(CK)[R3] Initialization Vector = SK_a
5. Construct the 16-byte Session Key by concatenating the last two blocks of the result:
   - ✓ SK= SK_a || SK_b

6.3.4 Cryptogram Generation

A cryptogram is calculated on a QR source device, using a key sent to the device by the Issuer. Cryptogram generation is a three-stage process:

1. The cryptogram input data is assembled.
2. The cryptogram is calculated.
3. The cryptogram response data is formatted.

6.3.4.1 Calculation of Cryptogram Input Data

Cryptogram input data is created by the concatenation of data elements. In the case of Consumer-Presented QR codes, no data is available from the Terminal. The data elements are of the following:

- Part of a QR data on the QR source device
- Data from the LUPC
- A constant value, i.e. default values

All Expresspay EMV mode CVNs create their cryptogram input data by concatenation in order of the data elements listed in Table 5-1: Cryptogram Input Data.

The format of each entry is a one- or two-byte tag, which identifies the desired data object, followed by a one-byte length which represents the number of bytes the field ***must*** occupy. Thus, the location of the Cryptogram Inputs within the Generate AC input data can be determined by examination of the CDOL1 data element.

The example below illustrates how the CPQR Application can determine the location of the data items required for cryptogram generation.

6.3.5 Calculation of the Cryptogram

The algorithm for calculating the cryptogram on QR devices is:

- For 2TDEA-based cryptograms, CVN: '11', the cryptogram ***must*** be generated as described in Section 6.4.1 Cryptogram Algorithm for Double Length DEA Keys.

6.4 Cryptogram Calculation

The following Section defines how the two cryptogram types are generated.

6.4.1 Cryptogram Algorithm for Double Length DEA Keys

The CPQR Application generates an Application Cryptogram for an ARQC since an Online request for approval is mandated. The QR source device creates a block of cryptogram input data "D."

The cryptogram calculation includes the following steps:

1. Padding.

Pad the Input data "D" to the right with the smallest of '00' bytes to the right so that the length of the resulting data is a multiple of 8 bytes:

D':=(D || '00'||'00'…||'00')

D' is then divided into 8-byte blocks: X_1, X_2,…, X_n

2. Application Cryptogram Session Key.

The Application Cryptogram Session Key *K* consists of the concatenation of a leftmost and rightmost key block:

$K = (K_L \,||\, K_R)$

3. Cryptogram calculation.

Process the 8-byte blocks with the DES cipher in CBC mode, using the left most key K_L:

$O_i := DES(K_L)[X_i \oplus O_{i-1}]$ *for* $i = 1, 2, \ldots, n$

With initial value

O_0 = ('00' || '00' || '00' || '00' || '00' || '00' || '00' || '00')

and with initial vector

K_0 = ('00' || '00' || '00' || '00' || '00' || '00' || '00' || '00')

Compute the 8 byte block O_{n+1} as follows:

$O_{n+1} := DES(K_L)[DES^{-1}(K_R)[O_n]]$

The cryptogram is the equal to O_{n+1}.