PAYMENTS ASSOCIATION OF NAMIBIA

NAMQR Code Standards
Version 5.0

09 Mav 2025

Table of Contents

1. Version

Version	5.0
Last Update Date	11-Apr-2025
Status	**Final version**
Reason for change	i. Added a new section, giving evidence of how the proposed NAMQR specifications can be adopted to facilitate payments to and from the SOVs using the existing as well as proposed payment streams. ii. Provided additional clarifications wherever necessary based on industry comments and feedback. iii. Realigned sections to improve readability and ease of comprehension of the document. iv. Corrected typo and other grammatical errors. v. Included tag for discount and cashback

2. Abbreviations and Glossary

Term	Definition / Full Form
2FA	Two-Factor Authentication
AA	ATM Account
AID	Application Identifier
AMC	Asset Management Company
Acquirer Entity	Any credit going to an NPS user will be credited in the acquirer e-money wallet account. The e-money provider receiving the funds in NPS P2M transactions will be acting as an acquirer entity.
ATM	Automated Teller Machine
B2B	Business-to-Business
B2G	Business-to-Government
B2P	Business-to-Person
BA	Bank Account
Bank	NPS Entity
Bank account	A saving / checking account with a bank in Namibia

Bank app	A Mobile app that allows the Customers and / or Merchants to initiate and / or complete transactions. Bank app can be operated by an NPS Member Entity.
BIN	Bank Identification Number
BoN	Bank of Namibia
CA	Card Account
CDCVM	Customer Device Cardholder Verification Method
CMBO	Currency Management and Banking Operations
CRC	Cyclic Redundancy Check
Customer	Customer is an individual having a valid bank account / card account / e-money wallet and who is either a payer or a payee in NPS transaction.
DD	Digital Dimensions
DPO	Direct Pay Online
DTH	Direct to Home
ECDSA	Elliptic Curve Digital Signature Algorithm
ECI	Extended Channel Interpretation
EFT	Electronic Funds Transfer
EMA	E Money Account
EMVCo	Europay, Mastercard, and Visa
EnCR	Enhanced Credit payments
EnDO	Enhanced Debit Orders
DTH	Direct To Home
FMI	Financial Market Infrastructure
FNB	First National Bank
FSD	Functional Specification Document
Full form alias	A payment address of the individual or merchant in an abstract form that identifies store of value details in a normalized notation. A full form alias appears before the handle of the store of value provider and can be in the form of fullformalias@IPP participant
FX	Foreign Exchange
G2P	Government-to-Person
IEC	International Electrotechnical Commission
IPN	Instant Payment Namibia (Fintech – Solution Operator)
IPP	Instant Payment Solution
ISO	International Organization for Standardization
Issuer Entity	All NPS users need to have a banking account with NPS enabled banks / e-money providers. While performing a P2M transaction, the user's bank account will be debited. The Issuer bank also holds the responsibility to authenticate the M-PIN set by the customer.
MAM	Minimum Amount
MCC	Merchant Category Code
MA	Merchant Account
Merchant	Merchant is an individual and / or a legal entity having a valid bank and / or e-money wallet account and has been allotted an MID under a particular MCC.
MID	Merchant Identifier
MTC	Mobile Telecommunications Company
NAD	Namibian Dollar
NAMFISA	Namibia Financial Institutions Supervisory Authority

NISS	Namibia Inter-Bank Settlement System
NPCI	National Payments Corporation of India
NPS	National Payment System
NPS Entity	A bank or an e-money provider which is allowed to acquire customers / merchants and provide payment services to individuals or businesses. An NPS entity provides an app to the customer / merchant and providing them the options to initiate / approve a financial transaction or non-financial request wherever necessary.
NREF	NamClear uses Unique 8-digit reference number, being human-readable and serves as a proxy for the information presented graphically.
NRTC	Near-Real-Time Credit payment
P2B	Person-to-Business
P2G	Person-to-Government
P2M	Person-to-Merchant
P2P	Person-to-Person
PAN	Payment Association of Namibia
PAN	Permanent Account Number
Payee	Payee is a Customer of an Issuer Entity who receives credit in her bank and / or e-money wallet account
Payer	Payer is a Customer of an Issuer Entity who authorizes debit to her bank and / or e-money wallet account in a payment transaction using 2FA
Payer Entity	A bank or an e-money provider that has been certified by NPS PSO to participate in NPS. All NPS users need to have a banking account with NPS enabled banks / e-money providers. While performing a P2P transaction, the user's bank account will be debited. The payer bank also holds the responsibility to authenticate the M-PIN set by the customer.
Payee Entity	Any credit going to an NPS user will be credited in the payee e-money wallet account. The e-money provider receiving the funds in NPS P2P transactions will be acting as a payee entity.
PF	Payment Facilitator
PII	Payment Instrument Issuer
PIX	Proprietary Application Identifier Extension
POI	Point of Interaction
POS	Point of Sale
POSC	Point of Sale Credit
POSD	Point of Sale Debit
PSM	Payment System Management
PSO	Payment System Operator
PSP	Payment Service Provider licensed by BoN and includes banks and Financial Institutions
QR	Quick Response
RID	Registered Application Provider Identifier
RFU	Reserved for Future Use
RTGS	Real Time Gross Settlement
SI	Standing Instruction
SHA	Secure Hash Algorithm
SOV	Store of Value Type e.g., bank account, card account, E-money
TLV	Tag – Length - Value
TPAP	Third-Party Application Provider

TPPP	Third-Party Payment Provider
TSD	Technical Specifications Document
UMN	Unique Mandate Number
UPI	Unified Payments Interface
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
UTF	Unicode Transformation Format
UUID	Universally Unique Identifier
VAE	Verified Address Entries

3. Executive Summary

The executive summary provides a brief overview of the NAMQR Code Standards which were developed in line with the Bank of Namibia's (the Bank) Strategy (2021-2024), to drive a digital transformation and modernised financial sector, the National Payment System (NPS) Vision and Strategy (2021-2025), under Theme 3: Consumer-Centric Innovation and the need by the NPS industry for standardised QR Codes. The Standards are based on the Bank's Guidelines, EMVCo QR Code standards, the Instant Payment Solution (IPS) QR specification document, and the Bank's relevant cybersecurity legal framework, among others and aims to ensure that payment QR codes are interoperable, safe, secure, and universally acceptable by all acquirers within the NPS and further promotes financial inclusion by enabling rural and informal vendors to accept digital payments, by expanding access to digital financial services.

The standardisation of the NAMQR Codes will promote payment choice, convenience, security as well as support interoperability across all payment streams, which facilitates a seamless user experience. These standards offer guidelines for the creation, encoding, and decoding of QR Codes, ensuring they are universally readable and optimised for performance. The detailed technical specifications provide for the establishment of a common structure and format for QR codes, including the length or size, error correction level, and encoding scheme, to ensure that they can be easily scanned and processed by various payment platforms.

The NAMQR Code will enhance the user experience by simplifying the process of initiating and accepting payments between customers and merchants. These Standards allow for the customisation of QR Codes while ensuring their scannability and helping to future-proof the technology as it evolves. Ultimately, the successful adoption of the NAMQR Code Standards will be defined by the simplicity, convenience, and security of making digital payments in Namibia.

4. NAMQR Code Specifications

4.1 Purpose

This section provides:

(a) A brief description of payee and payer presented NAMQR code payment, and the entities involved.
(b) The requirements on the NAMQR code displayed by the payee and payer, including format and content.

The processing of the NAMQR code by the mobile application and the network messages as a result of this processing are out of scope of this section.

4.2 High level transaction flows for Payee and Payer presented NAMQR code payments[1]

The granular details of the user journeys, functional specifications, the network message flows and formats, test and error case scenarios, alerts and calls to action for actual processing of the NAMQR code by the mobile application and / or USSD, are out of scope of this document.

4.3 Payee presented NAMQR code payment – using smart phone mobile banking application

The payee presented NAMQR code payment transaction enables payer to make payment using a payee generated and displayed NAMQR code based on the payee's details. For example, it can be used for a transfer of funds to a payee account designated by the payee account information over a payment network.

Payer is issued a mobile application that has the capability to scan the payee presented NAMQR code and initiate a payment transaction. This mobile application may be an existing mobile banking app offered by the Payer PSP or a third-party application provider. In both cases, the request to process the payment transaction is ultimately directed to the Payer PSP managing the account from which the funds will be withdrawn.

The Payer PSP receives the initial payment transaction and secures or withdraws the transaction amount from the payer's account.

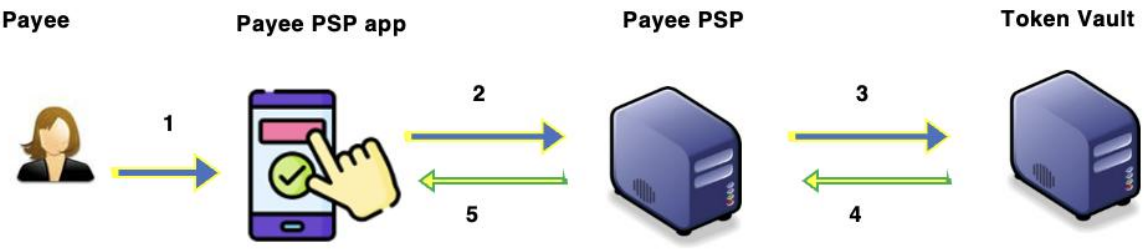
Upon receiving the payment transaction, the Payee PSP checks the validity of payee credentials (i.e., payee identifier alias value), resolves the payee identifier (if valid) to payee account information (e.g., bank account, e-money account, card account), credits the payment transaction amount associated with the payee account information, and sends notification of a successful transaction to payee. The Payer PSP also provides a notification to the payer (typically to their mobile application).

[1] Transaction flows shown here are for illustration purpose only and not specific to existing Namibia payment systems.

The payee presented NAMQR code payment (using smart phone mobile banking application) transaction flow is illustrated as follows:

Generation of NAMQR code with Payee Identifier and Token Vault Unique Identifier

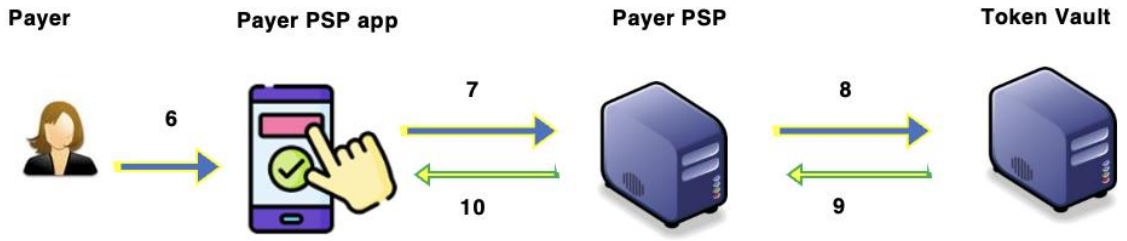
1. Payee initiates NAMQR code generation on payee PSP app and selects the bank account / e-money account / card account to be used for payment transaction (along with amount, transaction currency and any other parameters as required).
2. Payee PSP app sends 'Generate NAMQR' request to payee PSP.
3. Payee PSP assigns a payee identifier to the payee as an alias (e.g., payee mobile number as alias or any other unique number as assigned by payee PSP). The corresponding bank account / e-money account / card account details (selected at the time of NAMQR generation) are available at the payee PSP end mapped against the payee identifier. Payee PSP sends the parameters related to NAMQR to Token Vault [2]
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to payee PSP
5. Payee PSP generates NAMQR with the assigned Payee Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the payee PSP app (refer section 'NAMQR code payload data objects' for details of the parameters in NAMQR code)



Scanning of NAMQR code by payer PSP app and validation of NAMQR parameters through Token Vault

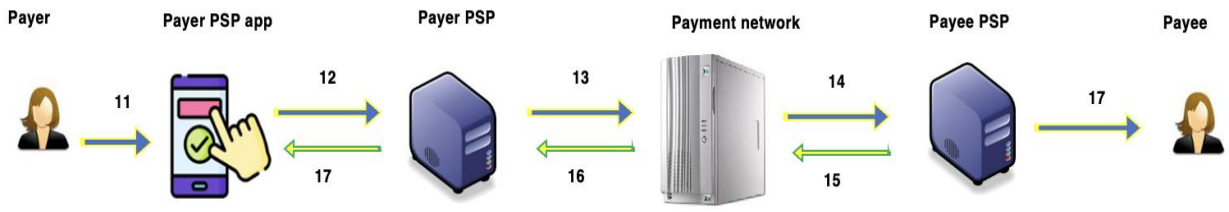
6. Payer scans NAMQR code using a mobile application (payer PSP app)
7. Payer PSP app sends the NAMQR code validation request to Payer PSP with list of NAMQR code parameters as scanned
8. Payer PSP sends the NAMQR code validation request to Token Vault
9. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault, and sends the NAMQR code validation successful response to payer PSP
10. Payer PSP sends the NAMQR code validation successful response to payer PSP app

[2] Token Vault may be hosted centrally or at bank side as per compliance with standard specifications



Transaction processing

11. Payer initiates and authenticates the transaction using 2FA on payer PSP app
12. Payer PSP app sends the transaction initiation request to payer PSP.
13. Payer PSP debits the payer account (based on the credentials) and sends transaction request [3] to payment network (e.g., NRTC, EnCR, IPP).
14. Payment network sends transaction request to payee PSP.
15. Payee PSP checks the validity of payee credentials (i.e., payee identifier alias value), resolves the payee identifier (if valid) to payee account information (e.g., bank account, e-money account, card account), credits the payment transaction amount associated with the payee account information and sends response to payment network.
16. Payment network sends response to payer PSP.
17. Payer PSP and payee PSP inform payer and payee respectively of the transaction outcome.



Different message flows are possible between the entities involved, depending on type of account (payer bank account or third-party e-money wallet) and the infrastructure supported by the payment network. Note that the specifics of this message flow from the mobile to the payment network is out of scope of this document.

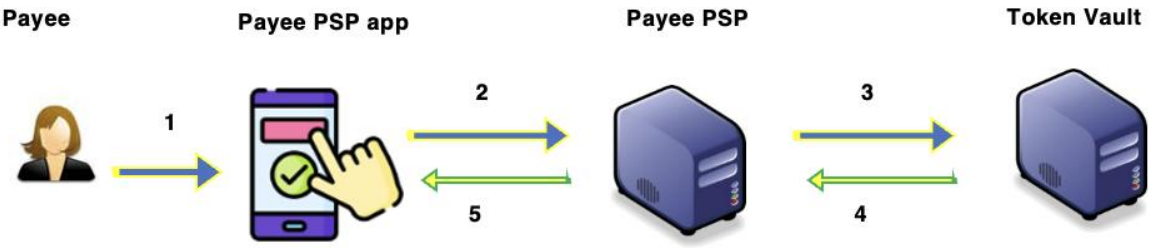
[3] The request from payer PSP to payment network can be sent as per the message format defined by the respective payment network (e.g., ISO 20022, ISO 8583, proprietary XML, etc) . For e.g., If NRTC is used to send the transaction, NRTC message formats shall be used for transmission of message from payer PSP to payment network and so on. Payer PSP app shall scan and read NAMQR code and populate the respective values in the request and send to payer PSP (as per the message format defined between payer PSP app and payer PSP switch), similarly payer PSP switch sends the request to payment network as per message format defined by the payment network. NAMQR code specifications only provides mechanism for payer PSP app to read data related to payee / merchant and does not affect the back-end transaction processing.

4.4 Payee presented NAMQR code payment (using USSD channel)

The payee presented NAMQR code payment (using USSD channel) transaction flow is illustrated as follows:

Generation of NAMQR code with Payee Identifier and Token Vault Unique Identifier

1. Payee initiates NAMQR code generation on payee PSP app and selects the bank account / e-money account / card account to be used for payment transaction (along with amount, transaction currency and any other parameters as required).
2. Payee PSP app sends 'Generate NAMQR' request to payee PSP.
3. Payee PSP assigns a payee identifier to the payee as an alias (e.g., payee mobile number as alias or any other unique number as assigned by payee PSP). The corresponding bank account / e-money account / card account details (selected at the time of NAMQR generation) are available at the payee PSP end mapped against the payee identifier. Payee PSP sends the parameters related to NAMQR to Token Vault [4]
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to payee PSP
5. Payee PSP generates NAMQR with the assigned Payee Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the payee PSP app (refer section 'NAMQR code payload data objects' for details of the parameters in NAMQR code)



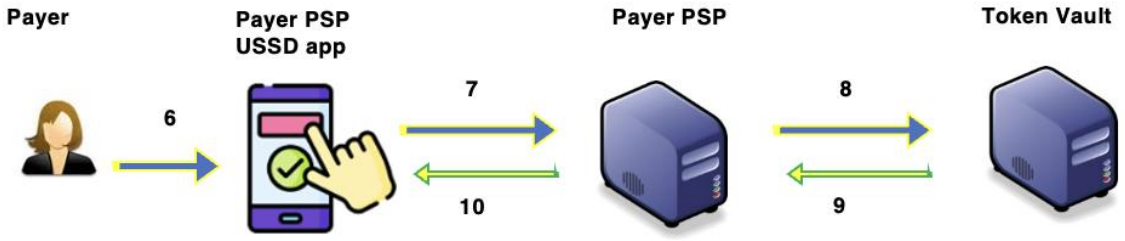
Token Vault Unique Identifier is displayed in text below QR code in case customer wants to make payment via USSD.

Payer enters Token Vault Unique Identifier in USSD menu and fetches NAMQR parameters through Token Vault

6. Payer enters Token Vault Unique Identifier in the respective menu using a USSD application (payer PSP USSD app)
7. Payer PSP USSD app sends the NAMQR code validation request to Payer PSP with Token Vault Unique Identifier
8. Payer PSP sends the NAMQR code validation request to Token Vault

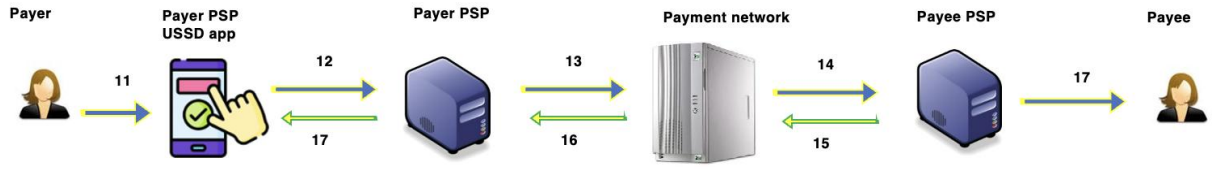
[4] Token Vault may be hosted centrally or at bank side as per compliance with standard specifications

9. Token Vault validates the Token Vault Unique Identifier, fetches NAMQR code parameters associated with Token Vault Unique Identifier, and sends the NAMQR code validation successful response to payer PSP along with NAMQR parameters
10. Payer PSP sends the NAMQR code validation successful response to payer PSP USSD app along with NAMQR parameters



Transaction processing

11. Payer initiates and authenticates the transaction using 2FA on payer PSP USSD app
12. Payer PSP USSD app sends the transaction initiation request to payer PSP.
13. Payer PSP debits the payer account (based on the credentials) and sends transaction request to payment network (e.g., NRTC, EnCR, IPP).
14. Payment network sends transaction request to payee PSP.
15. Payee PSP checks the validity of payee credentials (i.e., payee identifier alias value), resolves the payee identifier (if valid) to payee account information (e.g., bank account, e-money account, card account), credits the payment transaction amount associated with the payee account information and sends response to payment network.
16. Payment network sends response to payer PSP.
17. Payer PSP and payee PSP inform payer and payee respectively of the transaction outcome.



4.5 Payer presented NAMQR code payment – (Request to Pay)

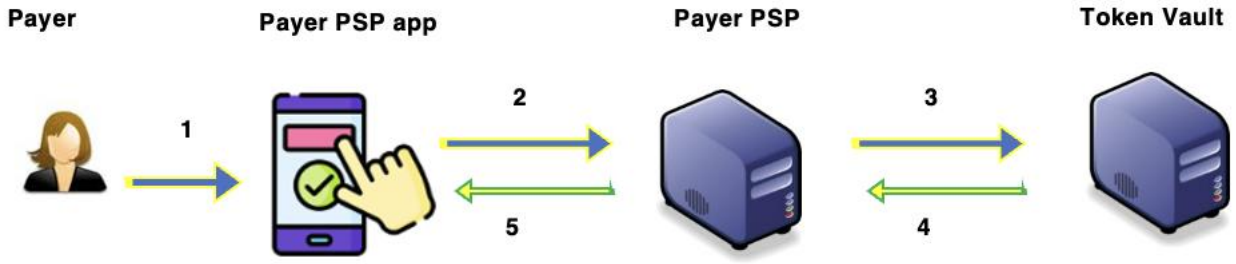
In a payer presented NAMQR Code transaction, payers can make payments—using credentials associated with their bank account / card account / e-money wallet and previously provisioned to their device—by selecting the NAMQR option for payment within their mobile application, which will result in the display of the NAMQR Code and having that NAMQR Code scanned at the time of payment to complete the transaction.

These transactions are always authorised online and given that the scanning of the NAMQR Code is a one-way transfer of data from the payer's device to the POI, the payload of the NAMQR Code does not contain any data from the POI.

The high-level solution architecture for the payer presented NAMQR code payment is as follows:

Generation of NAMQR code with Payer Identifier and Token Vault Unique Identifier

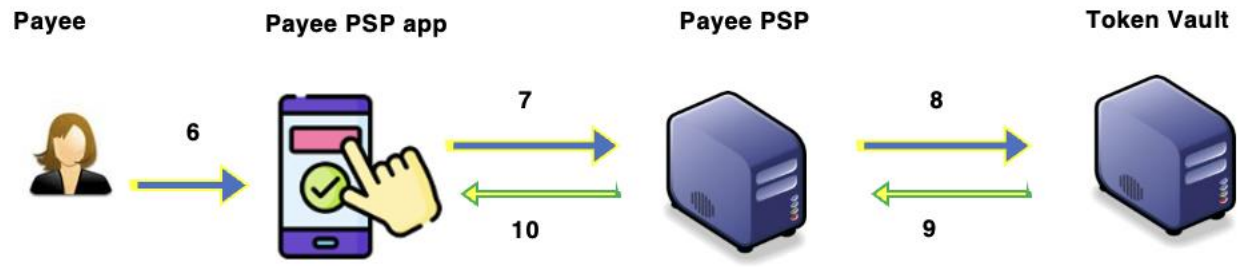
1. Payer initiates NAMQR code generation on payer PSP app and selects the bank account / e-money account / card account to be used for payment transaction (along with amount, transaction currency if required).
2. Payer PSP app sends 'Generate NAMQR' request to payer PSP.
3. Payer PSP assigns a payer identifier to the payer as an alias (e.g., payer mobile number as alias or any other unique number as assigned by payer PSP). The corresponding bank account / e-money account / card account details (selected at the time of NAMQR generation) are available at the payer PSP end mapped against the payer identifier. Payer PSP sends the parameters related to NAMQR to Token Vault [5]
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to payer PSP
5. Payer PSP generates NAMQR with the assigned Payer Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the payer PSP app (refer section 'NAMQR code payload data objects' for details of the parameters in NAMQR code)



Scanning of NAMQR code by payee PSP app and validation of NAMQR parameters through Token Vault

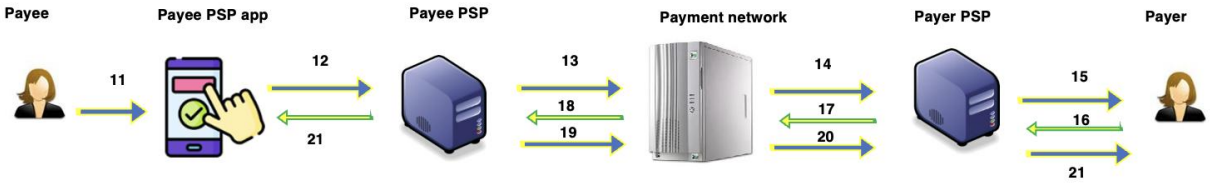
6. Payee scans NAMQR code using a mobile application (payee PSP app)
7. Payee PSP app sends the NAMQR code validation request to Payee PSP with list of NAMQR code parameters as scanned
8. Payee PSP sends the NAMQR code validation request to Token Vault
9. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault, and sends the NAMQR code validation successful response to payee PSP
10. Payee PSP sends the NAMQR code validation successful response to payee PSP app

[5] Token Vault may be hosted centrally or at bank side as per compliance with standard specifications



Transaction processing

11. Payee initiates the transaction
12. Payee PSP app sends the transaction initiation request to payee PSP.
13. Payee PSP sends transaction to payment network (e.g., IPP).
14. Payment network sends transaction to payer PSP.
15. Payer PSP checks the validity of payer credentials (i.e., payer identifier alias value), resolves the payer identifier (if valid) to payer account information (e.g., bank account, e-money account, card account), sends request to payer mobile to authenticate the transaction.
16. Payer views payee name and authenticates with M-PIN to pay through the bank account / e-money account / card account (selected at the time of NAMQR generation).
17. Payer PSP debits the payer account (based on the credentials) and sends transaction request to payment network.
18. Payment network sends transaction request to payee PSP.
19. Payee PSP credits the payee account and sends response to payment network.
20. Payment network sends response to payer PSP.
21. Payer PSP and payee PSP inform payer and payee respectively of the transaction outcome.



4.6 Strawman approach - Interoperable transaction from customer bank account on payment stream (e.g., NRTC, EnCR) to merchant on POSD stream [6]

Generation of NAMQR code with Merchant Identifier and Token Vault Unique Identifier

1. Merchant initiates NAMQR code generation on merchant app (e.g., POS terminal, ecommerce website) with amount, transaction currency.
2. Merchant app sends 'Generate NAMQR' request to Acquirer PSP.

[6] This conceptual flow is for illustration purpose only and can be customized as per actual respective payment stream specifications

3. Acquirer PSP assigns a merchant identifier to the merchant as an alias. The corresponding account details are available at the Acquirer PSP end mapped against the merchant identifier. Acquirer PSP sends the parameters related to NAMQR to Token Vault
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to Acquirer PSP
5. Acquirer PSP generates NAMQR with the assigned Merchant Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the merchant app (refer section 'NAMQR code payload data objects' for details of the parameters in NAMQR code)

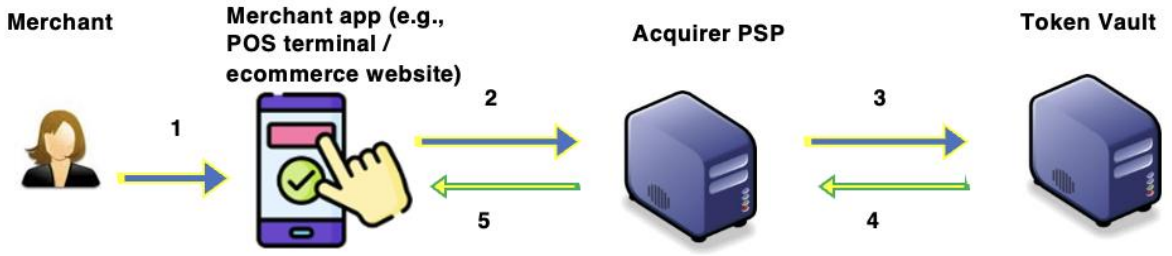
NAMQR parameters include the following:

Mandatory tags and parameters for static QR:

(00) – Payload format indicator
(01) – Point of initiation method
(02 - 16) – Tag to be followed by length and data as defined by card payment networks
(52) – Merchant category code
(58) – Country code
(59) – Payee name
(60) – Payee city
(65) – Token Vault Unique Identifier
(80) – Globally Unique Identifier, Initiation Mode
(63) – CRC

Additional tags and parameters for dynamic QR:

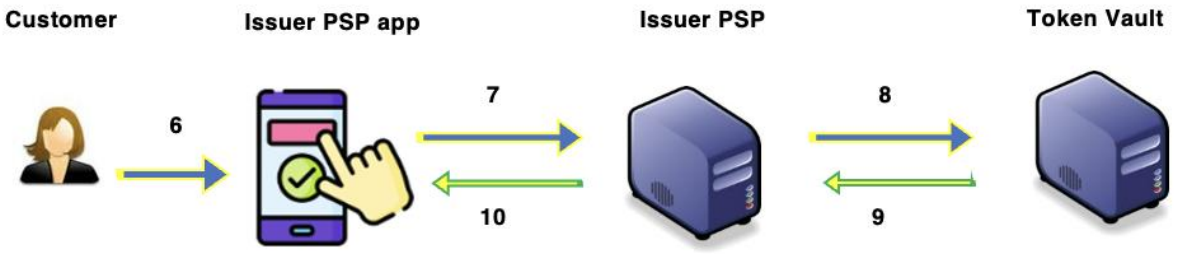
(53) – Transaction currency
(54) – Transaction amount
(62) – Reference label
(62) – Short description of the transaction
(81) – Globally unique identifier, invoice date, invoice name
(82) - NAMQR expiry date & time



Scanning of NAMQR code by Issuer PSP app and validation of NAMQR parameters through Token Vault

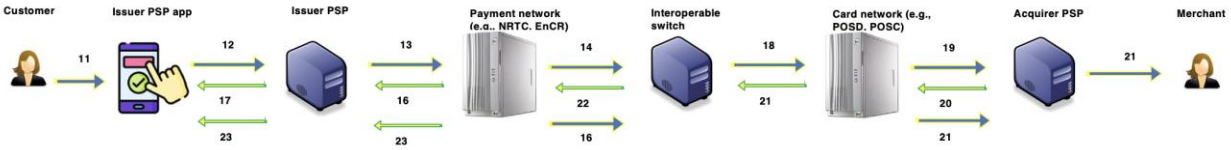
6. Customer scans NAMQR code using a mobile application (Issuer PSP app)

7. Issuer PSP app sends the NAMQR code validation request to Issuer PSP with list of NAMQR code parameters as scanned
8. Issuer PSP sends the NAMQR code validation request to Token Vault
9. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault, and sends the NAMQR code validation successful response to Issuer PSP
10. Issuer PSP sends the NAMQR code validation successful response to Issuer PSP app



Transaction processing

11. Customer initiates and authenticates the transaction using 2FA on Issuer PSP app
12. Issuer PSP app sends the transaction initiation request to Issuer PSP.
13. Issuer PSP debits the payer account (based on the credentials) and sends transaction request to payment network (e.g., NRTC, EnCR).
14. Based on the merchant identifier, payment network knows that the merchant belongs to card network and sends transaction request to interoperable switch.
15. Interoperable switch credits the interoperable account for payment network and sends response to payment network
16. Payment network sends response to Issuer PSP, and also sends transaction status confirmation to interoperable switch
17. Issuer PSP informs payer that transaction request has been received and they shall receive transaction status shortly
18. Interoperable switch debits the interoperable account for card network, translates to card network request and sends to card network switch (e.g., POSD, POSC)
19. Card network switch sends request to Acquirer PSP
20. Acquirer PSP checks the validity of merchant credentials (i.e., merchant identifier alias value), resolves the merchant identifier to merchant account information (e.g., bank account, card account), credits the payment transaction amount associated with the merchant account information and sends response to card network.
21. Card network sends response to interoperable switch, and also sends transaction status confirmation to Acquirer PSP switch. Acquirer PSP switch informs merchant of transaction status
22. Interoperable switch translates and sends response to payment network switch for the transaction status.
23. Payment network switch sends response to Issuer PSP to inform transaction status to the customer.



Settlement flow

1. Payment network (e.g., NRTC, EnCR) sends transaction data at the end of settlement cycle to interoperable switch operator
2. Similarly, card network (e.g., POSD, POSC) sends transaction data at the end of settlement cycle to interoperable switch operator
3. Interoperable switch operator performs reconciliation and takes action in case of any discrepancy (e.g., return, transaction credit confirmation)
4. Payment network performs settlement between Issuer PSP and interoperable switch operator settlement account (debit Issuer PSP settlement account and credit interoperable switch operator settlement account)
5. Similarly, card network performs settlement between interoperable switch operator settlement account and Acquirer PSP (debit interoperable switch operator settlement account and credit Acquirer PSP settlement account)

4.7 Strawman approach - Interoperable ATM cash withdrawal using IPP [7]

Customer selects “Cash Withdrawal using IPP” option on ATM and inputs the withdrawal amount

1. ATM sends request to Acquirer bank QR server / middleware
2. QR server / middleware sends request to Acquirer bank IPP switch
3. Acquirer bank IPP switch assigns a payee identifier to the payee as a full form alias. The corresponding bank account details are available at the acquirer bank end mapped against the payee identifier. Acquirer bank IPP switch sends the parameters related to NAMQR to Token Vault
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to Acquirer bank IPP switch
5. Acquirer bank IPP switch generates NAMQR dynamic QR with the assigned Payee Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and send it to QR server / middleware
6. QR server / middleware sends the dynamic QR data to ATM for displaying it on ATM.

NAMQR parameters include the following:

<u>Mandatory tags and parameters for static QR:</u>

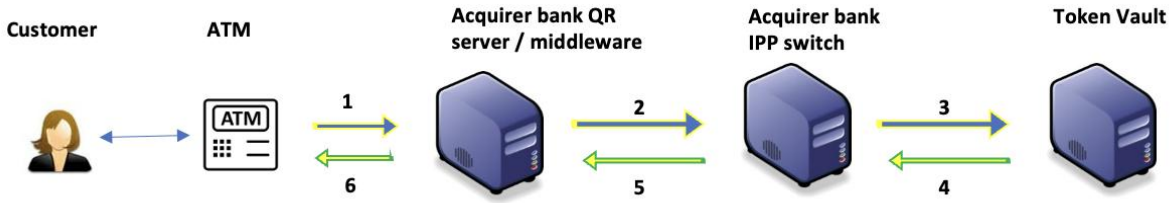
(00) – Payload format indicator
(01) – Point of initiation method
(26) - Globally Unique Identifier, Payee IPP full form alias
(52) – Merchant category code

[7] This conceptual flow is for illustration purpose only and can be customized as per actual respective payment stream specifications

(58) – Country code
(59) – Payee name
(60) – Payee city
(65) – Token Vault Unique Identifier
(80) – Globally Unique Identifier, Initiation Mode
(63) – CRC

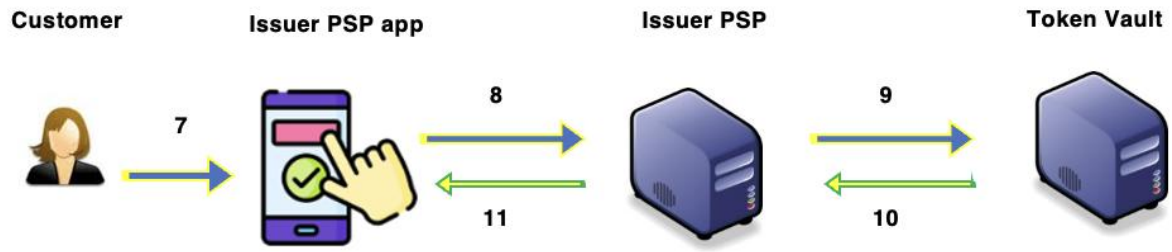
Additional tags and parameters for dynamic QR:

(27) – Transaction Reference
(53) – Transaction currency
(54) – Transaction amount
(62) – Short description of the transaction
(82) - NAMQR expiry date & time



Scanning of NAMQR code from any IPP enabled application and validation of NAMQR parameters through Token Vault

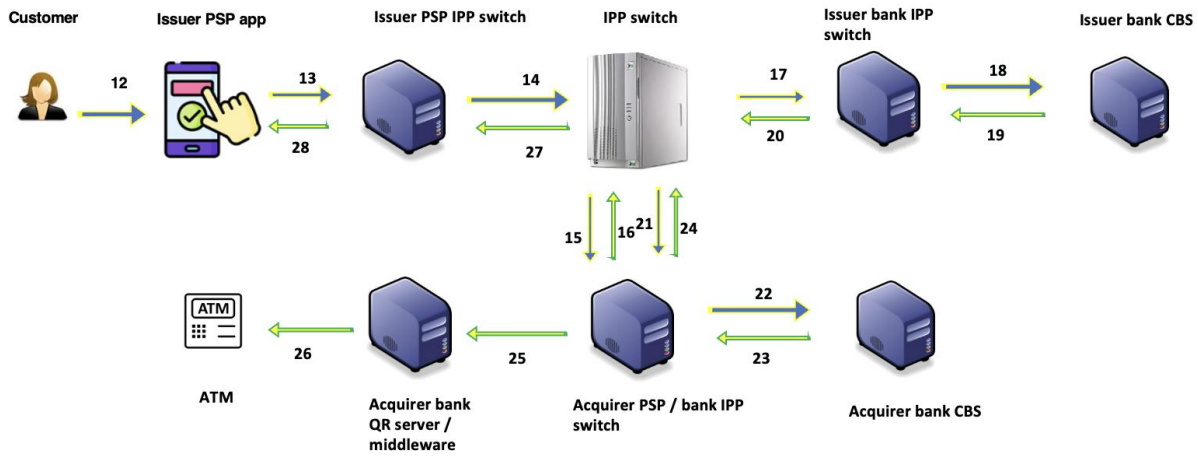
7. ATM would prompt customer to scan QR Code using any IPP app for Cash Withdrawal. Customer scans NAMQR code using a mobile application (Issuer PSP app)
8. Issuer PSP app sends the NAMQR code validation request to Issuer PSP with list of NAMQR code parameters as scanned
9. Issuer PSP sends the NAMQR code validation request to Token Vault
10. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault, and sends the NAMQR code validation successful response to Issuer PSP
11. Issuer PSP sends the NAMQR code validation successful response to Issuer PSP app



Transaction processing

12. '<BANK NAME> ATM CASH Withdrawal' i.e. Verified Payee Name on the IPP app along with the Amount shall be displayed - Customer to enter IPP PIN for authorisation

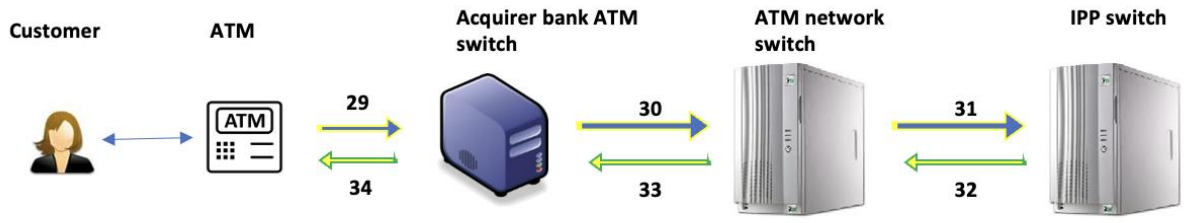
13. Issuer PSP app sends the transaction request to Issuer PSP
14. Issuer PSP shall validate the customer credentials & forwards the transaction to IPP switch. It shall be P2M in IPP
15. IPP switch sends the request to Acquirer bank IPP switch to resolve full form alias & return the Beneficiary Account No and BIN details (in this case it shall be office account of the Acquirer bank)
16. Acquirer bank IPP switch sends response to IPP switch
17. IPP switch sends the transaction to Issuer bank IPP switch,
18. IPP switch sends transaction it to its CBS for authorisation i.e. for debiting the customer account
    a. Based on the initiation mode / purpose, the Issuer bank shall know that it is an ATM cash withdrawal transaction
19. Issuer bank CBS responds to Issuer bank IPP switch
20. Issuer bank IPP switch responds to IPP switch
21. IPP switch sends the transaction response to Acquirer bank IPP switch
22. Acquirer bank IPP switch sends the transaction to Acquirer bank CBS for crediting the Office Account maintained for this purpose.
23. Acquirer Bank CBS responds to Acquirer bank IPP switch
24. Acquirer bank IPP switch responds to IPP switch.
25. Acquirer bank IPP switch (through QR server / middleware) to send notification to ATM for enabling FDK (Functional Display Key) for initiation of ATM cash withdrawal transaction
26. On receipt of the notification, ATM to display the next screen for customer to proceed with the cash withdrawal transaction
    a. "PROCEED: PRESS here for getting Cash" to be displayed at the FDK for informing the customer to press the button for getting cash. (Bank may suitability modify the text, if required)
27. IPP switch sends the confirmation to Payer PSP
28. Payer PSP displays the completion message on the customer's mobile i.e. IPP app



Once customer confirms to Proceed at the ATM for getting the cash

29. ATM sends the transaction to Acquirer bank ATM switch
30. Acquirer bank ATM switch sends the transaction to ATM network
31. ATM network checks the status of the transaction from IPP switch using the IPP transaction id and the Amount.

32. IPP switch to respond based on the final status of the transaction and return the customer Account No., BIN and IPP RRN.
33. ATM network responds to the Acquirer bank ATM switch. Customer Account No, BIN and IPP RRN shall be part of the response message
34. Acquirer bank ATM switch sends the response to ATM for dispensing cash. Cash is dispensed (for successful transactions)



Participation criteria

Issuers:

1. All IPP Issuer banks who are also ATM network Issuers can participate for offering interoperable cash withdrawal to their customers.

Acquirers:

1. ATM network Acquirers who are also IPP members or are sub-member of IPP member, can participate for offering interoperable cash withdrawal transactions at their ATMs.

Bank IPP apps and TPPPs:

1. All Bank IPP apps and TPPPs can participate for offering interoperable cash withdrawal transactions after certification with IPP.

Members can participate for offering interoperable cash withdrawal transactions after doing necessary changes (including reconciliation process) and certification with IPP.

Settlement and fund movement

In IPP:

1. There would be no fund movement in IPP settlement for cash withdrawal transaction amount
2. This transaction will be made available in IPP raw data files for reference with indicator as Initiation Mode

In ATM network:

1. Transactions shall be settled in ATM network along with the existing cash withdrawal transactions i.e. for Cash withdrawal amount, Interchange and Switching Fees.
2. These transactions shall be provided in settlement reports

3. Transaction shall be made available in existing ATM network raw data files
4. It shall have separate MCC i.e. 6013 (to be sent by Acquirer bank in online message) for identification of these transactions in RAW data files
5. Customer account no., BIN and IPP RRN shall be populated in existing fields in both the ATM network raw data files (i.e. Issuer and Acquirer raw data files) for facilitating reconciliation of these transactions.
6. Transactions in ATM network Issuer raw data files needs to be reconciled with Issuer Banks' CBS / IPP switch data files
7. The Office account used by Acquirer bank in IPP for credit leg is a notional / dummy account used for completion of IPP transaction. (It can be made EOD check account for nullifying the entries/amount at the end of the day)

4.8 Strawman approach - Interoperable transaction from customer bank account on NRTC payment stream to merchant on EnCR payment stream [8]

Generation of NAMQR code with Payer Identifier and Token Vault Unique Identifier

1. Customer initiates NAMQR code generation on Issuer PSP app and selects the bank account to be used for payment transaction (along with amount, transaction currency if required).
2. Issuer PSP app sends 'Generate NAMQR' request to Issuer PSP.
3. Issuer PSP assigns a payer identifier to the customer as an alias (e.g., payer mobile number as alias or any other unique number as assigned by Issuer PSP). The corresponding bank account details (selected at the time of NAMQR generation) are available at the Issuer PSP end mapped against the payer identifier. Issuer PSP sends the parameters related to NAMQR to Token Vault
4. Token Vault stores the NAMQR parameters and map them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to Issuer PSP
5. Issuer PSP generates NAMQR with the assigned Payer Identifier, Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the Issuer PSP app (refer section 'NAMQR code payload data objects' for details of the parameters in NAMQR code)

NAMQR parameters include the following:

<u>Mandatory tags and parameters for static QR:</u>

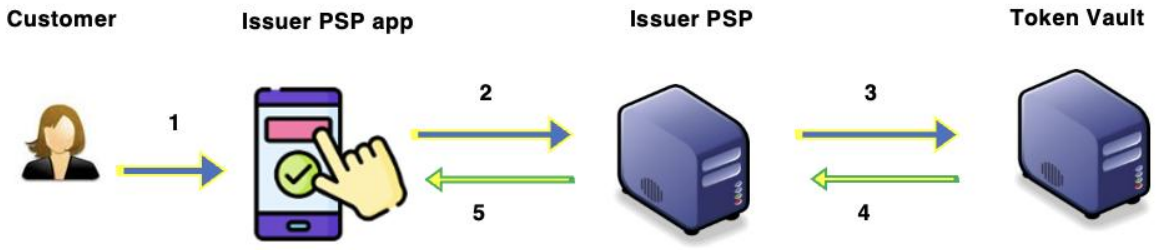
(00) – Payload format indicator
(01) – Point of initiation method
(28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias)
(52) – Merchant category code (with value '0000')
(58) – Country code
(59) – Payee name
(60) – Payee city
(65) – Token Vault Unique Identifier
(80) – Globally Unique Identifier, Initiation Mode

[8] This conceptual flow is for illustration purpose only and can be customized as per actual respective payment stream specifications.

(63) - CRC

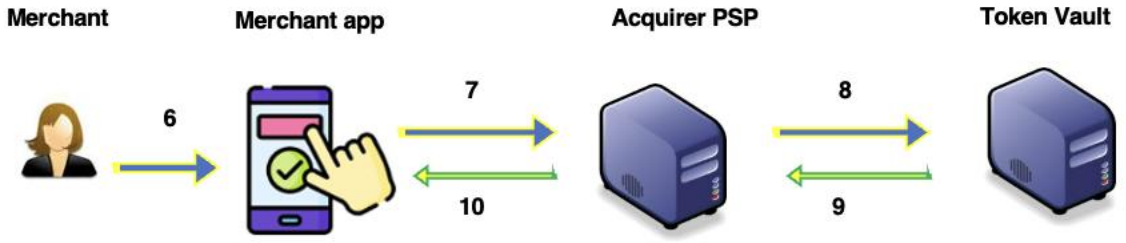
Additional tags and parameters for dynamic QR:

(53) – Transaction currency
(54) – Transaction amount
(62) – Reference label
(62) – Short description of the transaction
(82) - NAMQR expiry date & time



Scanning of NAMQR code by merchant app and validation of NAMQR parameters through Token Vault

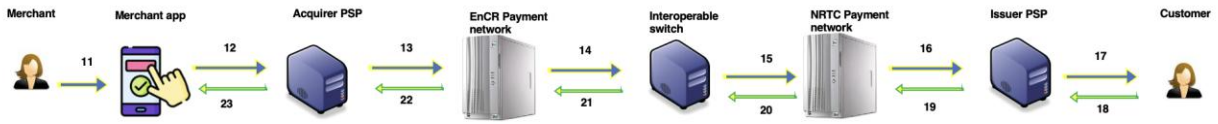
6. Merchant scans NAMQR code using a mobile application (merchant app)
7. Merchant app sends the NAMQR code validation request to Acquirer PSP with list of NAMQR code parameters as scanned
8. Acquirer PSP sends the NAMQR code validation request to Token Vault
9. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault, and sends the NAMQR code validation successful response to Acquirer PSP
10. Acquirer PSP sends the NAMQR code validation successful response to merchant app



Transaction processing

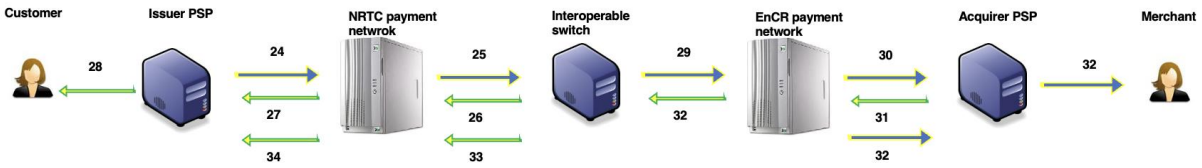
11. Merchant initiates the transaction
12. Merchant app sends the request to pay transaction initiation request to Acquirer PSP.
13. Acquirer PSP sends request to pay transaction to payment network (i.e., EnCR).
14. Based on the payer identifier, EnCR payment network knows that the customer belongs to NRTC payment stream and sends request to pay transaction request to interoperable switch.

15. Interoperable switch translates request to pay request to NRTC message format and sends request to NRTC payment network switch
16. NRTC payment network sends request to pay transaction to Issuer PSP.
17. Issuer PSP checks the validity of customer credentials (i.e., payer identifier alias value), resolves the payer identifier (if valid) to customer account information (e.g., bank account), sends request to customer mobile to authenticate the transaction.
18. Customer views merchant name and authenticates with M-PIN to pay through the bank account (selected at the time of NAMQR generation).
19. Issuer PSP sends request to pay transaction response to NRTC payment network.
20. NRTC Payment network sends request to pay transaction response to interoperable switch.
21. Interoperable switch sends request to pay transaction response to EnCR payment network
22. EnCR payment network sends request to pay transaction response to Acquirer PSP
23. Acquirer PSP informs merchant of the customer response



If customer approves the request, the transaction flow is as follows:

24. Issuer PSP debits the customer account (based on the credentials) and sends funds transfer transaction request to NRTC payment network
25. NRTC payment network sends funds transfer transaction request to interoperable switch.
26. Interoperable switch credits the interoperable account for payment network and sends response to NRTC payment network
27. NRTC payment network sends response to Issuer PSP, and also sends transaction status confirmation to interoperable switch
28. Issuer PSP informs payer that transaction request has been received and they shall receive transaction status shortly
29. Interoperable switch debits the interoperable account for EnCR payment network, translates to EnCR payment network request and sends to EnCR payment network switch
30. EnCR payment network switch sends request to Acquirer PSP
31. Acquirer PSP checks the validity of merchant credentials (i.e., merchant identifier alias value), resolves the merchant identifier to merchant account information (e.g., bank account, card account), credits the payment transaction amount associated with the merchant account information and sends response to EnCR payment network.
32. EnCR payment network sends response to interoperable switch, and also sends transaction status confirmation to Acquirer PSP switch. Acquirer PSP switch informs merchant of transaction status
33. Interoperable switch translates and sends response to NRTC payment network switch for the transaction status.
34. NRTC payment network switch sends response to Issuer PSP to inform transaction status to the customer.



Settlement flow

1. NRTC payment network sends transaction data at the end of settlement cycle to interoperable switch operator
2. Similarly, EnCR payment network sends transaction data at the end of settlement cycle to interoperable switch operator
3. Interoperable switch operator performs reconciliation and takes action in case of any discrepancy (e.g., return, transaction credit confirmation)
4. NRTC payment network performs settlement between Issuer PSP and interoperable switch operator settlement account (debit Issuer PSP settlement account and credit interoperable switch operator settlement account)
5. Similarly, EnCR payment network performs settlement between interoperable switch operator settlement account and Acquirer PSP (debit interoperable switch operator settlement account and credit Acquirer PSP settlement account)

4.9 NAMQR code payload data objects[9]

The data contained within a NAMQR code is organized as follows. Each data object is made up of three individual fields. The first field is a tag field by which the data object can be referenced. The second field is a length field that explicitly indicates the number of characters included in the third field i.e., the value field. A data object is then represented as a Tag - Length - Value (TLV) combination, where:

1. The tag is coded as a two-digit numeric value, with a value ranging from "00" to "99",
2. The length is coded as a two-digit numeric value, with a value ranging from "01" to "99",
3. The value field has a minimum length of one character and maximum length of 99 characters.

The Payload Format Indicator (tag 00) is the first data object. The tag 63 is cyclical redundancy check (CRC) and always the last object. The position of all other data objects is arbitrary and may appear in any order. Data objects within a template, such as the Additional Data Field Template (tag 62), may be placed in any position under their respective templates.

The format of a value field in a data object is either Numeric (N), Alphabetic (A), Alphanumeric (AN), Alphanumeric Special (ANS), or String (S). Note that Numeric is a subset of Alphanumeric Special and that Alphanumeric Special is a subset of String.

Alphanumeric format indicates that the data object may be coded using any characters from the [ISO 18004:2006-QR Code 2005 barcode symbology specs] alphanumeric mode, including the 9 symbol characters. Numeric format indicates the numeric decimal data 0-9 as defined in [ISO 18004:2006-QR Code 2005 barcode symbology specs].

[9] Refer document 'EMVCo-Merchant-Presented-QR-Specification-v1.1' and 'UPI Linking Specification cer 1 7 2_V12'

The length of the payload should not exceed 512 alphanumeric characters, and the number of characters should be reduced proportionally when multi-byte [Unicode] characters are used.

Note that, as data object values with a format of S may contain characters coded as UTF-8 and depending on the alphabet being used there may not be a one-to-one mapping of characters to bytes, special consideration would be needed to determine the number of bytes in the payload.

The table below lists the name of the data object, the tag of the data object, the length of the value field of the data object, the format of the value field of the data object, and whether the presence of the data object is Mandatory (M), Conditional (C), or Optional (O).

Following is the definition for the header used in the below table:

S - Static QR and **D** - Dynamic QR

4.10 Table: 1

Name	Tag	Format	Length	Presence		Description
				S	D	
Payload Format Indicator	00	N	02	M	M	Defines the version of the NAMQR template and the conventions on the tags, lengths and values. Payload Format Indicator is the first data object in the NAMQR code and allows the mobile application to determine the data representation of the remaining data included in the NAMQR code and how to parse the data. In this version of the specification, the Payload Format Indicator has the value "01". If this Payload Format Indicator has the value "99" (or any such value), then all tags as per existing EMVCo standards for customer presented card chip data to be followed (refer section 'EMVCo standards for customer presented card chip data').[10]
Point of initiation method	01	N	02	M	M	Identifies the communication technology (here QR code) and whether the data is static or dynamic. The Point of Initiation Method has the following values: 1. "11" for payee presented static NAMQR codes 2. "12" for payee presented dynamic NAMQR codes. 3. "13" for payer presented static NAMQR codes 4. "14" for payer presented dynamic NAMQR codes

[10] It must be noted that, EMVCo uses binary encoding for customer presented card chip data to generate QR code. We retained this protocol to ensure that this payment method is not excluded while developing NAMQR, by using value "99" (or any such value) in the tag "00" (in this case, all tags as per existing EMVCo standards for customer presented card chip data to be followed). To ensure compatibility with rest of QR code parameters which are only text based, EMVCo has provided mechanism for converting binary data to text data using base64 and encoding in a QR code. Hence, NAMQR parameters continue to have uniform text-based encoding despite including this particular EMVCo use case. It must be further noted that in all other use cases in these NAMQR specifications for Payer presented QR, only text-based encoding has been envisaged.

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>The value of "11" and “13” is used when the same NAMQR code is shown for more than one transaction (static NAMQR).
The value of "12" and “14” is used when a new NAMQR code is shown for every transaction (dynamic NAMQR).</td></tr>
<tr><td rowspan="18">Payee Account Information

Identifies the payee.

At least one Payee Account Information data object in the designated range of tags 02 to 51 shall be present.</td><td>02</td><td rowspan="18">ANS</td><td rowspan="18">Each variable up to 99</td><td rowspan="18">M</td><td rowspan="18">M</td><td>Tag to be followed by length and data as defined by Visa</td></tr>
<tr><td>03</td><td>Tag to be followed by length and data as defined by Visa</td></tr>
<tr><td>04</td><td>Tag to be followed by length and data as defined by Mastercard</td></tr>
<tr><td>05</td><td>Tag to be followed by length and data as defined by Mastercard</td></tr>
<tr><td>06</td><td>Tag to be followed by length and data as defined by Namibia domestic card scheme</td></tr>
<tr><td>07</td><td>Tag to be followed by length and data as defined by Namibia domestic card scheme</td></tr>
<tr><td>08</td><td>Tag to be followed by length and data as defined by NAMQR operator (as identified by the industry)</td></tr>
<tr><td>09</td><td>Tag to be followed by length and data as defined by Discover</td></tr>
<tr><td>10</td><td>Tag to be followed by length and data as defined by Discover</td></tr>
<tr><td>11</td><td>Tag to be followed by length and data as defined by American Express</td></tr>
<tr><td>12</td><td>Tag to be followed by length and data as defined by American Express</td></tr>
<tr><td>13</td><td>Tag to be followed by length and data as defined by JCB</td></tr>
<tr><td>14</td><td>Tag to be followed by length and data as defined by JCB</td></tr>
<tr><td>15</td><td>Tag to be followed by length and data as defined by UnionPay</td></tr>
<tr><td>16</td><td>Tag to be followed by length and data as defined by UnionPay</td></tr>
<tr><td>17</td><td>Template reserved payee presented NAMQR for existing Namibia payment system that does not use PAN or IPP full form alias as payee identifier - Tag to be followed by length and data as defined by existing payment system
<table>
<tr><th>Name</th><th>Tag</th><th>Format</th><th>Length</th><th colspan="2">Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
<tr><td>Globally Unique Identifier</td><td>00</td><td>ANS</td><td>Var. up to 32</td><td>M</td><td>M</td><td>A reverse domain name, as defined by existing payment system operator (e.g., na.com.namclear.nrtc).</td></tr>
<tr><td>Payee PSP Id</td><td>01</td><td>ANS</td><td>Var.</td><td>M</td><td>M</td><td>As defined by existing payment system</td></tr>
<tr><td>Payee Identifier</td><td>02</td><td>ANS</td><td>Var.</td><td>M</td><td>M</td><td>As defined by existing payment system</td></tr>
</table></td></tr>
</table>

						(ex, Mobile Number as alias)						
	18 - 25					Designated range of tags as defined by NAMQR operator (as identified by the industry) that are dynamically allocable.						
	26					Template reserved for IPP payee full form alias reference						
						Name	**Tag**	**Format**	**Length**	**Presence**		**Description**
										S	**D**	
						Globally Unique Identifier	00	ANS	Var. up to 32	M	M	An Application Identifier (AID) consisting of RID registered with ISO as defined by ISO 7816-5, or a UUID without the hyphen (-) separators or a reverse domain name, as defined by IPP operator (e.g., na.com.operator.IPP).
						Payee IPP full form alias	01	ANS	Var. up to 50	M	M	IPP full form alias can only contain "@" and any other special characters as may be defined in the IPP specifications.
						Org Id	02	N	6 – 12	O	O	Org Id of the payee PSP. In case of international NAMQR (i.e., Purpose = 11), this parameter shall contain international institution id. Mandatory in string only w.r.t. use case of signing and international, else optional.
						Merchant Id	03	AN	Var. up to 20	C	M	Merchant Id shall be passed in this tag. Parameter mandatory for international NAMQR (i.e.,

												Purpose = 11) and optional otherwise If “Point of initiation method = 13 or 14”, this parameter is not required.
						Minimum amount	04	N	Var. up to 13	O	O	Minimum amount to be defined by payee PSP and is minimum amount to be paid if different from transaction amount. If minimum amount tag is populated and transaction amount value is non-zero (dynamic), then transaction amount is editable. If the minimum amount tag is not present or is null or blank, then transaction amount field should NOT be editable. Note: if a payer enters the value less than value passed in minimum amount, then IPP will decline the transaction. To reduce such declines, payer PSP application should not allow entry of amount below minimum amount value. Minimum amount field is limited to numeric and the "." symbol. For IPP transactions, minimum amount is defined

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>only up to 2 decimal numbers i.e., “99.12’’.
It should always be an NAD value greater than zero.</td></tr>
<tr><td></td><td>27</td><td></td><td></td><td></td><td></td><td colspan="8">Template reserved for IPP payee full form alias reference</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Name</td><td>Tag</td><td>Format</td><td>Length</td><td>Presence</td><td></td><td>Description</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Globally Unique Identifier</td><td>00</td><td>ANS</td><td>Var. up to 32</td><td>M</td><td>M</td><td>An Application Identifier (AID) consisting of RID registered with ISO as defined by ISO 7816-5, or a UUID without the hyphen (-) separators or a reverse domain name, as defined by IPP operator (e.g., na.com.operator.IPP).</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Transaction Reference</td><td>01</td><td>AN</td><td>Var. up to 35</td><td>O</td><td>M</td><td>Transaction Reference Id. This could be the order number, subscription number, bill Id, booking Id, insurance renewal reference, etc. specific to IPP transactions only.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Reference URL</td><td>02</td><td>S</td><td>Var. up to 25</td><td>O</td><td>O</td><td>All Symbols can be used for URL. This should be a URL, when clicked, provides customer with further transaction details like complete bill details, bill copy, order copy, ticket details, etc. This can also be used to deliver digital goods such as mp3 files etc. after payment. This URL, when used, MUST BE related to the particular</td></tr>
</table>

												transaction and MUST NOT be used to send unsolicited information that are not relevant to the transaction.
						Category	03	N	2	C	C	Mandatory in case Reference URL is present 01 – Advertisement 02 – Invoice
	28					Template reserved payer presented NAMQR (i.e., Point of initiation method = 13 and 14) for existing Namibia payment system that does not use PAN or IPP full form alias as payer identifier - Tag to be followed by length and data as defined by existing payment system						
						Name	**Tag**	**Format**	**Length**	**Presence**		**Description**
										S	**D**	
						Globally Unique Identifier	00	ANS	Var. up to 32	M	M	A reverse domain name, as defined by existing payment system operator (e.g., na.com.namclear.nrtc).
						Payer PSP Id	01	ANS	Var.	M	M	As defined by existing payment system
						Payer Identifier (ex, Mobile Number as alias)	02	ANS	Var.	M	M	As defined by existing payment system
	29					Template reserved for payer presented NAMQR (i.e., Point of initiation method = 13 and 14) for IPP payer full form alias reference						
						Name	**Tag**	**Format**	**Length**	**Presence**		**Description**
										S	**D**	
						Globally Unique Identifier	00	ANS	Var. up to 32	M	M	An Application Identifier (AID) consisting of RID registered with ISO as defined by ISO 7816-5, or a UUID without the hyphen (-) separators or a reverse

												domain name, as defined by IPP operator (e.g., na.com.operator.IPP).
						Payer IPP full form alias	01	ANS	Var. up to 50	M	M	IPP full form alias can only contain "@" and any other special characters as may be defined in the IPP specifications.
	30-51					Designated range of tags as defined by NAMQR operator (as identified by the industry) that are dynamically allocable.						
Merchant Category Code	52	N	04	M	M	Merchant Category Code (MCC) of the payee as defined by [ISO 18245] and assigned by the Payee PSP. Merchant presented NAMQR code must contain non-zero MCC i.e., 'XXXX' assigned by the Acquirer PSP. Payee presented NAMQR code contains MCC '0000'. Payer presented NAMQR code (i.e., Point of initiation method = 13 and 14) contains MCC '0000'						
Transaction Currency	53	N	03	C	C	Indicates the currency code of the transaction. A 3-digit numeric value, as defined by [ISO 4217]. This value will be used by the mobile application to display a recognizable currency to the payer whenever an amount is being displayed or whenever the payer is prompted to enter an amount. If "Purpose = 11", this parameter is optional. If "Point of initiation method = 13", this parameter is not required. If "Point of initiation method = 14" and for other scenarios, this parameter is mandatory.						
Transaction Amount	54	ANS	Variable up to 13	O	C	The transaction amount (excluding convenience fees and VAT etc.), if known. For instance, "99.34". If present, this value is displayed to the payer by the mobile application when processing the transaction. If this data object is not present, the payer is prompted to input the transaction amount to be paid to the payee. This amount is expressed as how the value appears, amount "100.00" is defined as "100.00", or amount "99.85" is defined as "99.85". Transaction amount is defined only up-to 2 decimal numbers i.e., "99.12'' (as aligned with currency exponent associated with Namibia currency code defined in ISO 4217).						

						Transaction amount shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the amount includes decimals, the "." character shall be used to separate the decimals from the integer value and the "." character may be present even if there are no decimals. The above describes the only acceptable format for the Transaction Amount. It cannot contain any other characters (for instance, no space character can be used to separate thousands). The following are examples of valid Transaction Amounts: "98.73", "98" and "98.". The following are NOT valid Transaction Amounts: "98,73" and "3 705". Note: 0 is not a valid value. If transaction amount is not present (static) or if minimum amount is populated and transaction amount value is non-zero (dynamic), then transaction amount is editable. It should always be a final debit amount in NAD. If “Purpose = 11”, this parameter is optional. If “Point of initiation method = 13”, this parameter is not required. If “Point of initiation method = 14”: if present, this value is displayed to the payee by the mobile application when processing the transaction. If this data object is not present, the payee is prompted to input the transaction amount to be received from the payee.
Tip or convenience indicator	55	N	02	O	O	Indicates whether the customer will be prompted to enter a tip or whether the merchant has determined that a flat, or percentage, convenience fee is charged. A value of 01 shall be used if the mobile application should prompt the customer to enter a tip to be paid to the merchant A value of 02 shall be used to indicate inclusion of the data object Value of Convenience Fee Fixed (tag 56) A value of 03 shall be used to indicate inclusion of the data object Value of Convenience Fee Percentage (tag 57) Note that even if the Transaction Amount is not present in the NAMQR code, this data object may still be present. If “Point of initiation method = 13”, this parameter is not required. If “Point of initiation method = 14”: Indicates if payer has determined that a flat, or percentage, convenience fee is to be paid to the payee. A value of 02 shall be used to indicate inclusion of the data object Value of Convenience Fee Fixed

						(tag 56). A value of 03 shall be used to indicate inclusion of the data object Value of Convenience Fee Percentage (tag 57).
Value of convenience fee fixed	56	ANS	Variable up to 13	C	C	The fixed amount convenience fee when Tip or Convenience Indicator indicates a flat convenience fee. For example, "9.85", indicating that this fixed amount (in the transaction currency) will be charged on top of the transaction amount. The Value of Convenience Fee Fixed shall be present and different from zero if the data object Tip or Convenience Indicator (tag 55) is present with a value of 02. Otherwise, this data object shall be absent. If present, the Value of Convenience Fee Fixed shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the Value of the Convenience Fee Fixed includes decimals, the "." character shall be used to separate the decimals from the integer value. The "." character may be present even if there are no decimals. This amount is expressed as how the value appears, amount “100.00” is defined as “100.00”, or amount “99.85” is defined as “99.85”. Value of Convenience Fee Fixed is defined only up-to 2 decimal numbers i.e., “99.12’’ (as aligned with currency exponent associated with Namibia currency code defined in ISO 4217). The above describes the only acceptable format for the Value of Convenience Fee Fixed. It cannot contain any other characters (for instance, no space character can be used to separate thousands). Note: 0 is not a valid value. If “Point of initiation method = 13”, this parameter is not required. If “Point of initiation method = 14”: the fixed amount convenience fee when Tip or Convenience Indicator indicates a flat convenience fee.
Value of convenience fee percentage	57	ANS	Variable up to 05	C	C	The percentage convenience fee when Tip or Convenience Indicator indicates a percentage convenience fee. For example, "3.00" indicates that a convenience fee of 3% of the transaction amount will be charged, on top of the transaction amount. The Value of Convenience Fee Percentage shall be present if the data object Tip or Convenience Indicator (tag 55) is present with a value of 03 and only values between “00.01” and “99.99” shall be used. Otherwise, this data object shall be absent.

						If present, the Value of Convenience Fee Percentage shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the Value of the Convenience Fee Percentage includes decimals, the "." character shall be used to separate the decimals from the integer value and the "." character may be present even if there are no decimals. The Value of Convenience Fee Percentage shall not contain any other characters. For example, the "%" character must not be included. The above describes the only acceptable format for the Value of Convenience Fee Percentage. If "Point of initiation method = 13", this parameter is not required. If "Point of initiation method = 14": the percentage convenience fee when Tip or Convenience Indicator indicates a percentage convenience fee.
Country Code	58	AN	02	M	M	Indicates the country of the payee acceptance device. A 2-character alpha value, as defined by [ISO 3166-1 alpha 2] and assigned by the payee PSP. If "Point of initiation method = 13 or 14", this parameter indicates the country of the payer.
Payee Name	59	ANS	Variable up to 25	M	M	The name of the payee. The "doing business as" name for the merchant. If "Point of initiation method = 13 or 14", this parameter indicates the name of the payer.
Payee City	60	AN	Variable up to 15	M	M	City of operations for the payee. If "Point of initiation method = 13 or 14", this parameter indicates the city of operations for the payer.
Postal Code	61	AN	Variable up to 10	O	O	If present, the Postal Code should indicate the postal code of the payee's physical location. If "Point of initiation method = 13 or 14", this parameter indicates the postal code of the payer's physical location (if present).
Additional Data Field	62	ANS	Variable up to 99	O	O	If "Point of initiation method = 13", this template is not required. This template includes information that may be provided by the payee or may be requested from the payer to enable or facilitate certain use cases. Each of the data objects in below table with tags 01 to 08 can be used in two ways: either the payee can provide both the tag and its meaningful value, or the payee can include the tag with a special value to have the mobile application prompt the payer to input this information.

To prompt the payer for one or each of these values, the payee includes the respective tags in this template with a length of 3 and with a value equal to ***. When the payer is prompted by the mobile application to enter a value for each of these data objects, the length of the value to be entered should not exceed the length as indicated in below table, and overall, it should not exceed the length of 99 characters for the total size of the Additional Data Field.
The payee PSP / payee should provide only minimum information in order to avoid making the size of data onerous.
If present, the Additional Data Field Template shall contain at least 1 data object.
If present, each of the three positions in the Payee Channel (tag 11) identifies a characteristic of the channel used for a particular transaction. The values defined and meaning of the values are listed below.

Payee Channel: First Character – Media

This field indicates the Source channel i.e., creation point of the NAMQR.

Value	Meaning
0	Print – Merchant sticker
1	Print – Bill / Invoice
2	Print – Magazine / Poster
3	Print – Other
4	Screen / Electronic – Merchant POS / POI
5	Screen / Electronic – Website
6	Screen / Electronic – App
7	Screen / Electronic – Other
8	Screen / Electronic – ATM
9	Screen / Electronic – Pick from Gallery [11]

Payee Channel: Second Character – Transaction Location

Value	Meaning
0	At payee premises / registered address
1	Not at payee premises / registered address
2	Remote Commerce
3	Other

Payee Channel: Third Character – Payee Presence

[11] Applicable only to Issuer PSP to identify and pass

Value	Meaning
0	Attended POI
1	Unattended
2	Semi-attended (self-checkout)
3	Other

Examples of Payee Channel use cases

Use case	Media	Transaction Location	Merchant presence	Value
Retail outlet	Screen (Merchant POS)	At merchant	Attended	400
	Print (Merchant sticker)			000
Retail outlet self-checkout	Screen (Merchant POS)	At merchant	Semi-attended	402
	Print (Merchant sticker)			002
Vending machine, petrol station	Screen (Merchant POS)	At merchant	Unattended	401
	Print (Merchant sticker)			001
Street vendors, markets	Screen (App)	Not at merchant	Attended	610
	Print (Merchant sticker)			010
Ecommerce / Website	Screen (Website)	Remote	Unattended	521
Bill payment	Print (Bill / Invoice)	Not at merchant	Unattended	111
Magazine / poster	Print (Magazine / Poster)	Not at merchant	Unattended	211
Person-to-Person proximity	Screen / Electronic – App	At payee	Attended	600
Person-to-Person remote	Screen / Electronic – Pick from Gallery	Not at payee	Unattended	911

The data object with the tag 09 contains one or more values that indicate to the mobile application the data to provide as part of the transaction initiation request. This data should already be known by the mobile application, and the payer should not be unnecessarily prompted for the data.
One or more of the following characters may appear in the Additional Payer Data Request (tag 09), to indicate that the corresponding data should be provided in the transaction initiation to complete the transaction:

- "A" = Address of the payer
- "M" = Mobile number of the payer
- "E" = Email address of the payer

If more than one character is included, it means that each data object corresponding to the character is required to complete the transaction. Note that each unique character should appear only once.

Name	Tag	Format	Length	Presence		Description
				S	D	
Bill number	01	ANS	Var. up to 25	C	C	The invoice number or bill number. This number could be provided by the merchant or could be an indication for the mobile application to prompt the customer to input a Bill Number. For example, the Bill Number may be present when the NAMQR code is used for bill payment. If this tag is present, app should display the value to the customer. Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise.

						Mobile number	02	ANS	Var. up to 25	O	O	The mobile number could be provided by the payee or could be an indication for the mobile application to prompt the payer to input a Mobile Number. For example, the Mobile Number to be used for multiple use cases, such as mobile top-up and bill payment.
						Store label	03	ANS	Var. up to 25	O	O	A distinctive value associated to a store. This value could be provided by the merchant or could be an indication for the mobile application to prompt the customer to input a Store Label. For example, the Store Label may be displayed to the customer on the mobile application identifying a specific store. Store id will be passed in this field. Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise. If “Point of initiation method = 13 or 14”, this parameter is not required.
						Loyalty number	04	ANS	Var. up to 25	O	O	Typically, a loyalty card number. This number could be provided by the

												merchant, if known, or could be an indication for the mobile application to prompt the customer to input their Loyalty Number.
						Reference label	05	ANS	Var. up to 25	O	O	Any value as defined by the payee or payee PSP in order to identify the transaction. This value could be provided by the payee or could be an indication for the mobile app to prompt the payer to input a Reference Label. For example, the Reference Label may be used by the payer mobile application for transaction logging or receipt display.
						Customer label	06	ANS	Var. up to 25	O	O	Any value identifying a specific customer. This value could be provided by the merchant (if known) or could be an indication for the mobile application to prompt the customer to input their Customer Label. For example, the Customer Label may be a subscriber Id for subscription services, a student enrolment number, etc.
						Terminal label	07	ANS	Var. up to 25	O	O	A distinctive value associated to a terminal in the store. This value could be provided by the

												merchant or could be an indication for the mobile application to prompt the customer to input a Terminal Label. For example, the Terminal Label may be displayed to the customer on the mobile application identifying a specific terminal. Terminal id will be passed in this field. Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise. If “Point of initiation method = 13 or 14”, this parameter is not required.
						Short description of the transaction	08	ANS	Var. up to 25	O	O	Any value providing short description of the transaction. This value could be provided by the payee or could be an indication for the mobile application to prompt the payer to input a value providing short description of the transaction. For example, the short description of Transaction may have the value "International Data Package" for display on the mobile application.

												In the case of IPP transactions, this tag will be used for TN (i.e., Transactions Note which provides short description of the transaction).
						Additional Payer Data Request	09	ANS	Var. up to 3	O	O	Contains indications that the mobile application should include the requested information in order to complete the transaction. The information requested should be provided by the mobile application in the authorization without unnecessarily prompting the payer. For example, the Additional Payer Data Request may indicate that the payer mobile number is required to complete the transaction, in which case the mobile application should be able to provide this number (that the mobile application has previously stored) without unnecessarily prompting the payer.
						Merchant Tax Id	10	ANS	Var. up to 20	O	O	The tax identification number of the merchant, assigned by the Namibia governmental body.
						Payee channel	11	ANS	3	O	O	A payee channel establishes the

												environment in which a NAMQR code is presented to the payer. Covering use cases such as retail outlet, Ecommerce, bill payment with the purpose of improving transaction reporting. A three-character value that corresponds to the method used to present the NAMQR code by the payee including: display method, transaction location and payee presence.
						Designated range of tags	12 - 49	S	Var.	O	O	As defined by NAMQR operator (as identified by the industry) that are dynamically allocable
						Payment Link	50	S	Var.	O	O	
						Name	**Tag**	**Format**	**Length**	**Presence**		**Description**
										S	**D**	
						Globally Unique Identifier	00	ANS	Var. up to 32	M	M	An identifier that sets the context of the data that follows “com.mastercard“ value to be used with length 14
						Payment link	01	S	Var.	O	O	Tag 01 will be used for the payment link **preceded and ended by a space**. The payment link is either the static or dynamic one depending on the implementation model.

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>The length will depend on the number of characters in the payment link with 2 additional character accounting for the spaces
Note: only 1 Payment Link or URL is allowed per NAMQR Code</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Designated range of tags</td><td>51 – 99</td><td>S</td><td>Var.</td><td>O</td><td>O</td><td>As defined by NAMQR operator (as identified by the industry) that are dynamically allocable</td></tr>
<tr><td>Payee Information - Language Template</td><td>64</td><td>S</td><td>Var. up to "99"</td><td>O</td><td>O</td><td colspan="7">This template includes the language preference, one payee name and city in the Payee’s local language. This information is used for representation.
The Payee Information—Language Template includes payee information in an alternate language and may use a character set different from the Common Character Set. It provides an alternative to the payee information.
These data objects may be used by a mobile application to present the payee information in an alternate language.
If this template is present, it shall contain the Language Preference (tag 00) and Payee Name—Alternate Language (tag 01).
It may contain the Payee City—Alternate Language (tag 02).
The data objects with tags 01 and 02, if present, are defined with a format of String, so therefore may contain a different character set.
The equivalent data objects ‘Payee Name’ (tag 59) and ‘Payee City’ (tag 60) are defined with a format of Alphanumeric Special, and as such can only contain the Common Character Set.
All other tags within the Payee Information—Language Template are RFU for EMVCo.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Name</td><td>Tag</td><td>Format</td><td>Length</td><td colspan="2">Presence
S D</td><td>Description</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Language Preference</td><td>00</td><td>ANS</td><td>2</td><td>M</td><td>M</td><td>Identifies the alternate language used in the Payee Information—Language Template.</td></tr>
</table>

												Language Preference shall contain 2 alphabetical characters coded to a value defined by [ISO 639]. The value should represent the single language used to encode the Payee Name—Alternate Language and the optional Payee City—Alternate Language.
						Payee Name – Alternate Language	01	S	Var. up to 25	M	M	Indicates the payee's name in the alternate language. The Payee Name—Alternate Language shall be present. The Payee Name—Alternate Language should indicate the "doing business as" name for the merchant in the merchant's local language. If "Point of initiation method = 13 or 14", this parameter indicates the name of the payer.
						Payee City – Alternate Language	02	S	Var. up to 15	O	O	Indicates the payee city in the alternate language. If present, the Payee City—Alternate Language should indicate the city in which the payee transacts in the payee's local language. If "Point of initiation method = 13 or 14", this parameter indicates the city of operations for the payer.

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>RFU for EMVCo</td><td>03 – 99</td><td>S</td><td>Var.</td><td>Data objects reserved for EMVCo</td><td>Data objects in this range are reserved for future use for EMVCo.</td></tr>
<tr><td>Token Vault Unique Identifier[12]</td><td>65</td><td>N</td><td>xx</td><td>M</td><td>M</td><td colspan="6">xx-digit unique identifier for NAMQR code received from Token Vault</td></tr>
<tr><td>Digital Signature</td><td>66</td><td>ANS</td><td>Var. up to 99</td><td>C</td><td>C</td><td colspan="6">Digital Signature needs to be passed in this tag.
It is used for Securing the NAMQR.
Parameter mandatory for domestic NAMQR for IPP app-based transactions.
Parameter optional for domestic NAMQR for IPP USSD based transactions.
Parameter optional for domestic NAMQR for non-IPP transactions or interoperable IPP transactions with existing Namibia payment system.
Parameter optional for international NAMQR (i.e., Purpose = 11).
Parameter optional for payer presented NAMQR (i.e., Point of initiation method = 13 and 14).
Parameter optional for customer presented NAMQR (card chip data).</td></tr>
<tr><td>RFU for EMVCo</td><td>67 – 79</td><td>S</td><td>Each var. up to 99</td><td>O</td><td>O</td><td colspan="6">Data objects reserved for EMVCo</td></tr>
<tr><td>Unreserved template</td><td>80</td><td>ANS</td><td>Var. up to 99</td><td>M</td><td>M</td><td colspan="6">To add fields that are present in IPP Deep Linking Specifications but not present in EMVCo specifications
<table>
<tr><th>Name</th><th>Tag</th><th>Format</th><th>Length</th><th colspan="2">Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
<tr><td>Globally Unique Identifier</td><td>00</td><td>ANS</td><td>Var. up to 32</td><td>M</td><td>M</td><td>A reverse domain name, as defined by NAMQR operator (e.g., na.com.operator.namqr).</td></tr>
<tr><td>Initiation Mode</td><td>01</td><td>N</td><td>2</td><td>M</td><td>M</td><td>01 = Static NAMQR Code (Offline)
02 = Static Secure NAMQR Code (Offline)</td></tr>
</table></td></tr>
</table>

[12] NamClear has proposed NREF as their Token Vault Unique Identifier.

												13 = Static Secure NAMQR Mandate (Offline) 15 = Dynamic QR Code (Offline) 16 = Dynamic Secure QR Code (Offline) 17 = Dynamic Secure QR Mandate (Offline) 18 = ATMQR (Dynamic) 19 = Online STATIC QR Code 20 = Online STATIC Secure QR Code 21 = Online Static QR Mandate 22 = Online Dynamic QR Code 23 = Online Dynamic Secure QR Code 24 = Online Dynamic Secure QR Code Mandate
						Purpose	02	N	2	C	C	01 – NAMFISA 02 – AMC 03 – Travel 04 – Hospitality 05 – Hospital 06 – Telecom 07 – Insurance 08 – Education 09 – Gifting 11 – International 12 – Metro ATM NAMQR 13 – Non-metro ATM NAMQR 14 – SI

												15 – Corporate disbursement 18 – Government voucher 19 – Private Corporate voucher Mandatory in string only w.r.t. above mentioned use cases, else optional If present, payer PSP to pass as it is, else payer PSP to populate 00 - Default
						Merchant type	03	A	5	C	M	Values that can be populated: • LARGE • SMALL Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise If “Point of initiation method = 13 or 14”, this parameter is not required.
						Merchant genre	04	A	Var. up to 7	C	M	Values that can be populated: • ONLINE • OFFLINE Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise If “Point of initiation method = 13 or 14”, this parameter is not required.

						Merchant on-boarding type	05	A	Var. up to 10	C	M	Merchant on-boarding type denotes entity on-boarding the merchant and can be either of the following- • BANK • AGGREGATOR • NETWORK • TPAP Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise If “Point of initiation method = 13 or 14”, this parameter is not required.
						Merchant brand	06	AN	Var. up to 25	C	M	Brand name Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise If “Point of initiation method = 13 or 14”, this parameter is not required.
						Base amount	07	N	Var. up to 13	O	M	It will contain the purchase amount populated by merchant. Only mandatory, if purpose=”11”
						Base currency	08	A	3	C	C	Indicates the currency code of the transaction. A 3-digit alpha code value, as defined by [ISO 4217]. This value will be used by the mobile application to display a recognizable

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>currency to the customer whenever an amount is being displayed or whenever the customer is prompted to enter amount.
Only mandatory, If purpose=”11”</td></tr>
<tr><td>Unreserved template</td><td>81</td><td>ANS</td><td>Var. up to 99</td><td>C</td><td>C</td><td colspan="7">To add fields that are present in IPP Deep Linking Specifications but not present in EMVCo specifications
If “Point of initiation method = 13 or 14”, this template is not required.
<table>
<tr><th>Name</th><th>Tag</th><th>Format</th><th>Length</th><th colspan="2">Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
<tr><td>Globally Unique Identifier</td><td>00</td><td>ANS</td><td>Var. up to 32</td><td>M</td><td>M</td><td>A reverse domain name, as defined by NAMQR operator (e.g., na.com.operator.namqr).</td></tr>
<tr><td>Invoice date</td><td>01</td><td>ISO Date Time</td><td>Var. up to 27</td><td>C</td><td>C</td><td>This field is used to capture the bill invoice date.
Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise.</td></tr>
<tr><td>Invoice name</td><td>02</td><td>AN</td><td>Var. up to 25</td><td>C</td><td>C</td><td>This field is used to track the unique customer name present in the bill.
If this tag is present, app should display the value to the customer.
Parameter mandatory for international NAMQR (i.e., Purpose = 11) and optional otherwise.</td></tr>
</table></td></tr>
<tr><td>Unreserved template</td><td>82</td><td>ANS</td><td>Var. up to 99</td><td>C</td><td>C</td><td colspan="7">To add fields that are present in IPP Deep Linking Specifications but not present in EMVCo specifications
<table>
<tr><th>Name</th><th>Tag</th><th>Format</th><th>Length</th><th colspan="2">Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
</table></td></tr>
</table>

						Globally Unique Identifier	00	ANS	Var. up to 32	M	M	A reverse domain name, as defined by NAMQR operator (e.g., na.com.operator.namqr).
						Transaction Id	01	AN	35	O	O	This must be Payee PSP generated id when present. In case of Merchant payments, merchant may acquire the transaction id from payee PSP. If present, Payer PSP has to pass this parameter as transaction Id, however if the Payee PSP doesn't populate, the Payer PSP to populate the same. If "Point of initiation method = 13 or 14", this parameter is not required.
						NAMQR expiry date & time	02	ISO Date Time	27	O	O	NAMQR expiry date & time.
						NAMQR creation time stamp	03	ISO Date Time	27	O	O	This is the time stamp when the NAMQR was created. In case it is present, app should state that the NAMQR was created on this time stamp.
						Tier	04	AN	5	O	O	Denotes the tier of the city on basis of population: TIER1 | TIER2 | TIER3 | TIER4 | TIER5 | TIER6
						Transaction Type	05	A	Var. up to 7	O	O	This is transaction type which denote type of transaction: PAY / COLLECT / CREATE /

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>UPDATE / REVOKE / PAUSE / UNPAUSE
If “Point of initiation method = 13 or 14”, this parameter is not required.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Consent</td><td>06</td><td>A</td><td>Var. up to 25</td><td>O</td><td>O</td><td>The consent type denotes the purpose for which the payer’s consent is being taken.
This is for specific use cases as may be defined in future.
If “Point of initiation method = 13 or 14”, this parameter is not required.</td></tr>
<tr><td>Unreserved template</td><td>83</td><td>ANS</td><td>Var. up to 99</td><td>C</td><td>C</td><td colspan="7">To add fields that are present in IPP Deep Linking Specifications but not present in EMVCo specifications
If “Point of initiation method = 13 or 14”, this template is not required.
<table>
<tr><th>Name</th><th>Tag</th><th>Format</th><th>Length</th><th colspan="2">Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td></td><td>S</td><td>D</td><td></td></tr>
<tr><td>Globally Unique Identifier</td><td>00</td><td>ANS</td><td>Var. up to 32</td><td>M</td><td>M</td><td>A reverse domain name, as defined by NAMQR operator (e.g., na.com.operator.namqr).</td></tr>
<tr><td>Mandate name</td><td>01</td><td>AN</td><td>Var. up to 25</td><td>O</td><td>C</td><td>Mandate name, specifies the purpose of mandate
Applicable only for mandate NAMQR</td></tr>
<tr><td>Mandate type</td><td>02</td><td>ANS</td><td>Var. up to 25</td><td>O</td><td>O</td><td>Future use
Applicable only for mandate NAMQR</td></tr>
<tr><td>Validity start</td><td>03</td><td>N</td><td>8</td><td>C</td><td>C</td><td>Defines start time of mandate validity (Format ddmmyyyy)
Applicable only for mandate NAMQR</td></tr>
</table></td></tr>
</table>

						Validity end	04	N	8	C	C	Defines end time of mandate validity (Format ddmmyyyy) Applicable only for mandate NAMQR
						Amount rule	05	A	Var. up to 5	O	C	'MAX' or 'EXACT' rule applied to mandate (Optional, default value to be passed in online message in case amount rule is not passed in NAMQR is 'MAX') Applicable only for mandate NAMQR
						Recurrence	06	A	Var. up to 11	C	C	Specifies the frequency of mandate debit (ONETIME | DAILY | WEEKLY | FORTNIGHTLY | MONTHLY | BIMONTHLY | QUARTERLY | HALFYEARLY | YEARLY | ASPRESENTED) Applicable only for mandate NAMQR
						Recurrence rule value	07	ANS	Var. up to 25	O	C	Specifies date along with recurrence rule type for debit (FOR FUTURE USE) Applicable only for mandate NAMQR
						Recurrence rule type	08	A	Var. up to 6	O	C	Can have values: (BEFORE | ON | AFTER) Specifies date along with recurrence rule value for debit

												Applicable only for mandate NAMQR
						Revocable	09	A	1	O	C	Revocable tag can be passed as Y/N. In case this tag is not present in the NAMQR, app should by default pass the value as 'Y' Applicable only for mandate NAMQR
						Share to payee	10	A	1	O	C	Share to Payee option can be given as Y/N. In case the tag is not present in the QR, payer will have the option to opt for the same in the app. Applicable only for mandate NAMQR
						Block	11	A	1	O	C	Block – Y/N. This field is used for intimating remitter bank to block the necessary fund against payer account. Applicable only for mandate NAMQR
						UMN	12	ANS	Var. up to 25	O	C	Unique mandate number shared by payer for the payee to initiate the debit. (For Future Use when other type will be included) Applicable only for mandate NAMQR
						Skip	13	ANS	2	O	O	(Future use) Mandate can be executed for a non – registered mandate i.e., mandate is

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>not present with Payee PSP.
Applicable only for mandate NAMQR</td></tr>
<tr><td>Unreserved template</td><td>84</td><td>ANS</td><td>Var. up to 99</td><td>C</td><td>C</td><td colspan="8">To add fields that are present in IPP Deep Linking Specifications but not present in EMVCo specifications
If “Point of initiation method = 13 or 14”, this template is not required.
Name | Tag | Format | Length | Presence S | Presence D | Description
Globally Unique Identifier | 00 | ANS | Var. up to 32 | M | M | A reverse domain name, as defined by NAMQR operator (e.g., na.com.operator.namqr).
Split | 01 | ANS | Var. up to 67 | O | O | It will contain the split details of amount.
The PSP must compute the Amount value & Discount amount to show the final amount to customer for PIN authorization
(one or more split value will come)

DISCNT: 10|
DISPCT:10%|
CSHBCK: 10|
CSHPCT:10%|
FX:30|
MKUP: 5%

DISCNT indicates fixed discount
DISPCT indicates discount in percentage
CSHBCK indicates fixed cashback</td></tr>
</table>

												CSHPCT indicates cashback in percentage If present, the cashback may be displayed to the customer on the mobile application FX indicates the Foreign Exchange Rate MKUP gives the Mark Up rate in percentage The Value in these parameters shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the parameter includes decimals, the "." character shall be used to separate the decimals from the integer value and the "." character may be present even if there are no decimals. The parameters are defined only up-to 2 decimal numbers i.e., “99.12’’ (as aligned with currency exponent associated with Namibia currency code defined in ISO 4217). The percentage parameters shall only contain values between “00.01” and “99.99”.

												The above describes the only acceptable format. It cannot contain any other characters
CRC	63	ANS	04	M	M	Checksum calculated over all the data objects included in the NAMQR code. The CRC (tag 63) is the last data object in the NAMQR code and allows the mobile application to check the integrity of the data scanned without having to parse all of the data objects. The checksum shall be calculated according to [ISO / IEC 13239] using the polynomial '1021' (hex) and initial value 'FFFF' (hex). The data over which the checksum is calculated shall cover all data objects, including their Tag, Length and Value, to be included in the NAMQR Code, in their respective order, as well as the Tag and Length of the CRC itself (but excluding its Value). Following the calculation of the checksum, the resulting 2-byte hexadecimal value shall be encoded as a 4-character Alphanumeric Special value by converting each nibble to the corresponding Alphanumeric Special character. A nibble with hex value '0' is converted to "0" (= hex value '30'), a nibble with hex value '1' is converted to "1" (= hex value '31') and so on. Hex values 'A' to 'F' must be converted to uppercase characters "A" to "F" (= hex values '41' to '46'). Example: a CRC with a two-byte hexadecimal value of '007B' is converted to "007B" and included in the QR Code as "6304007B".								

4.11 EMVCo standards for customer presented card chip data [13]

EMVCo Standard - Customer Presented (NAMQR has proposed to follow the same standard for value 99 in tag 00)					
Name	**Tag**	**Format**	**Length**	**Presence**	**Comment**
Payload Format Indicator	85	AN	5	M	Defines the version of the QR Code. The first 3 characters are always "CPV" (Consumer Presented Version) and the last two characters must be decimal digits indicating the version of the payload format. Defines the QR Code format version and is the first data object of the payload. In this version of the

[13] Refer document 'EMVCo-Consumer-Presented-QR-Specification-v1.1' for detailed specifications

					specification, the Payload Format Indicator has the value "CPV01".
Application Template	61	B	var.	M	Contains the application specific data where the application is identified by the ADF name.
Common Data Template	62	B	var.		Contains the common data that is applicable to the POI App, for the application(s) in Application Template(s).
Application Specific Transparent Template	63	B	var.		Contains the application specific data that is transparent to the POI App, where the application is identified by the ADF name.
Common Data Transparent Template	64	B	var.		Contains the common data that is transparent to the POI App, for the application(s) in Application Template(s).
Application Definition File (ADF) Name	4F	B	5 to 16	M	Identifies the application as described in [ISO 7816-5]. The ADF Name may also be referred to as the Application Identifier (AID). The POS system shall maintain a list of applications supported by the POS system identified by their AIDs. Based on the Application Definition File (ADF) Name (tag '4F'); the POI matches the ADF against the list of supported AIDs
Application Label	50	ANS	1 to 16	O	Mnemonic associated with AID according to [ISO 7816-5]. Special characters limited to space. If the POI supports receipt printing, the following data objects may be printed on the receipt: • Application Label (tag '50')
Track 2 Equivalent Data	57	B	var. up to 19	C	Contains the data objects of the Track 2 according to [ISO 7813], excluding start sentinel, end sentinel, and LRC, as follows: • Primary Account Number: numeric, var. up to 19 digits • Field Separator ('D'): binary • Expiration Date (YYMM): numeric, 4 digits
Primary Account Number		N	var. up to 19 nibbles		
Field Separator of 'D'		B	1 nibble		
Expiration Date (YYMM)		N	4 nibbles		
Service Code		N	3 nibbles		

Discretionary Data		N	var.		• Service Code: numeric, 3 digits • Discretionary Data: numeric, var. • Pad with 'F' if needed to ensure whole bytes: binary Either Track 2 Equivalent Data must be present or Application PAN must be present. At least one of the two data objects must be present in the POI Data. Although it is not precluded that both data objects are present, considerations should be given, for example, relating to the overall size of data in the QR Code, when determining whether to include both data objects in the POI Data. Please check with the respective payment systems for specific implementation requirements. If the PAN (tag '5A') is absent, then the POI must extract the PAN from Track 2 Equivalent Data. Track 2 Equivalent Data (tag '57') contains the data objects of the track 2, in accordance with [ISO 7813], excluding start sentinel, end sentinel, and LRC. The Track 2 Equivalent Data has a maximum length of 19 bytes (38 nibbles)
Padded with 'F' if needed to ensure whole bytes		B	1 nibble		
Application PAN (Valid cardholder account number)	5A	CN	var. up to 10	C	
Cardholder Name	5F20	ANS	2 to 26	O	Indicates cardholder name according to [ISO 7813]. If the POI supports receipt printing, the following data objects may be printed on the receipt: • Cardholder Name (tag '5F20')
Language Preference	5F2D	AN	2 to 8	O	1 - 4 languages stored in order of preference, each represented by 2 alphabetical characters according to [ISO 639-1] If the Language Preference (tag '5F2D') is present in the QR Code Data, and if one of the listed languages is supported by the POI, then the supported language with the highest preference shall be used when displaying messages to the cardholder.
Issuer URL	5F50	ANS	var.	O	Contains customer information for electronic receipt delivery with the syntax defined by a standard URI scheme The value of the Issuer URL contains customer

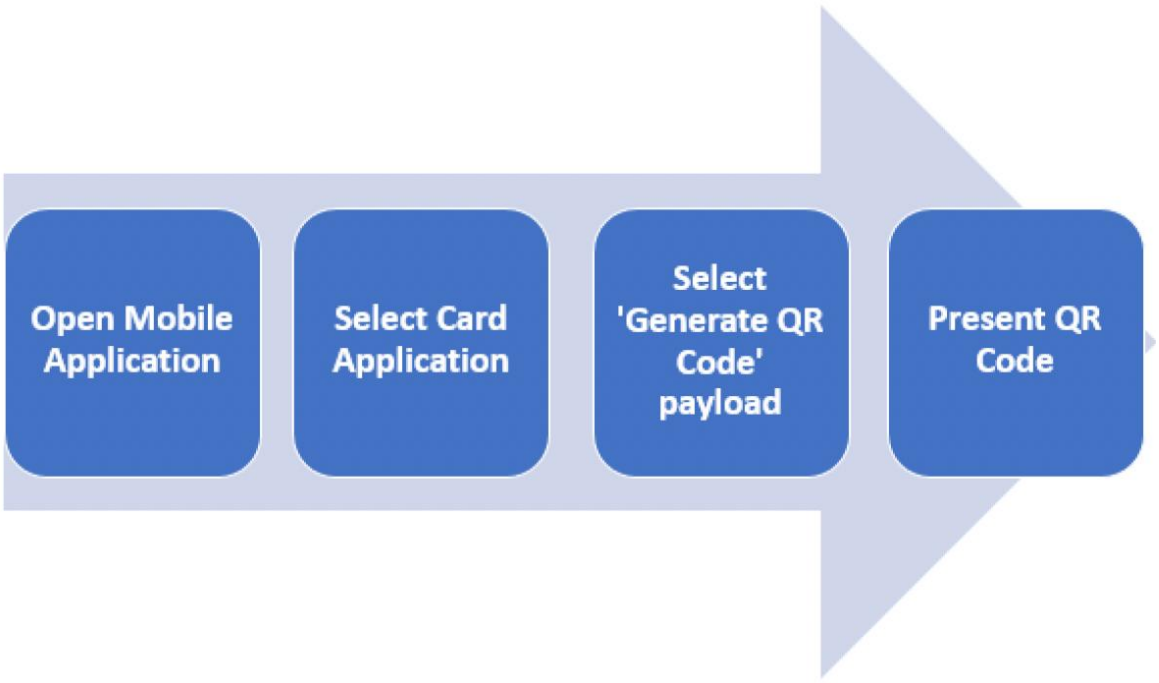
					information for electronic receipt delivery with the syntax defined by a standard URI scheme. Supported URI schemes are: • Phone number, defined in [RFC 3966] • Email address, defined in [RFC 6068] The following are examples of the Issuer URL: • If the value is a phone number: tel:+1-234-567-8910 • If the value is an email address: mailto:example@emvco.com If the POI supports electronic means for providing receipts, such as email or SMS, then the POI may analyse the Issuer URL (tag '5F50') for supporting data.
Application Version Number	9F08	B	2	O	Version number assigned by the payment system for the application. If this data is absent, the POI uses '00 10' (version 1.0) as the default value Based on the combination of the AID matching the ADF Name (tag '4F') and the Application Version Number (tag '9F08'), the POI determines the convention for mapping data listed in the Transparent Data to an online authorisation message. If the Application Version Number (tag '9F08') is absent, the POI shall use '00 10' (version 1.0) as the default value for the Application Version Number.
Token Requestor ID	9F19	N	6	O	Uniquely identifies the pairing of Token Requestor with the Token Domain. Processing of the Token Requestor ID (TRID, tag '9F19') is out of scope of this specification, however the POI shall be able to recognise the data object.
Payment Account Reference (PAR)	9F24	AN	29	O	Uniquely identifies the PAN to which a payment token is associated, as defined in [EMV Bulletin No. 167]. Permitted characters are alphabetic upper case and numeric. The PAR (tag '9F24') allows acquirers and

					merchants to link transactions, whether tokenised or not, that are associated to the same underlying account. The POI shall be able to recognise the PAR, but use of the PAR is out of scope of this specification.
Last 4 digits of PAN	9F25	N	2	O	Represents the last four digits of the underlying PAN affiliated with the Payment Token. If the POI prints the last four digits of the PAN on the receipt and the Last 4 Digits of PAN (tag '9F25') is present in the QR Code Data, then the POI shall use the value of the Last 4 Digits of PAN (tag '9F25') when printing the last four digits of the PAN on the receipt.

The following describes the high-level functionality of various components of the QR code processing architecture on the consumer device:

1. Mobile application / wallet – A consumer-facing user interface (UI) application provided by the issuer and provisioned to the customer's mobile device. It includes the functionality to encode the payment credentials based on this specification and then displays the resulting QR code.
2. QR code payload – The payload, consisting of payment token credentials and other data based on this specification, converted to base64 and encoded in a QR code.

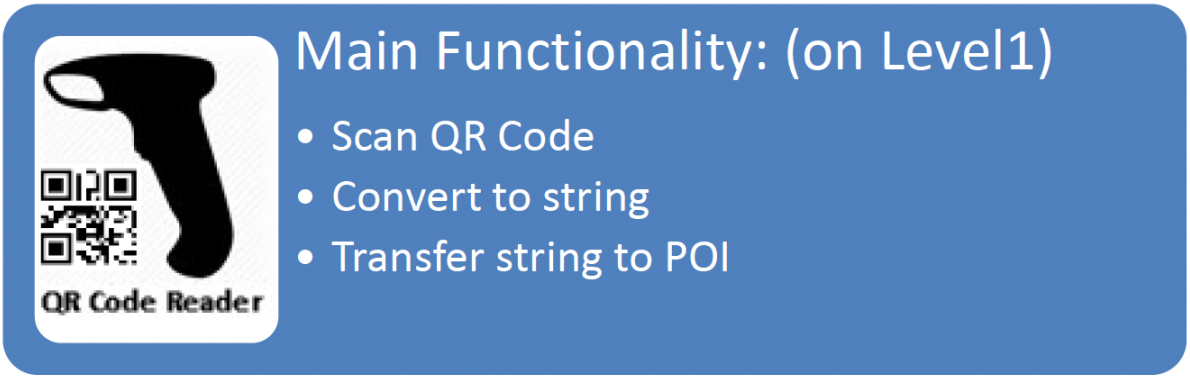
The customer device functional view is as follows:

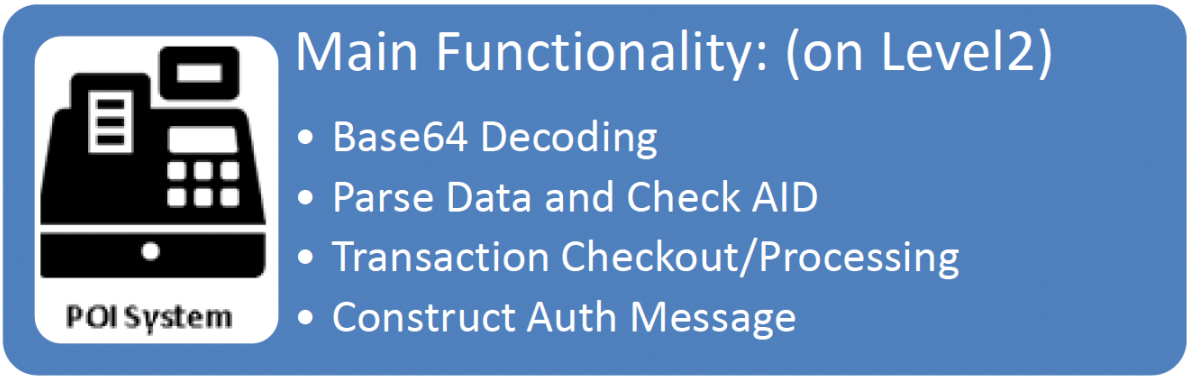


There are 2 logical components on the merchant device: the QR code reader and the POI application.

1. QR code reader: Scans the QR code, decodes the QR code and sends the data recovered to the POI system. This data constitutes the base64 encoded QR code payload.
2. POI application: The application developed by the POI vendor to process the base64 encoded QR code payload defined in this specification. Its functions include base64 decoding, parsing the data, checking content and format and transaction processing.

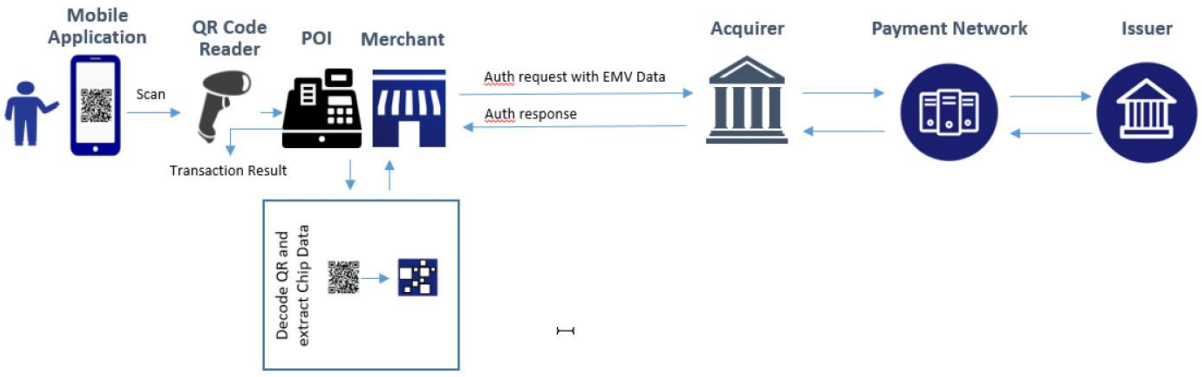
Merchant device functional view is as follows:





On the network the following are the roles as per the existing EMV infrastructure:

1. Acquirer—The acquirer / processor processing the authorization transaction received from the merchant.
2. Payment Network—Responsible for transaction routing to the issuer and any corresponding tokenization services and functions.
3. Issuer—The issuer of the original payment card, that is used in the QR Code transaction.



The examples for converting binary data to and from a QR Code as defined in this specification.

Note: The data object values provided in the examples below are for illustrative purposes only and may not be indicative of typical values for each data object.

Binary Data (shown as hex bytes):

85 05 43 50 56 30 31
61 13
    4F 07 A0 00 00 00 55 55 55
    50 08 50 72 6F 64 75 63 74 31
61 13
    4F 07 A0 00 00 00 66 66 66
    50 08 50 72 6F 64 75 63 74 32
62 49
    5A 08 12 34 56 78 90 12 34 58
    5F 20 0E 43 41 52 44 48 4F 4C 44 45 52 2F 45 4D 56
    5F 2D 08 72 75 65 73 64 65 65 6E
    64 21
        9F 10 07 06 01 0A 03 00 00 00
        9F 26 08 58 4F D3 85 FA 23 4B CC
        9F 36 02 00 01
        9F 37 04 6D 58 EF 13

Base64 Data:

hQVDUFYwMWETTwegAAAAVVVVUAhQcm9kdWN0MWETTwegAAAAZmZmUAhQcm9kdWN0MmJJWggSNFZ4kBI0WF8gDkNBUkRIT0xERVIvRU1WXy0IcnVlc2RlZW5kIZ8QBwYBCgMAAACfJghYT9OF+iNLzJ82AgABnzcEbVjvEw==

4.12 Key points related to NAMQR code specifications

(a) For payee presented NAMQR, MCC contains value ‘0000’. Tag 17 is reserved for payee presented NAMQR for existing Namibia payment system that does not use PAN or IPP full form alias as payee identifier. Tag 26 and 27 are reserved for payee presented NAMQR for IPP payee full form alias reference.

(b) For payer presented NAMQR, point of initiation method contains value ‘13’ or ‘14’ and MCC contains value ‘0000’. Tag 28 is reserved for payer presented NAMQR for existing Namibia payment system that does not use PAN or IPP full form alias as payee identifier. Tag 29 is reserved for payer presented NAMQR for IPP payer full form alias reference.

(c) For merchant presented NAMQR, replace ‘payee’ with ‘merchant’, ‘payer’ with ‘customer’, ‘payee PSP’ with ‘acquirer PSP’, ‘payer PSP’ with ‘issuer PSP’ in the section ‘NAMQR code payload data objects’.

(d) Merchant presented NAMQR must contain non-zero MCC i.e., ‘XXXX’ assigned by the acquirer PSP.

(e) If this Payload Format Indicator (tag 00) has the value "99" (or any such value), then all tags as per existing EMVCo standards for customer presented card chip data to be followed.

(f) It is preferred that the PSP presents the data in sequence, however the counterparty PSP app must be able to read the data elements in any sequence.6

(g) All elements would have a Tag, followed by Length and the Value i.e., TLV format. The length field is 2 numeric from 00 to 99.
(h) For the optimization of bit stream length, it is recommended to encode in Numeric followed by Alphanumeric, using combined mode as recommended in Annex J of ISO / IEC 18004-2006-QR code 2005 barcode symbology specs.
(i) Any data elements and data element values defined as “reserved for future use” are reserved for future definition by this specification. These data elements and data elements values are only to be assigned by NAMQR operator (as identified by the industry). A payer / payee PSP app that encounters data that it recognizes as "reserved for future use" must not act on the data. A payer / payee PSP cannot add proprietary data elements into those tags.
(j) Merchant Id, Store Id, Terminal Id will be used by acquirer merchant for reconciliation / confirmation purposes. This will be echoed in all messages.
(k) Null values: This needs to be handled by PSP as Null value and should not passed into online message directly as a string value “null”
(l) Space shall be handled as follows: while generating / creating / Reading a NAMQR, space (“ ”) should be represented as “%20” and not “%”as to be compliant with existing Internet Standard RFC 3986 section 2.1 Percent-Encoding.
(m) NAMQR has a provision where the merchants can share bills / invoices with the customers before the transaction is authorized. The bills / invoices can either be downloaded as PDF or can be viewed on a browser. This provision requires the PSP applications to display an option called ‘view invoice’. This option will be present for NAMQR initiated pay transactions. When the user scans a QR, then they will get an option on the app to click that URL. This URL will redirect them to the invoice which can be either viewed or downloaded.

4.13 Data coding of NAMQR

1. For NAMQR code, all the data should be encoded using Byte Mode. (Alphanumeric Mode, Numeric mode, Kanji, Structured Append, and FCN1 mode shall not be used).
2. If the NAMQR code includes characters other than Alphanumeric Special, then it shall include an ECI mode indicator and ECI Designator, where the ECI Designator includes the binary representation of an ECI Assignment number equal to 000026, to indicate UTF-8 encoding. (Note that Alphanumeric Special includes Numeric).

4.14 QR Code Encoding

QR codes have different density levels, determined by the version of the QR code, and different error correction modes, which help ensure the code can still be read even if it is partially damaged. Here's a brief overview:

Density (Versions) of QR Codes:

1. Version 1 to Version 40:
   a. QR codes have 40 different versions, each specifying the number of modules (small squares) in the code.

b. Version 1: 21 x 21 modules.
c. Version 40: 177 x 177 modules.
d. As the version number increases, the QR code can store more data, but the size and complexity also increase.

Error Correction Levels:

QR codes have four error correction levels, allowing the code to be read even if part of it is damaged. The level you choose affects the amount of data that can be stored and the size of the code.

1. **Level L (Low):**
   a. Recovers 7% of data.
   b. Most data storage capacity.
2. **Level M (Medium):**
   a. Recovers 15% of data.
   b. A balance between data storage and error correction.
3. **Level Q (Quartile):**
   a. Recovers 25% of data.
   b. More robust error correction, less data storage.
4. **Level H (High):**
   a. Recovers 30% of data.
   b. Highest error correction, least data storage.

General Guidance

Here are some factors to consider when selecting the level:

Environment Where the QR Code Will Be Used:

1. Clean and Controlled Environments (e.g., indoor settings):
   a. Use Level L or M: Since the risk of damage is low, you can prioritize data storage capacity.

2. Harsh or Dirty Environments (e.g., outdoor settings, industrial areas):
   a. Use Level Q or H: These environments pose a higher risk of the QR code being damaged, so stronger error correction is advisable.

Importance of Data Integrity:

1. Critical Data (e.g., financial information, secure access):
   a. Use Level H: If data integrity is crucial and even small errors could lead to significant issues, opt for the highest error correction level.
2. Less Critical Data (e.g., general information, marketing):
   a. Use Level L or M: For non-critical data, you can afford to use a lower level to store more data or keep the QR code size smaller.

QR Code Size Constraints:

1. Limited Space for Displaying QR Code:

a. Use Level L: If you need the QR code to be as small as possible, Level L allows for the maximum amount of data storage with the smallest footprint.
2. Space is Not a Concern:
   a. Use Level M, Q, or H: When space is not an issue, you can choose a higher level of error correction to ensure better reliability.

Amount of Data to Encode:

1. Large Amount of Data:
   a. Use Level L or M: These levels allow more data to be stored within the same QR code version.
2. Small Amount of Data:
   a. Use Level Q or H: If you are encoding a small amount of data, you can afford to use a higher level of error correction without significantly increasing the QR code size.

Expected Wear and Tear:

1. High Risk of Physical Damage:
   a. Use Level H: For codes that are likely to experience wear and tear, such as those on frequently handled products, use the highest level.
2. Low Risk of Physical Damage:
   a. Use Level L or M: For codes that will remain in a controlled environment or will not be exposed to much handling, lower levels of correction are sufficient.

Scanning Conditions:

1. Poor Scanning Conditions (e.g., low lighting, angled surfaces):
   a. Use Level Q or H: Higher error correction helps ensure the code can be read even under less-than-ideal conditions.
2. Good Scanning Conditions:
   a. Use Level L or M: If the QR code will be scanned under optimal conditions, lower levels will suffice.

4.15 NAMQR Encoding Recommendation

A balance between error correction level, data storage capacity, the likelihood of damage, and the importance of data integrity has to be found.

1. Limiting maximum payload to 512 characters as is done by EMVCo would be a good initial choice.
2. Several rendering formats may be allowed to accommodate different use cases.
3. The scanning application must ensure that the scanned payload is a valid NAMQR by validating the CRC, prompting a re-scan if needed.

Error Correction Level:

1. Level M (Medium) or Level Q (Quartile) are most commonly used:

a. Level M (15% error correction): Often chosen because it offers a good balance between data capacity and error correction. This level ensures that the QR code can be reliably scanned even if it's slightly damaged or printed in a lower-quality format, which is common in merchant environments.
b. Level Q (25% error correction): Sometimes chosen for environments where the QR code might be more prone to damage (e.g., outdoor merchants, kiosks). This level offers stronger error correction, which can be critical if the QR code is exposed to more wear and tear.

QR Code Version (Density):

1. Lower to Mid Versions (Version 1 to Version 10):
   a. Version 1 (21 x 21 modules) to Version 10 (57 x 57 modules) are typical, depending on the amount of data being encoded.
   b. Payee presented NAMQR codes would need to store a moderate amount of data, such as merchant account information, transaction amount, currency, and other payment-related information. These versions provide enough space to encode this data while keeping the QR code size manageable and easily scannable.

Key Considerations:

1. Readability: Ensuring that the QR code can be easily scanned by a wide range of consumer devices, including smartphones with varying camera qualities.
2. Data Capacity: Balancing the need to include sufficient transaction details without making the QR code too dense or difficult to scan.
3. Environmental Factors: Considering where the QR code will be displayed (e.g., on a printed receipt, on a POS screen, or as a sticker) and choosing an error correction level that compensates for potential damage or degradation.

Common Practice:

1. Level M with Versions 3 to 5 is a typical configuration, as it provides a good compromise between size, error correction, and data capacity. This setup ensures that the QR code remains small enough for practical use while still being resilient to minor damage or print quality issues.

5. Evidence of versatility and interoperability of the NAMQR specifications

5.1 Potentiality Matrix showcasing the comprehensive capability of NAMQR

The following payment canvas illustrates how the proposed NAMQR standards will avoid fragmentation and provide comprehensive interoperability in Namibia. The tags provided in the Section 4 cater to all of the following scenarios.

Payment type	Payment frequency	Presented by	QR generation	From account	To account
P2P	One-time	Payee	Payee has a default static NAMQR code or Payee enters the	Bank account, card account, e-	Bank account, card account,

			amount and generates a dynamic NAMQR code	money wallet, voucher	e-money wallet, cash
P2P	Recurring	Payee	Payee has a default static NAMQR code or Payee enters the amount, frequency, period etc. and generates a dynamic NAMQR code	Bank account, card account, e-money wallet	Bank account, card account, e-money wallet
P2P	One-time	Payer	Payer has a default static NAMQR code or Payer enters the amount and generates a dynamic NAMQR code	Bank account, card account, e-money wallet, voucher	Bank account, card account, e-money wallet, cash
P2P	Recurring	Payer	Payee enters the amount, frequency, period etc. and generates a NAMQR code	Bank account, card account, e-money wallet	Bank account, card account, e-money wallet
P2M	One-time	Merchant (Static NAMQR)	System generated one time, provided by Payment Processor / Acquirer bank	Bank account, card account, e-money wallet, voucher	Merchant account, e-money wallet
P2M	One-time	Merchant (Dynamic NAMQR)	Merchant enters the invoice no., amount and generates a NAMQR code	Bank account, card account, e-money wallet, voucher	Merchant account
P2M	Recurring	Merchant (Dynamic NAMQR)	Merchants enter the amount, frequency, period etc. and generates a NAMQR code	Bank account, card account, e-money wallet	Merchant account
P2M	One-time	Customer (Static NAMQR)	Payer has a default static NAMQR code	Bank account, card account, e-money wallet, voucher	Merchant account
P2M	Recurring	Customer (Dynamic NAMQR)	Payer enters the amount and generates a NAMQR code	Bank account, card account, e-money wallet	Merchant account, e-money wallet

Note: To and for transactions between voucher and / or cash will not be allowed.

5.2 Retail payments supported by NAMQR across the SOVs riding on the existing and proposed payment streams[14]

Provided below is the matrix showing how the existing payment systems as well as the new payment systems such as IPP can facilitate to and from payments across SOVs such as bank accounts, Emoney accounts, Card accounts and cash.

Destination Account	**Bank Account**		**E-Money Account** [15]		**Card Account**		**Cash**		**International**[16]	
Originating Account	**Use Case**	**Payment Stream**	**Use Case**	**Payment Stream**	**Use Case**	**Payment Stream**	**Use Case**	**Payment Stream**	**Use Case**	**Payment Stream**
Bank Account	NAMQR (i): P2P	NRTC, EnDO, EnCR, IPP	NAMQR (ix): P2P	NRTC, EnDO, EnCR, IPP	NAMQR (xiii): P2M (credit card bill payment)	NRTC, EnDO, EnCR, IPP	NAMQR (xv): Self-account cash withdrawal at ATM	IPP, ATM	NAMQR (xx): P2M	IPP
	NAMQR (ii): P2M / P2G	NRTC, EnDO, EnCR, IPP, POSD, POSC					NAMQR (xvi): Self-account cash withdrawal – Merchant / Agent	IPP, POSD, POSC		
E-Money Account[17]	NAMQR (iii): P2P	NRTC, EnDO, EnCR, IPP	NAMQR (x): P2P	NRTC, EnDO, EnCR, IPP	NAMQR (xiv): P2M (credit	NRTC, EnDO, EnCR, IPP	NAMQR (xvii): Self E-Money account	IPP, ATM	NAMQR (xxi): P2M	IPP

[14] Proposed NAMQR specifications are sufficient to carry the payload across any of these 2 different payment streams (ex., NRTC to IPP or vice versa). Achieving such interoperability, showcasing flows for NAMQR across such disparate payment streams is out of the scope of the current engagement of Digital Dimensions with BON /PAN.

[15] P2M transactions to E-Money account will be possible only if merchants can have E-Money accounts as per the extant BoN regulations.

[16] NAMQR can support this type of payment based on scope of IPP. BoN/ PAN to clarify if any of the existing payment streams support international transactions.

[17] NAMQR will support Transactions originating from or ending at E Money accounts only if such transactions are permissible under the extant BoN regulations. If yes, NAMQR can provide necessary tags and parameters during operationalization phase.

					card bill payment)		cash withdrawal at ATM			
	NAMQR (iv): P2M / P2G	NRTC, EnDO, EnCR, IPP, POSD, POSC					NAMQR (xviii): Self E-Money account cash withdrawal at Merchant / Agent	IPP, POSD, POSC		
Card Account	NAMQR (v): P2M / P2G	POSD, POSC, NRTC, EnCR, IPP	NAMQR (xi): P2P	POSD, POSC, NRTC, EnCR, IPP			NAMQR (xix): Self card account cash withdrawal at Merchant[18]	POSD, POSC, IPP		
	NAMQR (vi): Pay by link	On line payment gateway[19]								
Cash[20]										
Voucher	NAMQR (vii): P2P	IPP	NAMQR (xii): P2P	IPP						
	NAMQR (viii): P2M / P2G	IPP								

[18] NAMQR will support cash withdrawal at Merchant only if such transactions are permissible under the extant BoN regulations.

[19] We recommend to provide for such payment links subject to users being allowed to make payments using other SOVs such as bank accounts, EMoney accounts etc. besides Visa and Mastercard.

[20] We have not considered to include cash payments to any other SOVs (such as Self-account cash deposit – Branch / Agent or cash payments to merchants etc.) while developing these NAMQR standards.

A glance at the above table will make it apparent that the proposed NAMQR standards can be easily configured to facilitate a particular use case riding on any of the existing payment streams so long as such a use case is supported by that payment stream. The above table is to illustrate potential of NAMQR and by no means an exhaustive list of use cases. NAMQR will support new use cases as clarified above.

5.3 NAMQR tags and corresponding parameters for the use cases mentioned in the above sections 5.1 and 5.2

Showcased below are the tags and their corresponding parameters of NAMQR to further provide evidence of how the proposed standards can indeed support various use cases listed in this document. We have also identified which of the existing payment streams can use which tags to accomplish the intended use case.[21]

Sr. No.	Use case	Payment stream	Frequency	Mandatory NAMQR tags and corresponding parameters for static QR [22]	Additional tags and corresponding parameters for dynamic QR
1	NAMQR (i) – Payee presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
2		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 1 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule	No additional tags besides the tags in Sr. No. 1

[21] This table has been derived by using the NAMQR specifications formulated in the Section 4 to substantiate versatility and interoperability of NAMQR to facilitate payments across various SOVs riding on the rails of the existing payment streams.

[22] This table is for illustration purpose only. For optional tags and other details, refer section 'NAMQR code payload data objects'.

				type, Revocable, Share to payee, Block	
3		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
4		IPP	Recurring	Additional tags besides the tags in Sr. No. 3 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 3
5	NAMQR (i) – Payer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
6		EnDO	Recurring	No additional tags besides the tags in Sr. No. 5	No additional tags besides the tags in Sr. No. 5

7		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
8		IPP	Recurring	No additional tags besides the tags in Sr. no. 7	No additional tags besides the tags in Sr. No. 7
9	NAMQR (ii) – Merchant presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
10		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 9 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 9
11		IPP	One-time	(00) – Payload format indicator	(27) – Transaction Reference (53) –

				(01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
12		IPP	Recurring	Additional tags besides the tags in Sr. No. 11 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 11
13		POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) – CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
14		POSD, POSC	Recurring	Additional tags besides the tags in Sr. No. 13 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule	No additional tags besides the tags in Sr. No. 13

				type, Revocable, Share to payee, Block	
15	NAMQR (ii) – Customer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
16		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
17	NAMQR (iii) – Payee presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time

				(65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	
18		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 17 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 17
19		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
20		IPP	Recurring	Additional tags besides the tags in Sr. No. 19 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 19
21	NAMQR (iii) – Payer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias)	(53) – Transaction currency (54) – Transaction amount (62) – Reference label

				(52) – Merchant category code (with value ‘0000’) (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(62) – Short description of the transaction (82) - NAMQR expiry date & time
22		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value ‘0000’) (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
23	NAMQR (iv) – Merchant presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
24		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 23 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule,	No additional tags besides the tags in Sr. No. 23

				Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	
25		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
26		IPP	Recurring	Additional tags besides the tags in Sr. No. 25 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 25
27		POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time

28		POSD, POSC	Recurring	Additional tags besides the tags in Sr. No. 27 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 27
29	NAMQR (iv) – Customer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
30		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
31	NAMQR (v) – Merchant presented QR	POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data	(53) – Transaction currency (54) – Transaction amount (62) – Reference label

				as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
32		POSD, POSC	Recurring	Additional tags besides the tags in Sr. No. 31 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 31
33		NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
34		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 33 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 33

35		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
36		IPP	Recurring	Additional tags besides the tags in Sr. No. 35 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 35
37	NAMQR (v) – Customer presented QR	POSD, POSC	One-time	If tag 00 (Payload format indicator) has value “99” (or any such value), all tags as per existing EMVCo standards for customer presented card chip data to be followed (refer section ‘EMVCo standards for customer presented card chip data’), as below: (85) – Payload format indicator (61) – Application template (62) – Common data template (63) – Application specific transparent template (64) – Common data transparent template (4F) – Application definition file (ADF) name (50) – Application label (57) – Track 2 Equivalent Data	

				(5A) – Application PAN (Valid cardholder account number) (5F20) - Cardholder Name (5F2D) - Language Preference (5F50) - Issuer URL (9F08) - Application Version Number (9F19) - Token Requestor ID (9F24) - Payment Account Reference (PAR) (9F25) - Last 4 digits of PAN	
38	NAMQR (vi) – Merchant presented QR	Pay by link	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (62) – Payment link (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
39	NAMQR (vii) – Payer presented QR (request to pay)	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value ‘0000’) (53) – Transaction currency (54) – Transaction amount (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier	

				(80) – Globally Unique Identifier, Initiation Mode, Purpose (82) - NAMQR expiry date & time, NAMQR creation time stamp (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block, UMN (Unique Mandate Number) (63) - CRC	
40	NAMQR (viii) – Customer presented QR (request to pay)	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (53) – Transaction currency (54) – Transaction amount (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode, Purpose (82) - NAMQR expiry date & time, NAMQR creation time stamp (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block, UMN (Unique Mandate Number) (63) - CRC	
41	NAMQR (ix) – Payee	NRTC, EnCR	One-time	(00) – Payload format indicator	(53) – Transaction currency

	presented QR			(01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
42		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 41 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 41
43		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
44		IPP	Recurring	Additional tags besides the tags in Sr. No. 43 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule	No additional tags besides the tags in Sr. No. 43

				type, Revocable, Share to payee, Block	
45	NAMQR (ix) – Payer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
46		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
47	NAMQR (x) – Payee presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time

				(65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	
48		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 47 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 47
49		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
50		IPP	Recurring	Additional tags besides the tags in Sr. No. 49 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 49
51	NAMQR (x) – Payer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias)	(53) – Transaction currency (54) – Transaction amount (62) – Reference label

				(52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(62) – Short description of the transaction (82) - NAMQR expiry date & time
52		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
53	NAMQR (xi) – Payee presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
54		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 53 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule,	No additional tags besides the tags in Sr. No. 53

				Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	
55		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
56		IPP	Recurring	Additional tags besides the tags in Sr. No. 55 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 55
57	NAMQR (xi) – Payer presented QR (request to pay)	POSD, POSC	One-time	If tag 00 (Payload format indicator) has value "99" (or any such value), all tags as per existing EMVCo standards for customer presented card chip data to be followed (refer section 'EMVCo standards for customer presented card chip data'), as below: (85) – Payload format indicator (61) – Application template (62) – Common data template (63) – Application specific transparent template (64) – Common data transparent template	(53) – Transaction currency (54) – Transaction amount

				(4F) – Application definition file (ADF) name (50) – Application label (57) – Track 2 Equivalent Data (5A) – Application PAN (Valid cardholder account number) (5F20) - Cardholder Name (5F2D) - Language Preference (5F50) - Issuer URL (9F08) - Application Version Number (9F19) - Token Requestor ID (9F24) - Payment Account Reference (PAR) (9F25) - Last 4 digits of PAN	
58	NAMQR (xii) – Payer presented QR (request to pay)	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (53) – Transaction currency (54) – Transaction amount (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode, Purpose (82) - NAMQR expiry date & time, NAMQR creation time stamp (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block, UMN (Unique Mandate Number)	

				(63) - CRC	
59	NAMQR (xiii) – Merchant presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
60		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 59 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 59
61		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
62		IPP	Recurring	Additional tags besides the tags in Sr. No. 61 (83) - Globally Unique Identifier, Mandate name,	No additional tags besides the tags in Sr. No. 61

				Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	
63	NAMQR (xiii) – Customer presented QR (request to pay)	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method (28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
64		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
65	NAMQR (xiv) – Merchant presented QR	NRTC, EnCR	One-time	(00) – Payload format indicator (01) – Point of initiation method (17) - Globally Unique Identifier, Payee PSP Id, Payee Identifier (e.g., Mobile Number as alias) (52) – Merchant category code	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction

				(58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
66		NRTC, EnCR	Recurring	Additional tags besides the tags in Sr. No. 65 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 65
67		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
68		IPP	Recurring	Additional tags besides the tags in Sr. No. 67 (83) - Globally Unique Identifier, Mandate name, Mandate type, Validity start, Validity end, Amount rule, Recurrence, Recurrence rule value, Recurrence rule type, Revocable, Share to payee, Block	No additional tags besides the tags in Sr. No. 67
69	NAMQR (xiv) – Customer presented	EnDO	One-time	(00) – Payload format indicator (01) – Point of initiation method	(53) – Transaction currency (54) – Transaction amount

	QR (request to pay)			(28) - Globally Unique Identifier, Payer PSP Id, Payer Identifier (e.g., Mobile Number as alias) (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
70		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
71	NAMQR (xv) – ATM presented QR	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
72	NAMQR (xvi) –	IPP	One-time	(00) – Payload format indicator	(27) – Transaction Reference (53) –

	Merchant / Agent presented QR			(01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
73		POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
74	NAMQR (xvi) – Customer presented QR (request to pay)	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value ‘0000’) (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time

75	NAMQR (xvii) – ATM presented QR	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (82) - NAMQR expiry date & time
76	NAMQR (xviii) – Merchant / Agent presented QR	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
77		POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time

				(63) - CRC	
78	NAMQR (xviii) – Customer presented QR (request to pay)	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (29) - Globally Unique Identifier, Payer IPP full form alias (52) – Merchant category code (with value '0000') (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (82) - NAMQR expiry date & time
79	NAMQR (xix) – Merchant presented QR	POSD, POSC	One-time	(00) – Payload format indicator (01) – Point of initiation method (02 - 16) – Tag to be followed by length and data as defined by card payment networks (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode (63) - CRC	(53) – Transaction currency (54) – Transaction amount (62) – Reference label (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
80		IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier	(27) – Transaction Reference (53) – Transaction currency (54) – Transaction amount (62) – Short description of the transaction (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time

				(80) – Globally Unique Identifier, Initiation Mode (63) - CRC	
81	NAMQR (xix) – Customer presented QR	POSD, POSC	One-time	If tag 00 (Payload format indicator) has value “99” (or any such value), all tags as per existing EMVCo standards for customer presented card chip data to be followed (refer section ‘EMVCo standards for customer presented card chip data’), as below: (85) – Payload format indicator (61) – Application template (62) – Common data template (63) – Application specific transparent template (64) – Common data transparent template (4F) – Application definition file (ADF) name (50) – Application label (57) – Track 2 Equivalent Data (5A) – Application PAN (Valid cardholder account number) (5F20) - Cardholder Name (5F2D) - Language Preference (5F50) - Issuer URL (9F08) - Application Version Number (9F19) - Token Requestor ID (9F24) - Payment Account Reference (PAR) (9F25) - Last 4 digits of PAN	
82	NAMQR (xx) – Merchant presented QR international payment	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias, Org Id, Merchant Id	(27) – Transaction Reference (62) – Bill number, Store label, Terminal label (62) – Short description of the transaction

				(52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode, Purpose (63) - CRC	(80) – Merchant type, Merchant genre, Merchant on-boarding type, Merchant brand, base amount, base currency (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time
83	NAMQR (xxi) – Merchant presented QR international payment	IPP	One-time	(00) – Payload format indicator (01) – Point of initiation method (26) - Globally Unique Identifier, Payee IPP full form alias, Org Id, Merchant Id (52) – Merchant category code (58) – Country code (59) – Payee name (60) – Payee city (65) – Token Vault Unique Identifier (80) – Globally Unique Identifier, Initiation Mode, Purpose (63) - CRC	(27) – Transaction Reference (62) – Bill number, Store label, Terminal label (62) – Short description of the transaction (80) – Merchant type, Merchant genre, Merchant on-boarding type, Merchant brand, base amount, base currency (81) – Globally unique identifier, invoice date, invoice name (82) - NAMQR expiry date & time

6. NAMQR Security Risks and Mitigation Measures

The following security threats must be addressed for NAMQR:

6.1 Tampering and Spoofing

Tampering and spoofing of QR codes involve attackers replacing or altering legitimate QR codes with their malicious versions. This can happen in both physical and digital environments:

1. Physical Tampering: Attackers can place stickers or posters with fraudulent QR codes over legitimate ones in public places like restaurants, retail stores, or advertisements. Users scanning these codes can be redirected to malicious websites or payment portals, leading to unauthorized transactions or data theft (European Payments Council) (Better Regulation).

2. Digital Spoofing: Online, attackers can embed malicious QR codes in emails, social media posts, or websites. These codes may appear to lead to legitimate sites or services but instead direct users to phishing sites or download malware onto their devices (Better Regulation).

6.2 Data Theft

Data theft via QR codes occurs when sensitive information embedded in QR codes is intercepted or accessed by unauthorized parties. This can happen in several ways:

1. Unencrypted Data: If QR codes contain unencrypted payment information, personal details, or authentication credentials, they can be easily intercepted and read by malicious actors. This information can then be used for fraudulent activities (European Payments Council) (Better Regulation).
2. Insecure Transmission: When users scan QR codes, the data transmitted over insecure networks can be intercepted. Attackers can capture this data during transmission, leading to potential data breaches (Better Regulation).
3. Embedded Malware: QR codes can be used to distribute malware that, once installed on a user's device, can steal sensitive information. This malware can track keystrokes, capture screenshots, or access stored data on the device (European Payments Council).

6.3 Insecure QR Code Generation

Insecure generation of QR codes refers to the creation of QR codes without proper security measures, making them vulnerable to manipulation and fraud:

1. Poor Security Practices: If QR codes are generated using tools or platforms that do not implement secure coding practices, they can be easily altered or replicated by attackers. Secure generation involves using cryptographic techniques to ensure the integrity and authenticity of the QR codes (European Payments Council).
2. Lack of Verification: Without proper verification mechanisms, users have no way to confirm the authenticity of the QR codes they are scanning. Secure QR code systems should include features that allow users to verify that the code is legitimate before proceeding with transactions (Better Regulation).

6.4 NAMQR Security Risks Mitigations

6.4.1 Threat of Data Confidentiality

NAMQR data is considered non confidential because it does not directly reveal sensitive information like bank account details. Instead NAMQR proposes to use an alias (or any surrogate value such as mobile number or any such other unique number mapped to an SOV assigned by PSPs to their respective account holders to protect privacy of the payers and the payees).

Refer sections 'Payee presented NAMQR code payment (using smart phone mobile banking application', 'Payee presented NAMQR code payment (using USSD channel)' and 'Payer presented NAMQR code payment – (Request to Pay)' for illustration of transaction flow using Payee / Payer Identifier.

6.4.2 Threat of Data Integrity

The threat of compromise of data integrity can be mitigated by the use of CRC and Token Vault.

Refer tag '63' in section 'NAMQR code payload data objects' for details of CRC.

For the below mentioned scenarios, mitigation measure recommended for NAMQR may be a Certified Token Vault[23]:

1. Domestic NAMQR for transactions using existing Namibian payment systems
2. Domestic NAMQR for interoperable transactions between existing Namibian payment systems and proposed IPP.
3. Domestic NAMQR for app based and USSD based transactions (using existing Namibian payment systems and proposed IPP).
4. International NAMQR (i.e., Purpose = 11).
5. Payer presented NAMQR (i.e., Point of initiation method = 13 and 14).
6. Customer presented NAMQR (card chip data)

At the time of NAMQR code generation, payee/payer PSP receives request for NAMQR code generation from the respective payee / payer along with the various parameters. Payee / payer PSP sends the NAMQR parameters to Token Vault. Token Vault stores the NAMQR parameters and maps them against a Token Vault Unique Identifier and sends this xx-digit unique identifier to payee / payer PSP. Payer / payer PSP generates NAMQR with the assigned Token Vault Unique Identifier (in tag 65) and other parameters and NAMQR code is displayed on the payee PSP app.

When this NAMQR code is scanned by the payer / payee PSP app, the respective payer / payee PSP sends NAMQR code validation request to Token Vault. Token Vault validates the NAMQR code parameters as scanned with the NAMQR parameters available in the Token Vault and sends the NAMQR code validation successful response to payer / payee PSP. In this manner, the Token Vault ensures that the NAMQR code is validated and if there is any discrepancy in any of the parameters (e.g., merchant identifier, amount, etc), Token Vault shall provide failure response and hence prevent transaction using invalid NAMQR code.

Refer sections 'Payee presented NAMQR code payment (using smart phone mobile banking application', 'Payee presented NAMQR code payment (using USSD channel)' and 'Payer presented NAMQR code payment – (Request to Pay)' for illustration of transaction flow using Token vault.

7. Comparison between EMVCo, NQR and NAMQR specifications

[23] For the purpose of this document, "Token Vault" means any generic Token Vault operated by a Payment System Operator (PSO) or a PSP as per the terms of authorisation issued by BON to such a PSO and / or PSP. BON may consider, at its discretion, one common Token Vault as a national infrastructure and "public good" to be operated by an entity specifically approved by BON for this purpose or allow any PSP(s) to use their proprietary Token Vaults or a combination of both, so long such Token Vault(s) adhere to the common standards, specifications, protocols and are accessible to all the PSPs for a fair price.

Parameter	NAMQR specifications	NQR specifications by Namclear	EMVCo specifications
Interoperability	Across card rails, existing payment streams and IPP	Across card rails, existing payment streams and IPP	Only within card rails and ATM payment system
Key security feature	CRC (tag '63' in NAMQR code specifications) A duly certified Token Vault may be used (refer section 'NAMQR Security Risks Mitigation' for details). When IPP is implemented, Signed QR may be used for App based IPP transactions (refer section 'Signed QR')	Token Vault	CRC (tag '63')
Person-to-Person one-time (payee presented)	Tags Available	Tags Available	Tags not available
Person-to-Person recurring (payee presented)	Tags Available	Tags Available	Tags not available
Person-to-Person one-time (payer presented)	Tags Available	Tags Available	Tags not available
Person-to-Person recurring (payer presented)	Tags Available	Tags Available	Tags not available
Person-to-Merchant one-time (merchant presented)	Tags Available	Tags Available	Available
Person-to-Merchant recurring (payee presented)	Tags Available	Use case available, required tags not available	Tags not available
Person-to-Merchant one-time (payer presented)	Tags Available	Tags Available	Not available (card data available, but not bank account or e-money wallet)
Person-to-Person recurring (payer presented)	Tags Available	Tags not available	Tags not available
Digital voucher	Tags Available	Use case available, required tags not available	Tags not available
Cash withdrawal from ATM	Tags Available	Available	Tags not available
International merchant payment	Tags Available	Tags not available	Tags not available

Customer presented static QR with Payment card chip data	Tags Available	Tags not available	Tags available
Score	14/14	9/14	3/14

8. Compliance of NAMQR Specifications with the relevant BoN Guidelines[24]

Sr. No.	BoN guideline	NAMQR specifications
1	Banks, authorized non-bank payment service providers and Fintech's should be able to offer both types of payment QR codes (i.e., Merchant Presented QR code and Customer Presented QR code) to the public given the role and benefits of both options to consumers and merchants.	**Compliant** Both merchant presented and customer presented codes are included in NAMQR specifications.
2	Both merchant and consumer presented QR codes can either be static or dynamic	**Compliant** Both merchant and customer presented QR codes can be static or dynamic.
3	NPS should adopt open source QR code specifications without differentiating between merchant presented and customer presented QR codes	**Compliant** There is only one NAMQR specifications that include both merchant presented, and customer presented QR codes.
4	Before deciding on and building a QR specification, it is important to clearly define the payment use cases and business application scenarios in the domestic payment ecosystem. Consideration should be given to whether the QR codes will be used in-store at merchants, whether they will have both online and offline payment capabilities, and whether they are peer-to-peer payments and / or cross-border payment scenarios, among others. The NPS industry should be guided by international best practice.	**Compliant** NAMQR specifications cater to various use cases including the following: 1. In-store at merchants 2. Online and offline payment capabilities

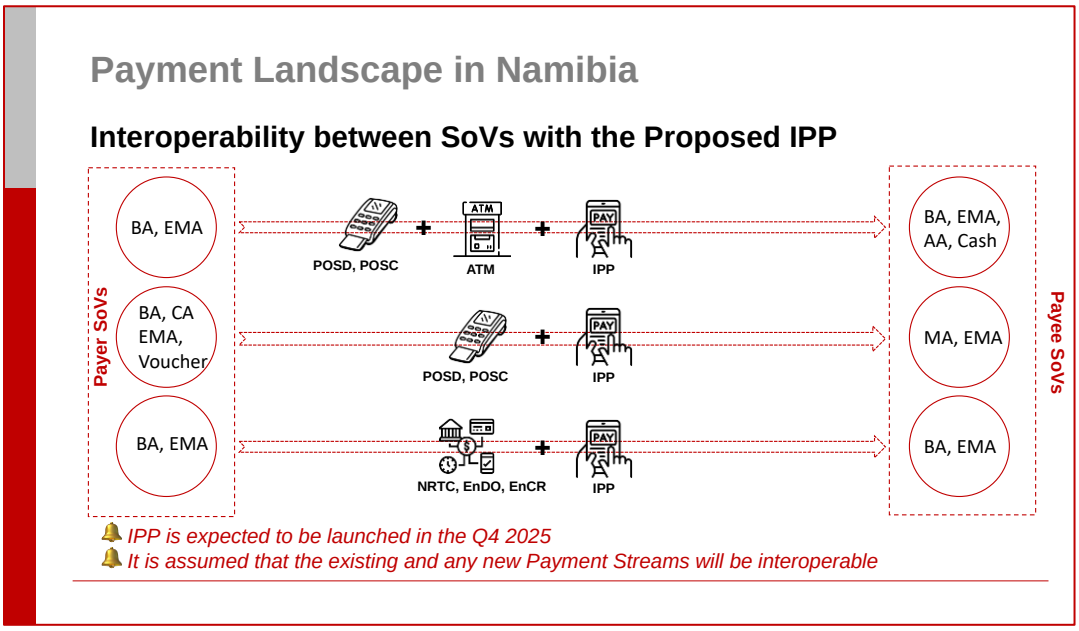
[24] Refer 'Guidelines on the Standardization of Quick Response'

<table>
<tr><td></td><td></td><td>(refer tag ‘Initiation mode’ in unreserved template 80)
3. P2P payments
4. Cross border payments with international NAMQR (i.e., purpose = 11)</td></tr>
<tr><td>5</td><td>Technical specifications: The industry should establish a common structure and format for QR codes, including the length or size, error correction level, and encoding scheme, to ensure that they can be easily scanned and processed by various payment platforms.</td><td>Compliant
Single NAMQR specifications with common structure and format of QR code, including the length or size, error correction level, and encoding scheme</td></tr>
<tr><td>6</td><td>Level of interoperability: The industry should ensure that payment QR codes can be used across different payment platforms, banks, FinTech’s, payment service providers, and wallets, etc., facilitating seamless transactions for users. All QR code standards should be interoperable with all payment instruments to fulfil the matrix presented in the table below.
<table>
<tr><th></th><th>Bank</th><th>Non-Bank</th><th>EFT</th><th>Card</th><th>E-money</th><th>App</th></tr>
<tr><td>Bank</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Bank</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>EFT</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Card</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E-money</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>App</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td><td>Compliant
NAMQR code can be used across different payment platforms and interoperable with all payment instruments.</td></tr>
<tr><td>7</td><td>Security and privacy: The industry should ensure that they implement measures to protect user information and transaction data from unauthorised access, tampering, and other security threats. All safety and privacy aspects of payment QR codes should at a minimum be guided by and comply to Determination of the Operational and Cybersecurity Standards within the National Payment System (PSD-12). Two-factor authentication should be required for every QR Code payment.</td><td>Compliant
CRC (tag ‘63’ in NAMQR code specifications)
A certified Token Vault – as approved by BON - may be used (refer section ‘NAMQR Security Risks Mitigations’ for details).
When IPP is implemented,</td></tr>
</table>

		Signed QR may be used for App based IPP transactions (refer section 'Signed QR')
8	Accessibility and usability: The industry should ensure that payment QR codes are easily accessible to users, with clear guidelines on how to generate, scan, and use them.	**Compliant** NAMQR is accessible from smart phone as well as feature phone over USSD channel. Refer comment above.
9	Cost effectiveness: It is the Bank's position that QR codes solutions should be in the public interest, promote competition and efficiency and comply with the standards determined by the Bank	**Compliant**

9. NAMQR to facilitate Interoperability across existing and proposed payment streams

The NAMQR standard has been developed with an objective to achieve interoperability across the existing and proposed payment streams in Namibia. The following illustration depicts how the examples illustrated in the Section 6 'Day to day examples of several Use Cases for P2P and P2M retail payments will be supported by NAMQR while using various payment rails in Namibia.



8

NOTE: This illustration highlights how NAMQR can avoid fragmentation and promote interoperability within and across existing payment systems (NRTC, EnCr, EnDO, POSD, POSC, ATM) as well as the proposed IPP.

10. Summary of the existing and proposed retail payment streams in Namibia

Following payment streams, and the relevant payment stream participants[25] were considered for development of the NAMQR standards.

Payment stream	Purpose	Participants
NRTC	In the Near Real-Time Credit Stream, a financial institution initiates a payment from an account (A) belonging to one of its account holders to bank account (B) at a different financial institution. If all conditions are met, the funds are transferred from account A to account B within seconds.	Financial institutions and PSPs authorized by BoN
EnDO	In the Enhanced Debit Order Stream, a financial institution requests payment to an account (A) belonging to one of its account holders, from bank account (B) at a different financial institution. If all conditions are met, this results in the transfer of funds from account B to account A.	Financial institutions and PSPs authorized by BoN
EnCR	In the Enhanced Credit Stream, a financial institution initiates a payment from an account (A) belonging to one of its account holders to bank account (B) at a different financial institution. If all conditions are met, this results in the transfer of funds from account A to account B, in a matter of hours.	Financial institutions and PSPs authorized by BoN
ATM	The ATM Stream facilitates cash withdrawals at ATMs using a debit or credit card as the payment instrument. This process results in funds being transferred from the cardholder's account to the financial institution that owns the dispensed cash.	Financial institutions and PSPs authorized by BoN
POSD	The POS Debit Payment stream enables payments to be made at merchant points of sale using a debit card as the payment instrument. This results in the transfer of funds from the cardholder's bank account to the merchant's account.	Financial institutions and PSPs authorized by BoN, merchants
POSC	The POS Credit Payment stream allows payments to be made at merchant points of sale using a credit card as the payment instrument. This results in the transfer of funds from the cardholder's account to the merchant's account.	Financial institutions and PSPs authorized by BoN
IPP – Proposed[26]	The central payment and clearing system operated by Instant Payment Namibia to facilitate the real-time	Financial institutions and PSPs authorized by BoN. Banks and PIIs (Payment Instrument Issuers) will be

[25] Role of the participants in various payment streams is as approved by BoN from time to time. NAMQR specifications per se do not enhance nor diminish the extant roles of any participants. NAMQR specifications have been formulated to facilitate carriage of the requisite payload by generating the QR code appropriate for the given payment stream.

[26] Refer document '20250116_IPP Functional Specification Document (FSD)_v6.0'

	processing and routing of instant payment transactions between instant payment switch participants.	considered as SOV (Store of Value) providers while PFs (Payment Facilitators) and TPPPs (Third Party Payment Providers), also referred to as Enablers can provide auxiliary services such as mobile applications and integration services as per extant guidelines of BoN.

11. Day to day examples of several Use Cases for P2P and P2M retail payments

The following are a few of the sample use cases to illustrate the potential of NAMQR to facilitate payments across all existing payment streams as well as IPP using any of the SOVs.

1. Proximity payment at a merchant using merchant presented Dynamic QR code
2. Proximity payment at a merchant using merchant presented Static QR code
3. DTH payments from home
4. Cash withdrawals from ATM
5. Agent cash-out
6. International merchant payment at merchant location
7. Purchase of new subscription with merchant presented mandate
8. Gifting digital Cash vouchers (Mandate QR created by Payer)
9. Customer presented static QR for P2M Transactions
10. Payee presented Mandate for P2P recurring transactions

11.1 Proximity payment at a merchant using Dynamic QR code

1. Mary uses her bank provided mobile application to make payments to nearby grocery store.
2. After the purchase, grocery store PoS application generates a dynamic NAMQR code with the payment details.
3. Mary opens the bank app on her mobile and scans the NAMQR code on the PoS device or on the bill printed by the PoS.
4. Bank app takes her straight to pay screen with all values pre-populated from the NAMQR code.
5. She verifies the info on screen and clicks pay to complete the payment.
6. Both merchant and she get confirmation instantly.

11.2 Proximity payment at a merchant using Static QR code

In this scenario, say, a small one-person shop could simply print a static QR code issued by the acquirer bank (as per NAMQR specifications) containing the merchant address (e.g., IPP full form alias or merchant identifier) and name without need for any integration with a billing system to generate a dynamic NAMQR code. In the case of static QR codes, a customer simply scans the NAMQR code using a mobile banking application, enters the amount and authorizes the payment using the M-PIN.

1. Mary uses her bank provided mobile application to make payments to nearby grocery store.

2. Mary opens the bank app on her mobile and scans the NAMQR code displayed at the Merchant's counter.
3. The mobile banking application takes her to the "pay now" screen where she views the merchant's name, enters the amount and authorizes the payment using the M-PIN.
4. Both the merchant and Mary get confirmation instantly.

11.3 DTH payments from home

1. Nadeem subscribes to DTH in his house and wants to make a payment for on demand subscription.
2. Nadeem selects the channel and clicks "buy now".
3. DTH shows the details along with a NAMQR code for payment.
4. Nadeem opens his bank app on his mobile and scans the NAMQR code on the TV screen.
5. Bank app takes him straight to pay screen with all values pre-populated from the NAMQR code.
6. He verifies the info on screen and clicks pay to complete the payment.
7. He gets a confirmation on his mobile and the TV channel is automatically turned on for him to view.

11.4 Cash withdrawals from ATM

1. Deepak visits the ATM to withdraw cash.
2. Deepak inputs the amount for withdrawal on ATM display.
3. ATM shows the details along with a NAMQR code for payment.
4. Deepak opens his bank app on his mobile and scans the NAMQR code on the ATM screen.
5. Bank app takes him straight to pay screen with all values pre-populated from the NAMQR code.
6. He verifies the info on screen and click pay to complete the payment.
7. He gets a confirmation on his mobile and the ATM dispenses the cash.

11.5 Agent cash-out

1. Agent initiates the cash-out transaction with their Agent app (as provided by acquirer bank), generates a dynamic NAMQR code with the payment details such as amount.
2. Customer opens the bank's mobile banking application on their mobile and scans the NAMQR code on the Agent app.
3. The mobile banking application takes customer to the "pay now" screen where all the values (as per step 2) are pre-populated by reading the NAMQR code.
4. Customer verifies the information on screen (e.g., merchant name, amount), enters M-PIN and clicks pay to complete the payment.
5. Both agent and customer get confirmation instantly.

11.6 International merchant payment at merchant location

1. Mary uses her bank app to make payments to grocery store present aboard.
2. After the purchase, international grocery store PoS application generates a dynamic NAMQR code with the payment details.
3. Mary opens the bank app on her mobile and scans the NAMQR code on the PoS device or on the bill printed by the PoS.

4. Bank app takes her straight to pay screen with all values pre-populated from the NAMQR code.
5. Bank app display information containing foreign currency, FX rate & payable NAD value to Mary. Mary verifies the information and clicks pay to complete the payment.
6. Both merchant and she get confirmation instantly.

11.7 Purchase of new subscription with mandate (QR created by merchant)

1. A subscription form has been released by Chandan Co. for various services. To make the payment of the service seamless, Chandan Co. has printed mandate QRs (unique for each form) on their subscription forms.
2. A user who wants to avail the service, fills the form, scans the QR and authorizes the mandate. Finally, he submits the form to Chandan Co.
3. After the success purchase of the services, Chandan Co. will execute the mandate and received the funds.

11.8 Gifting digital Cash vouchers (Mandate QR created by Payer)

1. A corporate is gifting cash voucher to its employee on a festival occasion.
2. It creates mandate on the IPP full form alias of the employee's
3. NAMQR is generated for the mandates basis the above specification and is shared with the respective employee.
4. When the employee scans the QR, funds are immediately credited to his account.

11.9 Customer presented static QR for P2M Transactions

1. Customer generates a NAMQR code to pay through either bank account or card account or e-money wallet.
2. Merchant app scans customer NAMQR code and sends transaction to acquirer bank.
3. Acquirer bank sends transaction to NPS stream that they are onboarded with.
4. NPS stream sends transaction to the NPS stream that Issuer bank is onboarded with.
5. Issuer bank sends request to customer mobile to authenticate the transaction.
6. Customer views merchant name and authenticates with M-PIN to pay through bank account or e-money wallet or Card Pin to pay through card account.
7. Customer and merchant receive transaction status.

11.10 Payee presented Mandate for P2P recurring transactions

1. The payee bank app displays a mandate NAMQR with terms of mandate.
2. The payer uses her payer bank app to scan the mandate QR.
3. She views "Account name" of the payee.
4. She elects to authorize with her bank account and PIN.
5. Mandate is created and stored at payee and payer bank.
6. On the date of execution as per the mandate terms, the payer account gets debited, and the payee account gets credited.

Annexure I - Signed QR [27]

1. Signed QR

1.1 Signed QR

Namibia is in the process of launching IPP which is a version of UPI operated by NPCI in India. IPP specifications provide for a signed QR and it has been assumed that when banks implement IPP, they will also have implemented the signed QR which is an integral feature of UPI and hence IPP. This document discusses signed QR in the context of NAMQR because it will be a readily available component of IPP and not a separate requirement of NAMQR implementation. Moreover, as clarified earlier in the section 6.4 'NAMQR Security Risks Mitigation', NAMQR data is considered non confidential because it does not directly reveal sensitive information like bank account details, instead using an alias (or any surrogate value such as mobile number or any other such value assigned by the PSPs to identify their respective users) mapped to that SOV), thus protecting privacy of the payer and the payee. It is reiterated that the signed QR feature will be used only while making payments using IPP through mobile apps.

The threats of compromise of data integrity can also be mitigated through signed QR. QR code signing proves data integrity. Signed QR can be used for domestic [28] NAMQR for IPP app based transactions. Signing of QR provides security while making payments by the customer, and help reduce issues related to non-verified entities, that can act as a source of QR and can imitate as an authorized source.

Signed QR principles / rules:

1. "All QR based transactions if not originating from the trusted sources" (all unsigned QR) will appear as a warning to the end user. In case the QR is not signed, a warning message has to be displayed on the payer's app. Only post confirmation from the payer, app should move forward.
2. If QR is signed, then the application should bypass passcode page. PSP needs to skip the app passcode in case of signed QR.
3. Acquirer PSP changes: An Acquirer PSP should be able to generate a digital signature-based QR for which a public key will be uploaded by Acquirer PSP into IPP central system through dedicated API.
4. Issuer PSP changes: An Issuer PSP should be able to download public key of that specific merchant using dedicated API. Whenever QR is accessed by the customer, the validation of public key should happen and if it is not a signed QR, Issuer PSP will throw an error "Unsolicited / Unauthenticated QR call". Thus, the choice will be given to the customer to proceed or decline the transaction.
5. P2P PSP changes: A payee PSP should be able to generate a digital signature-based QR for which a public certificate will be uploaded by payee PSP into IPP central system through dedicated API.
6. PSP needs to follow the deep linking specifications.

1.2 Manage Verified Address Entries

[27] Refer document 'UPI Linking Specification cer 1 7 2_V12' for Signed QR specifications shared in this section

[28] Signed QR for international transactions is not available as per extant IPP specifications.

IPP offers a mechanism to protect users from attempts to spoof well known merchants such as Insurance, Travel, e-commerce players, telecom players, bill payment entities, etc. This mechanism is an API, where the PSPs can manage, and access the common collection of verified address entries. IPP, with the help of PSPs, has defined a process to manage these entries.

Merchant or acquirer PSP on behalf of merchant need to generate a key pair (public and private key with ECDSA 256 + SHA 256 specifications).

If acquirer PSP has generated the key pair, then private key can either be shared with merchant for QR generation or can be integrated in SDK directly. Merchant and acquirer PSPs shall also add provision for update of key pairs.

Key Upload: Then merchant needs to share this public key with its acquirer PSP. Then acquirer PSP will upload its merchant public key on IPP with Manage VAE API. If acquirer PSP has generated the key for its merchant, then it can directly upload on IPP.

1.3 List Verified Address Entries - Signed QR

Issuer PSP app reads the signed QR.

If OrgId = '000000' & MCC is non-zeros, then Issuer PSP should call ListVAE with reference to Merchant IPP full form alias for fetching merchant specific key (Verified merchant will fall under this rule).

If OrgId and MCC are non-zeros, then Issuer PSP should call first ListVAE with Merchant IPP full form alias. If no entry is found in ListVAE, then the Issuer PSP can call ListKeys with parent OrgId to get the keys (mostly non verified merchants will fall under this rule).

Key Download: Issuer PSP server needs to download all merchant keys and cache it on their server. This cache needs to be updated daily by the Issuer PSP server. Each public key downloaded must be mapped with the Merchant IPP full form alias for which the key was uploaded.

Searching the key: OrgId & Merchant IPP full form alias need to be extracted first. As the Orgid id '000000', the public key needs to be looked in list VAE cache with Merchant IPP full form alias as search parameter. This key will be used for verifying the signature.

1.4 List Keys – Signed QR

Payer PSP app reads the signed QR. If OrgId present in QR is non-zeros & MCC = 0000, then Payer PSP should call ListKeys for fetching Payee PSP keys.

This scenario broadly refers to QR generated by Payee PSP applications for P2P transactions. In such scenarios, public key could not be found in List VAE as the Payee is not a merchant.

Key Download: Payer PSP server needs to download all PSP app keys and cache it on their server. This cache needs to be updated daily by the payer PSP server. Each public key downloaded must be mapped with the payee PSP OrgId for which the key was uploaded.

Searching Key: OrgId & Payee IPP full form alias need to be extracted first. As the orgid id ‘159991’, the public key needs to be looked in List Keys cache with OrgID as the search parameter. This key will be used for verifying the signature.

1.5 Reading Signed QR

1. Following is the verification logic for reading the signed QR on IPP

    a. If OrgId present in QR is non-zeros & MCC = 0000, then Payer PSP should call ListKeys for fetching Payee PSP keys
    b. If OrgId = 000000 & MCC is non-zeros, then Issuer PSP should call ListVAE with reference to Merchant IPP full form alias for fetching merchant specific key (Verified merchant will fall under this rule)
    c. If OrgId and MCC are non-zeros, then Issuer PSP should call first ListVae with Merchant IPP full form alias. If no entry is found in ListVAE, then the Issuer PSP can call ListKeys with parent OrgId to get the keys (mostly non verified merchants will fall under this rule).
    d. Both OrgId and MCC = 0000 such a scenario doesn’t exist

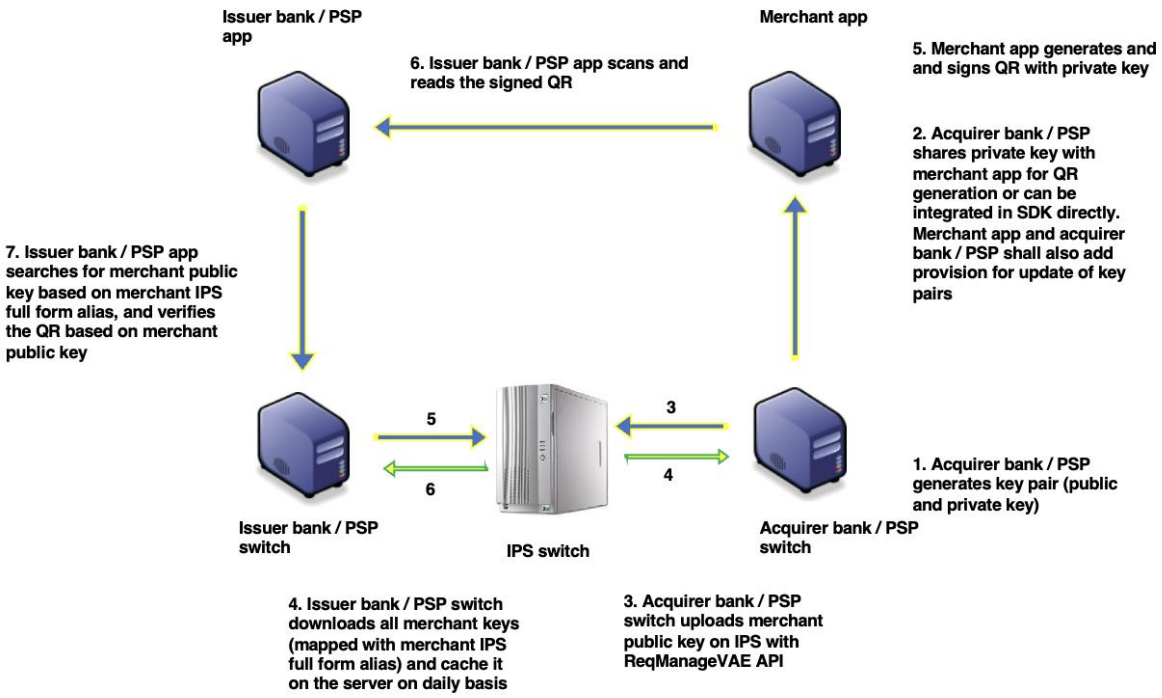
1.6 Signature

Signing of QR can be broadly segregated into merchant initiated & payee-initiated QR. The signing method for both are similar, however verification method for both of them varies.

Merchants can initiate QR from their mobile application, generate signed QR from their terminal, POS, exit sensors. All the mentioned protocol for merchant-initiated method follow identical process for signing and verification.

1.7 Merchant initiated

1. IPP plays central role to provide certificate registry for all Acquirer PSPs and Merchants.
2. Acquirer PSP adds the public key for all their merchants using Manage VAE API which has block to capture public key of the merchant.
3. Issuer PSP uses the List VAE API to retrieve the public key of the merchant.
4. Merchant app uses the private key to sign the hashed content of the QR (SHA256 with RSA).
5. The Issuer PSP app uses the public key to verify the content integrity.
6. This helps to secure the data flows between PSPs apps using QR.



1. **Key generation:** Merchant app or the acquirer PSP switch on behalf of merchant needs to generate a key pair (public and private key with (ECDSA 256 + SHA 256) specifications.

   If acquirer PSP switch has generated the key pair, then private key can either be shared with merchant app for QR generation or can be integrated in SDK directly. Merchant app and acquirer PSP shall also add provision for update of key pairs.

2. **Key Upload:** If merchant app has generated the key pair, then merchant app needs to share this public key with their acquirer PSP switch. Then acquirer PSP switch will upload their merchant public key on IPP with Manage VAE API. If acquirer PSP has generated the key for their merchant, then it can directly upload on IPP.

   Acquirer PSPs public key will be available at VAE or List key entry.

   a. List VAE is having the merchant entry and having Signature key, then the key will be used for validating QR
   b. List VAE is having merchant entry and no signature key, use parent key for checking signature basis parent Org ID
   c. No entry in List VAE, use parent key for checking signature basis parent Org ID (non-verified merchant).
   d. List Keys are used in case of fetching keys for P2P

3. **Signing of QR**:

   a. Step 1: The merchant generates a QR string.

b. Step 2: The Specified QR string needs to be signed using ECDSA with SHA256 algorithm.
c. Step 3: The output of the signature should be encoded with base 64.
d. Step 4: The final encoded value should be appended to original QR string in the respective tag.

4. **Key Download:** Issuer PSP server needs to download all merchant keys and cache it on their server. This cache needs to be updated daily by the Issuer PSP server. Each public key downloaded must be mapped with the Merchant IPP full form alias for which the key was uploaded.

5. **Searching the key:** Orgid & Merchant IPP full form alias need to be extracted first. As the orgid id '000000', the public key needs to be looked in list VAE cache with Merchant IPP full form alias as search parameter. This key will be used for verifying the signature.

6. **Verifying the QR:**

   a. Step 1: The signature part needs to be extracted and separate the original text from the encrypted code.
   b. Step: 2 Then the appended value must be decoded with base 64
   c. Step 3: The entire QR string excluding the signed part will be passed into verify function along with signature and the public key of merchant for verification.

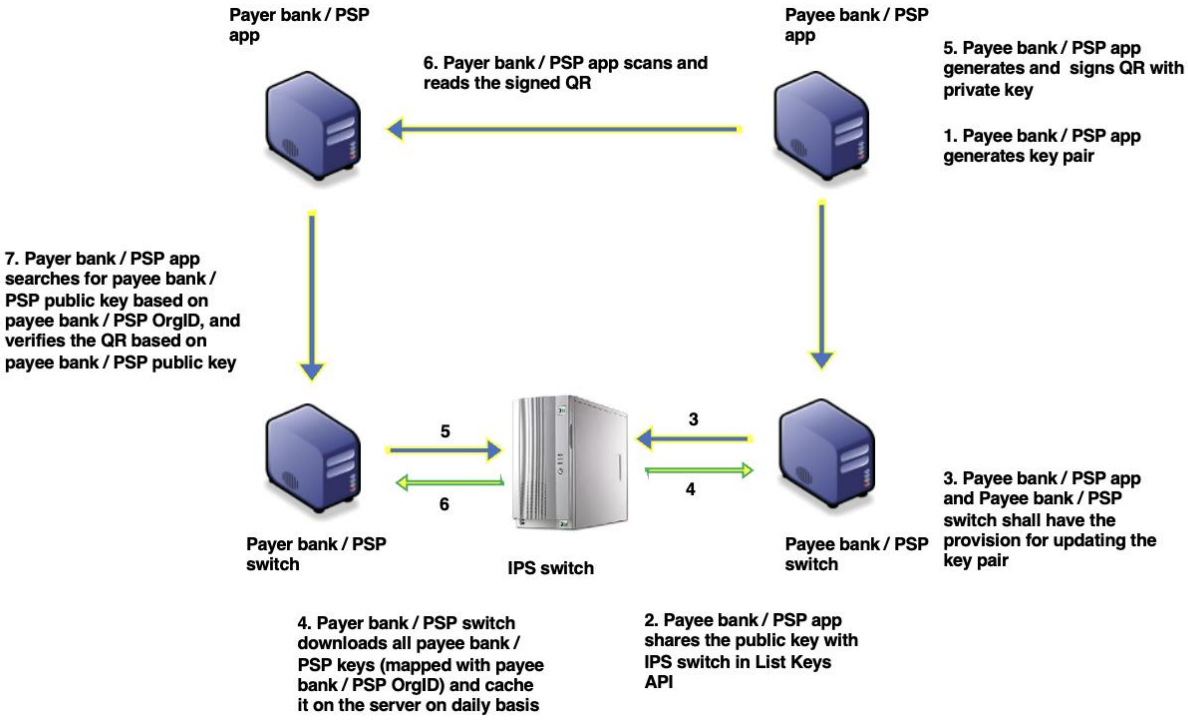
7. **Actions:**

   a. If the verification is successful, then the application should bypass passcode page
   b. If verification is failure either due to corruption or tampering the signature, then the QR request must be declined stating 'QR is tampered or corrupt'
   c. If signature is not present in QR, then the application should show warning message to user that the 'source of QR could not be verified' and shall request for passcode to proceed with the payment.

1.8 Payee initiated

This scenario broadly refers to QR generated by payee PSP app for P2P transactions. In such scenarios, public key could not be found in List VAE as the Payee is not a merchant.

1. Payee PSP app generates key pair and shares the public key using List Keys API with IPP .
2. Payer PSP retrieves all the other payee PSP keys using the List Keys API.
3. Payee PSP app uses the private key to sign the hashed content of the QR (SHA256 with RSA).
4. The Payer PSP app uses the public key to verify the content integrity.



1. **Key generation & upload:** The key pair will be generated by the Payee PSP app and shall be shared with IPP for the keys to get updated in List Keys API. Payee PSP app and Payee PSP switch shall have the provision for updating the key pair.

2. **Signing of QR:**

   a. Step 1: The payee PSP app generates a QR string
   b. Step 2: The Specified QR string needs to be signed using SHA256 with ECDSA algorithm
   c. Step 3: The output of the signature should be encoded with base 64
   d. Step 4: The final encoded value should be appended to original QR string in the respective tag.

3. **Key Download:**

Payer PSP server needs to download all payee PSP app keys and cache it on their server. This cache needs to be updated daily by the payer PSP server. Each public key downloaded must be mapped with the payee PSP OrgID for which the key was uploaded.

4. **Searching Key:**

OrgID & Payee IPP full form alias needs to be extracted first. As the orgid id ‘159991’, the public key needs to be looked in List Keys cache with OrgID as the search parameter. This key will be used for verifying the signature.

5. **Verifying the QR:**

Step 1: The signature part needs to be extracted and separate the original text from the encrypted code

Step 2: Then the appended value must be decoded with base 64

Step 3: The entire QR string excluding the signed part will be passed into verify function along with signature and the public key of payee for verification

6. Actions:

a. If the verification is successful, then the application should bypass passcode
b. If verification is failure either due to corruption or tampering the signature, then the QR request must be declined stating ‘QR is tampered or corrupt’
c. If signature is not present in QR, then the application should show warning message to user that the ‘source of QR could not be verified’ and shall request for passcode to proceed with the payment.