Pursuant to Article 36, paragraph 1, sub-paragraph 1.17, and Article 65, paragraphs l and 2, of Law No. 03/L-209 on the Central Bank of the Republic of Kosovo, (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010) amended and supplemented by Law No. 05/L -150 (Official Gazette of the Republic of Kosovo No. 10/3 April 2017), Article 8, paragraph 1, sub-paragraph 1.1, and paragraph 2, sub-paragraph 2.3, of Law No. 04/L-155 on Payment System (Official Gazette of the Republic of Kosovo No. 12/3 May 2013), the Executive Board of the Central Bank of the Republic of Kosovo, at the meeting held on 20 September 2024, approved the following:

INSTRUCTION

ON QR CODE STANDARD

Article 1
Purpose and Scope

1. The purpose of this instruction is to define rules and technical requirements for operating of QR Code structure in Republic of Kosova. This QR code specification covers retail payments and bill payment.
2. The standard of QR code will help promote wider use of mobile retail payments in Kosovo through interoperability and the provision of a consistent user experience for merchants and consumers.
3. This Instruction shall apply to payment transactions that are made via QR code. All payment service providers providing QR codes in the Republic of Kosovo are subject to the provisions of this Instruction.

Article 2
Definition of Terms

1. “CBK” - Central Bank of the Republic of Kosovo

2. “Account” The identifier that uniquely distinguishes an individual account but does not include the identifier of financial institution at which the account is held
3. “Account Servicing Payment Service Provider (ASPSP)” A PSP providing and maintaining a payment account for a payer / payee.
4. “Basic Bank Account number (BBAN)” The identifier that uniquely distinguishes an individual account, at a specific financial institution, in a particular jurisdiction. The BBAN includes the bank identifier of the financial institution servicing that account
5. “CICO Agent (Cash-in Cash-out Agents)” Cash-in Cash-out Agents can be individuals or organizations, and typically operate in areas where traditional banks are not present. Some of the services that are provided through this agency banking model include cash deposits, cash withdrawals, bill payments, and mobile money transfers.
6. “Consumer” The person purchasing/using the goods and/or services.
7. “Consumer-presented data/QR Code” Data provided by the consumer at the merchant’s POI (Point of Interaction). Also referred to as Payer-presented QR Code
8. “Credit Transfer” A payment instruction given by an originator (Payer/Debtor) to an originator participant (Debtor Participant) requesting the execution of a credit transfer transaction, comprised of the information necessary for the execution the credit transfer and is directly or indirectly initiated.
9. “Customer” A payer or a beneficiary may be either a consumer or a business (merchant).
10. “Digital Wallet” A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
11. “International Bank Account Number (IBAN)” An internationally agreed system of identifying bank accounts across national borders to facilitate the communication and processing of cross-border transactions and includes the country code, 2 check digits and a BBAN.
12. “Instant Payment System / Fast Payment System” Electronic retail payment solutions available 24/7/365 and result in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee’s account with confirmation to the payer (within seconds of payment initiation).
13. “Lock Transaction” The conditional Lock Transaction messages are sent between the consumer’s MCT service provider and the Merchant’s MCT service provider via the HUB to prevent that multiple Consumers from different MCT service providers paying for the same transaction after strong customer authentication. The Transaction Lock function is required in instances where the QR-code stays active for a time period that could enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator. If two Consumers perform an SCA on the same transaction, the Consumer with the successful SCA for which the lock function sent by their MCT service provider reaches the MSCT service provider of the Merchant first is the one for which the transaction is locked.

14. “Merchant” A beneficiary within a payment scheme for payment of the goods or services purchased by the consumer. A merchant may also be referred to as payee i.e., the beneficiary/creditor in the transaction and includes private individuals, businesses, corporates, governments, etc.
15. “Merchant-presented data/QR Code” Data provided by the merchant’s POI to the consumer.Also referred to as Payee-presented QR Code
16. “MCT” Mobile Initiated Credit Transfer
17. “MCT Service Provider” A service provider that offers or facilitates an MCT service to a payer and/or payee based on a fast payment transaction. This may involve the provision of a dedicated MCT application for download on the customer’s mobile device or the provision of dedicated software for the merchant POI (physical or virtual). As an example, an MCT service provider could be a PSP (e.g., an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP.
18. “QR Code” Quick Response Code is a type of two-dimensional matrix barcode
19. “QR Code Payload Method” refers to way in which (or the format used) for the QR Code Payload i.e. whether the QR Code will contain a Token or Proxy or Data in Clear Text.
20. “Payee-presented data/QR Code” Data provided by the merchant’s POI to the consumer. Also referred to as Merchant-presented QR Code.
21. “Payer-presented data/QR Code” Data provided by the consumer at the merchant’s POI. Also referred to as Consumer-presented QR Code.
22. “Payment Scheme/ Scheme” The scheme is a set of rules, practices, procedures, standards and contracts, defined by Payment Service Operator (CBK) that Participants must adhere to in order to participate in the Payment System (e.g., IPS)
23. “Payee” A natural or legal person who is the intended recipient/beneficiary of funds (examples include merchant, business and an individual).
24. “Payer” A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives the order to initiate a payment.
25. “Payload/QR Payload” All the data included in the QR Code related to a transaction.
26. “QR Payload Issuer” The entity responsible for issuing the payload. This may be the MSCT service provider or a different entity (e.g., an acquirer), operating under this MSCT service provider.
27. ”Point of Interaction (POI)” The initial point in the merchant’s environment (e.g. POS, vending machine, payment page on merchant website, QR code on a poster, etc.) where data is exchanged with a consumer device (e.g., mobile phone, wearable, etc.) or where consumer data is entered to initiate an instant credit transfer.
28. “PSD2” PSD2 is a European regulation for electronic payment services. It seeks to make payments more secure in Europe, boost innovation and help banking services adapt to new technologies.

29. “Proxy” A Proxy is an easy to remember identifier linked to the Customer's account that enables Customers to make payments using this identifier instead of an account number. It is sometimes referred to as an “alias” and is used retrieve a payment account identifier linked to the said proxy (e.g., mobile phone number, e-mail address, etc.). As an example, a proxy could be used to replace an IBAN and is then used to retrieve the associated account details.
30. “Tokenisation” Process of substituting payment account, PSU identification data or transaction related data with a surrogate value, referred to as a token.
31. “Token” Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payment account (e.g., the IBAN), consumer identification data (e.g., CustomerID) or transaction related data. Payment Tokens must not have the same value as or conflict with the real payment account related data. If the token is included in the Payee-presented data it might be referred to as a merchant token; if the token is included in the consumer-presented data it might be referred to as a consumer token.

Article 3
Role and function of QR Code

1. A QR Code is a type of two-dimensional barcode which allows for the encoding of data in both horizontal and vertical axes. QR Codes are machine-readable and can thus be read by most smartphone cameras. They are user-friendly and have become ubiquitous in many sectors and are increasingly being used in payments. A QR code is based on proximity technology for the data exchange between two parties, such as the consumer and the merchant, to enable the initiation of a payment.
2. QR Code will support access to innovative digital payment instruments and channels aiming to further develop digital financial services in the jurisdiction driving financial inclusion, meeting the needs of individuals, businesses, the financial sectors and keeping pace with the regional and international financial and economic developments.
3. QR Codes provide a myriad of benefits for both the consumer and the merchant including convenience and ease of use, better security, and cost effectiveness for merchants and acquirers.
4. QR Code specification will promote interoperability facilitating payments between different payment schemes, e-wallets and banks encouraging merchants to adopt the QR code as a payment method.
5. The QR Code provides a valuable additional user experience for initiating and accepting payments between customers and merchants. In particular, QR code standard will bring practical benefits to providers and customers in a number of ways, including:
   5.1. Simplifying the process of initiating and making payment transactions.
   5.2. Use of QR codes is expected to increase the safety and security of payment transactions by direct data capture that avoids payment mistakes.

5.3. Use of QR codes will unify payment modes across the entire industry, so that customers do not have to go through the process of memorizing different merchant payment numbers every time they make purchases.

Article 4
The QR code standard used

1. This QR Code Standard provides guidance on how data should be presented by the participants including what fields are mandatory/optional. Customer scanning apps must interpret the data according to this standard.
2. The CBK has selected the EPC QR Code standard on which to develop their domestic QR Code Standard to enable the use of QR codes for the use cases envisaged by the CBK.
3. EPC QR Code standard comprises:

   3.1. EPC024-22 Version 2.0 "Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers", 10 January 2023, and

   3.2. EPC212-21 Version 1.1 "Standardisation and governance of QR-codes for IPS at POI"
4. The use of the EPC QR Code Standard will also make interoperability with other the European Payment Schemes easier in the future.
5. Guidelines for QR Code structure and the implementation model is described in Annex 1 " EPC QR Code Specification for Instant Payments".

Article 5
Principles to provide QR code

1. The following principles apply to a Financial Institution/Government entities wishing to provide Consumers with QR code enabled products and services:

   1.1. All QR code-based products and services must comply with the defined QR code standard and the rules of the scheme in which those product and services are used;

   1.2. In order to reduce the risk of fraud and theft of a Payer or Payee's credentials, only credit push and request to pay model payments (which result in credit push payments) are supported, whereby the Payer instructs its financial institution to debit their account and credit the Payee;

   1.3. The appropriate security measures must be implemented to ensure the safety and confidentiality of Customer data refer to Article 13;

1. In the use cases where Consumer-presented mode is used, in line with the EPC requirements, the proposed model makes use of tokenization to avoid the consumer's account details being exposed;

2. Any new product and service innovations based on QR code must be interoperable, and the financial institution/service operator must adhere to the certification process defined by CBK. The financial institution will have to obtain the approval of the CBK to implement any new innovations and must prove the interoperability of the innovation;
3. In the event of disputes, the scheme rules as prescribed by the scheme in which the QR code was used to initiate a payment or a request for payment, will apply;

Article 6
QR code modes of exchange

1. There are two modes of exchange:
   1.1. Payee-presented mode (also referred to as Merchant-presented mode) where the data refers to merchant identification data and transaction data, and
   1.2. Payer-presented mode (also referred to as Consumer-presented mode) where the data refers to Consumer identification data.
2. The Payee-presented QR code enables the Payee (e.g., a merchant) to present a request for payment to a Payer, who can then verify the associated transaction information and the authorise the payment to the Payee or reject the request for payment. It supports multiple payment types, including bill payments, online payments, and point-of-sale payments. This interaction requires the Consumer to possess a smartphone, with an application which allows the Consumer to scan the Payee presented QR code, to initiate a payment transaction. The payment is then processed by the Consumer's application on their device, and is routed to the merchant's financial institution, and both parties are typically notified of the success of the transaction.
3. The Payer-presented QR code enables the Payer to make payments using credentials associated with an account and provisioned on their device. The Payer generates a QR code from within their mobile application and the Payee scans the QR code, communicates with the Payer's payment service provider, who then initiates the payment (with the explicit approval of the Payer) for the goods and/or services and finally sends the confirmation of payment to the Payee. It supports the online payments, point of sale payments, the depositing and withdrawal of cash.

Article 7
Implementation Model

1. The QR codes implementation model for Kosovo is based on the decentralised model where each Participant must provide their own technology for generating, decoding, decrypting and verifying a QR Code, including performing the tokenisation and detokenization, if applicable.

Article 8
Type of QR codes

QR codes are classified into static and dynamic QR codes:

1. Static QR code, and
2. Dynamic QR code.

Article 9
Static QR code

1. A static QR code contains information that is fixed and cannot be changed once the QR code has been generated. A static QR code, once generated, is used for multiple transactions. The static QR codes have lower requirements, as only one of the parties needs a feature phone, and the other can use a printed QR code.
2. Static QR codes can be used in the context of Payee-presented and Payer-presented QR codes.
3. They are well suited for small merchants (e.g., florist or merchants that sell goods at a fresh produce market, etc.) that encode their payment details in the QR code. It can also be suitable for transactions with a fixed amount (such as bus Tickets). The QR code can then be scanned by the Consumer using their mobile application and, if required, the Consumer enters the amount when prompted to do so. The merchant's information, such as shop name, is displayed on the mobile device for verification and once the payment is confirmed by the Consumer the payment is initiated.
4. In the context of Consumer-presented static QR codes, they can be used in creating Financial Identities to access various banking services.
5. The static QR code can be riskier than the dynamic QR code as any fraudster could overlay the merchants' QR code (in case of Merchant presented Static QR Code) with a fake QR code or photograph a Consumer's QR code (in case of Consumer presented Static QR Code) and the transaction amounts are paid into the incorrect Payee account. There are certain mitigating actions that can be used such as the use of a Token or URL instead of the payment credentials. The Token or URL is then used to retrieve the payment details.
6. In the example shown in **Error! Reference source not found.**, at the Annex 2 "Diagrams and payment flow", the scenario is presented where the payment credentials are included in the QR code (thus not on the scenario where a Token or URL is used).

Article 10
Dynamic QR code

1. In the case of a dynamic QR code, a different code is generated specifically for each transaction. This makes them the best fit for payment and business purposes. Dynamic QR codes are commonly used in payments, e-commerce payments, bill payments as well as payments at self-service kiosks.
2. Dynamic QR codes can be used in the context of Payee-presented and Payer-presented QR

codes.

3. A typical use case of Payee-presented dynamic QR codes is the payment for online shopping where a Consumer purchases goods or services and then proceeds to the checkout at an online shop, the merchant then generates the dynamic QR code and presents it to the Consumer to scan, embedded with the details of the transaction. The Consumer then scans with a mobile application, the dynamic QR code (with the details of the transaction embedded) to initiate the payment. The merchant's information (such as Merchant Name) and variable invoice information (such as payment amount) are displayed on the mobile device for verification before the payment is initiated.
4. In the context of Consumer-presented mode (Payer-presented mode) the Consumer that wishes to deposit cash (Cash in) can generate a QR Code using the application on their mobile device indicating the participating payment service provider (CICO Agent) at which they wish to deposit the cash and their account. Then take the cash to the participating payment service provider (CICO Agent) who will then scan the QR Code and take the cash which is then reflected immediately as a credit in the account of the consumer.
5. In the example shown in **Error! Reference source not found.**, at the Annex 2 "Diagrams and payment flow" scenario is presented where the payment credentials are included in the QR code (thus not on the scenario where a Token or URL is used).

Article 11
Use Cases for Kosova

1. Use Cases mapping to QR Code is shown in below table:

Table 1: Mapping to QR Code Use Case

	Use Case	QR Mode Used	QR Code Type
1	Instant Credit Transfer	Payee-presented	Dynamic
2	Payment Initiation	Payee-presented	Static Dynamic
3	E-commerce	Payee-presented	Dynamic
4	Request to Pay	Payee-presented	Dynamic
5	Bill Presentment and Payment	Payee-presented	Static Dynamic
6	Cash-in	Payer-presented	Dynamic
7	Cash-out	Payer-presented	Dynamic

Article 12
Stakeholders/Actors

1. The stakeholders involved in the process of making payments with QR code and mentioned in this guidance, are as follows:

    1.1. Account Servicing Payment Service Provider (ASPSP): A PSP providing and maintaining a payment account for a Payer or Payee. Also referred to as the Payer Participant/Debtor Agent, Payee Participant/Creditor Agent, Bank, Participant. The MCT Service Provider and the ASPSP could be the same institution and in many cases that is the case.

    1.2. Cash-in Cash-out Agent (CICO Agent): A Cash-in Cash-out Agent can be an individual or organization and they typically operate in areas where traditional banks are not present. Some of the services that are provided through agency banking include cash deposits, cash withdrawals, bill payments, and mobile money transfers. The role of CICO can be covered by the MCT Service Provider but could be different. Depending on the model implemented the CICO could be a Participant in the CBK FPS (Direct or Indirect Participant) or they could only have a relationship with an MCT Provider (i.e. the relationship is between the CICO Agent and the MCT Service Provider).

    1.3. CBK FPS: Refers to the Fast Payment Clearing (Instant Payment), which will be implemented.

    1.4. Consumer: The person purchasing/using the goods and/or services. Also referred to as the Payer. In some scenarios the Consumer could be a Business purchasing goods or services.

    1.5. HUB: The “infrastructure” that enables interconnectivity between the respective MCT service providers and other stakeholders in the QR Code ecosystem. It could be existing networks, the future CBK FPS or any other interbank network.

    1.6. Mobile (instant) Credit Transfer Application (MCT App): The mobile application hosted on the mobile device and is provided by the MCT Service Provider.

    1.7. Mobile (instant) Credit Transfer (MCT) Service Provider: A service provider that offers or facilitates an MCT service to a payer and/or payee based on a fast payment transaction. This may involve the provision of a dedicated MCT application for download on the customer’s mobile device or the provision of dedicated software for the merchant POI (physical or virtual). As an example, an MCT service provider could be a PSP (e.g., an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP. Note: the MCT Service Provider and the ASPSP could be the same institution and in many cases that is the case.

    1.8. Merchant: A beneficiary within a payment scheme for payment of the goods or services purchased by the consumer. A merchant may also be referred to as payee i.e., the beneficiary/creditor in the transaction and includes private individuals, businesses, corporates, governments, etc.

    1.9. Payee reference party: A person/entity on behalf of or in connection with whom the payee receives a payment.

    1.10. Payee: An individual, a business or merchant who is the intended recipient/beneficiary of funds (examples include merchant, business and an individual).

1.11. Payload Issuer: The entity responsible for issuing the QR payload. This may be the MSCT service provider or a different entity (e.g., an acquirer), operating under this MSCT service provider.

1.12. Payer: An individual, a business or merchant who holds a payment account and allows a payment instruction to be processed against that account i.e. the party responsible for the payment of funds.

1.13. Token Service Provider (TSP): Is a TTP (Trusted Third Party) that provides Tokenisation Services which provides surrogate values for the sensitive information related to the identification data of the payer or payee and transaction data such as transaction amount or transaction identifier. The TSP manages the generation and issuance of tokens, maintains the mapping of tokens to the related data. The TSP also provides token processing capabilities which include tokenising of sensitive date and detokenizing of tokens to obtain the related transaction data. The role of TSP can be covered by the MCT Service Provider but could be different.

2. Some of the above-mentioned actors are played by the same entities making the number of stakeholders involved in the payment flow smaller.
3. In particular, the Consumer ASPSP will also be the Consumer MCT service provider and, in case of Consumer presented QR code also the Payload Issuer and Token Service Provider. This actor will be called the Payer Participant.
4. The Business ASPSP will also be the Business MCT service provider and, in case of Business presented QR code also the Payload Issuer and Token Service Provider. This actor will be called the Payee Participant.
5. Figure 2 and 3 of the Annex 2 ”Diagram and payment flow” shows the simplified conceptual diagram for Kosova QR Code Ecosystem Stakeholders/Actors for Business and Consumer.

Article 13
QR Code Security Requirements

1. This section deals with the security considerations related to the QR Code specifically (i.e. security between the Payer and Payee), security aspects related to other proximity technologies for the exchange of messages between the Customers, ASPSPs, MCT Service Providers, TSPs etc., are not covered and must be specified by the associated scheme.
2. A QR code may contain both sensitive and non-sensitive data that can be used by different entities involved in the processing of the MCT transactions. Non-sensitive data includes application information such as, payer/payee name, download URL, etc. – this kind of data can remain in clear. Sensitive data includes IBANs1, a customer identifier of the Payer (e.g. the CustomerID might be the Payer’s credentials to access to the online banking system).

3. Interception of or tampering with sensitive data could lead to fraudulent transactions or data leakage and as such security measures must be implemented to protect the sensitive data and the integrity of the data elements within the QR code e.g. sensitive data should not be included in the QR code in clear-text and techniques must be used to ensure the integrity of the data elements within the QR code.
4. In this QR code standard sensitive data is protected through the use of Tokens and Proxies and the integrity of the data is protected through the inclusion of an Integrity Check field in the domestic implementation.
5. For both modes, appropriate security measures should be applied by the entity/application creating the QR code and include the following additional measures:
   5.1. The MCT application must not allow the use of the screenshot function when displaying the QR Code or notify the server side to invalidate the displayed QR code when detecting a screenshot attack.
   5.2. The Payer/Payee device must be able to recognise illegitimate codes and reject them or display a warning message.

Article 14
Annexes

1. Two annexes are integral part of this Instruction:
   1.1. Annex 1 - EPC QR Code Specification for payments
   1.2. Annex 2 - Diagrams and payment flow
2. Examples in Annex 1 are included only for understanding better the use of the QR code standards but are not part of the standard. The detailed description on how the QR code is used for various use cases will be defined in the related QR code scheme rules

Article 15
Entry into Force

This instruction shall enter into force on 1 October 2024, while by 1 June 2025 full adaptation to the requirements of this instruction must be achieved.

Annex 1

1. EPC QR CODE SPECIFICATION FOR PAYMENTS

The EPC QR Code Standard was developed to support QR codes for the account based SEPA (Instant) Credit Transfers but the focus has now expanded to ensuring interoperability of mobile initiated credit transfers across the SEPA and the larger European continent. The EPC QR code standard, "Standardisation of QR codes for Mobile Initiated SEPA (Instant) Credit Transfers [**Error! Reference source not found.**]", was developed by the Multi-stakeholder Group on Mobile Initiated SEPA (instant) Credit Transfers (MSG MCT). In the development of the standard the MSG MCT leveraged the previous version of the "Standardisation and governance of QR codes for IPS at POI [**Error! Reference source not found.**]"and the "MCT Payments and Interoperability Guidance **Error! Reference source not found.**".

The EPC QR Code Standard is used as the standard upon which the QR Code specification for Kosovo is developed and adapted to suite domestic requirements.

1.1. QR Code Notational Conventions

The abbreviations listed in Table 2: Abbreviations, are used throughout this specification.

Table 2: Abbreviations

Abbreviation	Description
An	Alphanumeric
Ans	Alphanumeric Special
b	These data objects consist of either unsigned binary numbers or bit combinations that are defined elsewhere in this specification
C	Conditional
ISO	International Standards Organization
M	Mandatory
N / n	Numeric
O	Optional
QR Code	Quick Response Code
RFU	Reserved for Future Use
S	String
Var	Variable

The data objects will always be one of the formats listed in Table 3: Data object formats.

Table 3: Data object formats

Format	Description
Numeric (N/n)	Values that can be all digits, from "0" to "9".
Alphanumeric (an)	Alphanumeric: contain a single character per byte. The permitted characters are alphabetic (a to z and A to Z, upper and lower case) and numeric (0 to 9)
Alphanumeric Special (ans)	Values that can be represented by the Common Character Set. The Alphanumeric Special alphabet includes ninety-six (96) characters in total and includes the numeric alphabet and punctuation
b	These data objects consist of either unsigned binary numbers or bit combinations that are defined elsewhere in this specification
cn	Compressed numeric data objects consist of two numeric digits (having values in the range Hex '0'–'9') per byte. These data objects are left justified and padded with trailing hexadecimal 'F's
String (S)	Values represented by any precomposed character(s) defined in [**Error! Reference source not found.**].

1.2. QR Code Conventions or Rules

The encoding of the different data fields in the QR code must be standardised as defined in the sections below.

Note that the Payload must comply with the standards defined in this document and include the minimum data (i.e. all mandatory fields) as described in this section (optional fields are at the discretion of the Payload issuer). Additionally, the parameters have to be structured so that the URL in its entirety is a valid URL according to the URL specification (https://www.w3.org/Addressing/URL/url-spec.txt).

1.2.1. QR Code Traceability

The QR Code can be uniquely identified using the remittance reference for proxy and clear methods and using a token itself for the token method. The MCT Service Provider that generates the Transaction must link the Transaction with the remittance reference or token to guarantee the full traceability of the end-to-end transaction starting from the point of initiation.

1.2.2. QR Code Encoding

For conversion of a character to its binary representation, this specification uses UTF-8 encoding as defined by Unicode[2]. A character in UTF-8 can be up to 4 bytes depending on the language.

In UTF-8 the first 128 characters are encoded using 1 byte (the ASCII characters) and the extended UTF-8 character set (i.e. the following 1920 characters are encoded using 2 bytes) and supports Cyrillic characters (i.e. Cyrillic characters use 2 bytes).

1.2.3. Encoded character sets:

For the purposes of this QR Code Standard most data elements will use the standard UTF-8 character set and some data elements, such as names of people and places, will use the UTF-8 extended character set to

[2] https://home.unicode.org/

support the Cyrillic characters. Data elements that use the UTF-8 extended character set will be marked as such.

1.2.3.1 QR Code dimension and correction level

Generally, less dense QR Codes are more easily read by scanners, whereas denser QR Codes are more difficult to read. Similarly, QR Codes with larger physical dimensions are easier to read than QR Codes of smaller physical dimensions. QR Codes should be optimized so that they do not carry irrelevant or redundant data and have sufficiently large physical dimensions to facilitate easier reading.

In order to achieve the best result, a total size not greater than 512 alphanumeric characters is recommended.

Moreover, higher error correction levels increase the QR Code's density. Lower levels of error correction result in a less dense QR Code. An error correction level of "L" is recommended.

1.3 QR Code URL Structure

The QR code data structure is URL based and is composed of five parts:

- First part of the URL: ordinary domain structure.
- Second part of the URL: version.
- Third part: type (this may refer to the payment context).
- Fourth part: An identifier of the MCT service provider is needed by the Hub for routing purposes for the exchange of messages between the respective MCT service providers.
- Fifth part: payload information.

The first four parts will be referred in the document as “the URL Header”

The URL structure of the QR code has been defined as follows:

Payee presented QR Code
/HTTPS://<Domain name>/<Version>/<Type>/<Payee MCT service provider ID>/<Payload>
Payer presented QR Code
/HTTPS://<Domain name>/<Version>/<Type>/<Payer MCT service provider ID>/<Payload>

1.3.1 QR Code Payload Methods

In the context of Payee-presented QR codes, the standard provides for the following three QR Code Payload Methods:

- The *Payee-presented data includes a “Payee token”* in which case a detokenization process must take place using the token provided in the QR code payload provided to the Payer via their MCT service provider to derive the payment details (Payee identification and transaction data). This requires interfacing with the Payee’s MCT service provider prior to the initiation of the MCT transaction.
- The *Payee-presented data includes a “proxy”* for Payee identification data in which case the data related to the proxy must be provided by the Payee’s MCT service provider upon request from the Payer’s MCT service provider prior to the initiation of the MCT transaction.

- The *Payee-presented data are all in clear-text* (i.e., the Payee's name, trade name, IBAN of the Payee's account, transaction amount, etc. are all in clear-text). The MCT transaction can be initiated immediately using the data.

Payee presented QR Code
QR Code with Token [Version]+[Type]+ [Payee MSCT Service Provider ID] + [(payee) token]
QR Code with Proxy [Version]+[Type]+ [Payee MCT Service Provider ID] + [proxy] + [a clear-text name/value string]
QR Code with clear text data [Version]+[Type]+ [Payee MCT Service Provider ID] + [a clear-text name/value string]

Important Note: The method with Proxy and clear text data is only allowed for domestic use. For cross-border use, only the token method is permitted.

Note that in the last two methods described above, appropriate security measures must be implemented to ensure the integrity and confidentiality of the data as described in section **Error! Reference source not found. Error! Reference source not found.**.

At the domestic level, the Payee MCT service provider must support all three options specified above so that the Payee can select the best option depending on the use case and the Payer's MCT service provider should be able to support all types.

In the context of Payer-presented QR codes, the standard provides for the following QR Code Payload Method:

- The *Payer-presented data includes a "Payer token"* in which case a detokenisation process must take place using the token provided in the QR code payload provided to the Payee via their MCT service provider to derive the payment details (Payer identification and transaction data). This requires interfacing with the Payer's MCT service provider prior to the initiation of the MCT transaction.

Payer presented QR Code
QR Code with Token [Version]+[Type]+ [Payer MCT Service Provider ID] + [(payer) token]

In the context of Payer-presented QR codes, options containing the CustomerIDs (CustomerIDs might be a payer's credential for access to the online banking system) in clear-text are not permitted and only the one case where the Payer identification data is a token is permitted (unless explicitly stated otherwise and the Payer's credentials are protected). But the data set can also include an additional clear text value string to support additional value-added services (e.g. loyalty programs).

1.3.2 URL Header Data Fields Definition

1.3.2.1. Domain Name

The Domain name refers to an MCT interoperability framework or scheme i.e., to the interoperability domain for MCT service providers and must refer to an "MCT interoperability framework" or "an MCT scheme or participant" operated under the MCT interoperability framework. To provide maximum flexibility and decentralised administration of local apps the Domain name should support the main domain (qr.INTFRM.org), subsequent subdomains (xy.INTFRM.org) and local URLs (qr.xy.xy).

For WB6 interoperability, a specific domain name will be defined.

For Domestic use, the domain names are defined based on specific use cases.

Table 4: Domain names

Value	Description	Domain owner	Type of QR
xxx.qrc.bqk-kos.org	Domestic Payments	CBK	All

CBK will define the allowed domain names for cross-border transactions at a later stage.

Important Note: The list of permitted Domain names is managed and authorised by CBK only.

1.3.2.2.Version

The Version refers to the specification version of the QR code and allows future updates to the QR code. It is currently:

/1/, which refers to the first version of the QR code.

1.3.2.3.Type

The Type indicates what kind of payment context is expected.

The pre-defined payment context can also determine what kind of query parameters will be allowed in the Payload e.g., because of security issues, a QR code used at the POI would not allow clear-text data.

Table 5: Type – Kind of Payment

Value	QR Code Mode	Description	EPC Standard / Kosovo Specific	Allowed Methods
Standard EPC Types				
/m/	Payee presented QR Code	mobile payment at the POI	EPC Standard	Token
/e/	Payee presented QR Code	e-commerce (and m-commerce) payment	EPC Standard	Token

Value	QR Code Mode	Description	EPC Standard / Kosovo Specific	Allowed Methods
Standard EPC Types				
/i/	Payee presented QR Code	invoice payment	EPC Standard	Proxy/Clear
/p/	Payee presented QR Code	person-to-person payment	EPC Standard	Token
/w/	Payee presented QR Code	opening a URL in a WebView (e.g. virtual POI).	EPC Standard	Token

Important Note: Additional types can be defined for domestic use cases.

1.3.2.4. MCT Service Provider Identifier

A standardised identifier needs to be assigned to every MCT service provider for routing purposes. This will require eligibility checking and registration of the MCT service provider under the FPS Scheme. CBK will be responsible for the issuance of the MCT service provider ID. The MCT service provider identifier is required for routing purposes and exchange of messages between the respective MCT service providers.

The coding of the MCT service provider ID shall be three (3) characters alphanumeric (an).

1.3.2.5. Header Data Objects

In the tables below, the Header data are listed.

Interpretation of Table

- ***Field ID:*** This is a value used to reference a field easily, but it's not used in the QR code.
- ***Data Object Name***: Is the generic name of the field
- ***Format***: format of the field as described in Table 3: Data object formats
- ***Length***: Field length
- ***Character Set:*** *Indicates the character set applicable to that data element.*
  - UTF-8 Std = standard subset of UTF-8 characters
  - UTF-8 EXT = extended set of characters that includes the Cyrillic characters.
- ***Value***: Default value when applicable
- ***Description and Rules***: Describes the field and defines the rules and conditions where applicable

FIELD ID	Data Object Name	Format	Length	Char Set	Value	Description and Rules
			"HEADER"			
H01	Domain Name	ans	var up to 70	UTF-8 Std	xxx.qrc.bqk-kos.org	• The domain name refers to the interoperability domain for MCT service providers or a Domestic QR code domain
H02	Version	n	1	UTF-8 Std	1	• Version of the QR code
H03	Type	an	1	UTF-8 Std		• Refer to section 4.3.2.3
H04	MCT Service Provider	an	3	UTF-8 Std		• Used for routing purposes (in case of use of token or Proxy)

1.3.3 Payload Data

1.3.3.1 Payload Data Structure

Data Objects in the Payload must strictly follow the sequence as defined in section 1.4.2. Payload Data Objects.

Standard URL query parameters are used to delimit the data objects within the payload: "?" as the starting parameter for the payload and "&" as the delimiter of information data within the payload. The payload fields are recognised by a two or three-letter name followed by "=" and separated by &. The fields are defined as mandatory, conditional or optional, depending on the method, type and use case. If an Optional or Conditional field is not used, its name will not be present in the payload. Please refer to **Error! Reference source not found.** for examples of payload.

EPC standards leave the definition of the payload structure to the domestic markets. For this reason, only the payload with the token method is allowed in the cross-border space.

Important Note: The list of permitted Field Names is managed and authorised by CBK only.

1.3.3.2.Payload Data Objects

The tables below list the Payload data for the three Payee-presented and single Payer-presented QR Code Payload Methods, as defined in section 1.3.1 QR Code Payload Methods. Note that the purpose of the table below is to provide a full list of the data objects.

Interpretation of Table

- ***Field Name:*** value used to identify a field inside the payload.
- ***Data Object Name***: the generic name of the field
- ***Format***: format of the field as described in Table 3: Data object formats
- ***Length***: Field length
- ***Character Set:*** *Indicates the character set applicable to that data element.*
  - UTF-8 Std = standard subset of UTF-8 characters
  - UTF-8 EXT = extended set of characters that includes the Cyrillic characters.
- ***QR Code contains***: This is divided into three methods (Token, Proxy, and Clear Data) and can have the following values:
  - M = Mandatory (red colour)
  - C = Conditional and required under certain defined conditions (orange colour)
  - O = Optional (green colour)

  If the field is not applicable is marked with a grey colour
- ***Value***: Default value when applicable
- ***Description and Rules***: Describes the field and defines the rules and conditions where applicable

Table 1: List of Data Objects for Payee Presented QR code

FIELD Name	Data Object Name	Format	Length	Char Set	QR Code contains			Value	Description and Rules
					Token	Proxy	Clear		
PAYLOAD									

Pmt=	Payload Method	an	1	UTF-8 Std		O	O		• Identifies the payload method for the QR types which allows more than one method • “1” - Clear • “2” - Proxy • “3” - Token
Pid=	QR Payload Issuer ID	an	var up to 5	UTF-8 Std	O	O	O		• Identifies the party that generated the QR code. • Not required if it's the same as the MCT Service provider

Tkn=	Token	an	var up to 300	UTF-8 Std	M				• The requirement is that it is unique and can be used to retrieve transaction data.
									• The Token typically points to:
									  • Account Holder Name
									  • Payee Trade Name
									  • IBAN/Account ID
									  • Payee Category Code
									  • Payment Instrument Type
									  • Purpose of credit transfer / Payment Type
									  • Remittance information
									  • Transaction Currency
									  • Transaction amount
									  • Any other Field according to use case

Pxt=	Proxy Type	ans	1	UTF-8 Std		M			• “1” - Mobile • “2” - National ID • “3” - Business Registration • “4” - Payment Scheme UID (RFU)

Prx=	Proxy		an	var up to 70	UTF-8 Std		M			
	One of these must be present for Proxy	Mobile Number	N	var. up to 15	UTF-8 Std					
		National ID	N	10	UTF-8 Std					
		Business Registration number	ans	9	UTF-8 Std					• Corporate/business license number
		Scheme Payment UID (Alias)	ans	RFU	UTF-8 Std					
Anm=	Account Holder Name		an	var. up to 70	UTF-8 EXT			C		
Tnm=	Payee Trade Name		an		UTF-8 EXT			O		• Mandatory for C2B and B2B
Ibn=	IBAN		an	var. up to 34	UTF-8 Std			C		• This field contains the IBAN • This field's length has been aligned to the accommodate the international standard for IBANs taking future regional and international initiatives into account • If IBAN field is present the Account ID field cannot be present • In some specific use case (such as KOS-GIRO) both IBAN and Account ID may not be present

Aid=	Account ID	an	var. up to 34	UTF-8 Std			C		• This field can be any other Account ID other than IBAN (i.e. Wallet ID, Card number). • In case the ASPSP cannot be derived from the Account ID the ASPSP ID must be present • If the Account ID field is present IBAN field cannot be present • In some specific use case (such as KOS-GIRO) both IBAN and Account ID may not be present
Asp=	Account Servicing PSP	an	3	UTF-8 Std		C	C		• Mandatory only if the Account ID doesn't contain the ASPSP ID
Pcc=	Payee Category Code (MCC)	an	4	UTF-8 Std		C	C		• Mandatory for C2B, B2B. • Referred to as the Merchant Category Code. • Must be ISO 18245 compliant.
Pit=	Payment Instrument Type	an	var. 3 to 4	UTF-8 Std		M	M	ICT/RTG/ACH	• ICT – Instant Credit Transfer • RTG – RTGS • ACH – Automated Clearing House
Ppt=	Purpose of Payment / Payment Type	an	var. up to 4	UTF-8 Std		M	M		• To identify the type of Payment Transaction and the associated use case as defined by Central Bank Scheme rules.
Rmt=	Remittance information	an	var. up to 35	UTF-8 Std		M	M		• Transaction specific information • Information supplied by the payer in the Instant Credit Instruction and transmitted to the payee in order to facilitate the payment reconciliation

Cur=	Transaction Currency	an	var. up to 3	UTF-8 Std		M	M	EUR	• Currency in which the Payer/Payee transacts depending on the use case.
Amt=	Transaction amount	N	var. up to 12	UTF-8 Std		M	M		• The Transaction Amount shall be different from zero, 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 number of digits after the decimal mark is 2 digits. • The above describes the only acceptable format for the Transaction Amount. It cannot contain any other characters (for instance, no space character or comma can be used to separate thousands). Example: EUR12.3 • (only for domestic QR Code). If the value is 0, the mobile application must prompt the consumer to enter the transaction amount.
Cty=	City	ans	var. up to 15	UTF-8 Std		O	O		• Mandatory for C2B and B2B • The Payee/Payer City is the city of the payee/payer’s physical location.

Bil=	Bill Number	ans	var. up to 25	UTF-8 Std		O	O		• The invoice number or bill number for the goods and/or services provided to the Consumer. It may be used to identify a specific transaction. • This number could be provided by the merchant (and is thus present when the QR code is generated) or could be used as an indication for the mobile application to prompt the Consumer to input a Bill Number.
Stl=	Store Label	an	var. up to 25	UTF-8 Std		O	O		• A distinctive value associated with a store. This value could be provided by the Payer or Payee or could be an indication for the mobile application to prompt the Consumer to input a Store Label.
Tid=	Terminal ID	ans	var. up to 25	UTF-8 Std		O	O		• A unique value associated to a terminal in the store. For example, the Terminal Label may be displayed to the Payer or Payee on the mobile application identifying a specific terminal or used for issue fraud resolution.
Ptn=	Payee Tax ID	ans	10	UTF-8 Std		O	O		• The tax identification number of the Payee/merchant, assigned by the governmental body of the jurisdiction.
Uid=	Utility ID	ans	var. up to 25	UTF-8 Std		O	O		• The Identification of the Utility Providers as allocated by the Central Bank

Cid=	Customer ID	ans	var. up to 25	UTF-8 Std		O	O		• The Identification number of the customer • Used for Bill Payment use cases
Qid=	QR unique sequence number	ans	8	UTF-8 Std		O	O		• Unique sequence number as assigned by the QR Payload Issuer
Dtt=	QR code Date & Time	N	var. up to 29	UTF-8 Std		O	O		• Date and time when the QR Code was generated. UTC Time format YYYY-MM-DDThh:mm:ss.sssZ or UTC with offset YYYY-MM-DDThh:mm:ss.sss+/-hh:mm • Example 2022-02-14T15:29:17.615+01:00
Adr=	Address	an	var. up to 70	UTF-8 EXT		O	O		• The address of the Payer or Payee
Pnm=	Payer Name	ans	var. up to 70	UTF-8 EXT		O	O		• The name of the Payer
Pac=	Payer Account	ans	var. up to 34	UTF-8 Std		O	O		• The Account of the Payer
Sec=	QR Security Token	ans	var. up to 64	UTF-8 Std		O	O		• Security Cryptographic Hash calculated on QR code data
Lyn=	Loyalty number	ans	var. up to 25	UTF-8 Std		O	O		• Loyalty number of the client
Prc=	Provision Code	n	2	UTF-8 Std		O	O		• Provision Code
Ord=	Invoice serial number	ans	var up to 4	UTF-8 Std		O	O		• Invoice Serial number
Cr=	Enu Code	ans	10	UTF-8 Std		O	O		• Electronic cash device – Electronic cash device, fiscal device for cash invoice issuing

Sw=	Software	ans	10	UTF-8 Std		O	O		• The software code installed on the ENU
Pdt=	Payment Due Date	ans	var. up to 20	UTF-8 Std		O	O		• Date in the format dd.mm.yyyy hh:mm:ss
Sft=	Swift Code	ans	8	UTF-8 Std		O	O		• Swift code
Cbn=	Creditor Bank Name	ans	var. up to 70	UTF-8 EXT		O	O		• Creditor Bank name
Qic=	QR Integrity Check	ans	8	UTF-8 Std		O	O		• When Present Is always the last field. • Checksum calculated over all the data object included in the QR Code • The algorithm depends from the use case".

Table 2: List of Data Objects for Payer Presented QR code

FIELD ID	Data Object Name	Format	Length	Char Set	QR Code contains	Value	Description and Rules
					Token		
PAYLOAD							

Pid=	QR Payload Issuer ID	an	3	UTF-8 Std	O		• Identifies the party that generated the QR code. • Not required if it's the same as the MCT Service provider

Tkn=	Token	an	var up to 300	UTF-8 Std	M		• The requirement is that it is unique and can be used to retrieve transaction data.
							• The Token typically points to:
							  • Account Holder Name
							  • Payee Trade Name
							  • IBAN/Account ID
							  • Payee Category Code
							  • Payment Instrument Type
							  • Purpose of credit transfer / Payment Type
							  • Remittance information
							  • Transaction Currency
							  • Transaction amount
							  • Any other Field according to use case

TBD	TBD	an	var up to 70	UTF-8 Std	O		• Clear text. Field to be defined depending of Use Case

1.3.4. Payload Examples

1.3.4.1.Examples of the composition of a QR Code for international use:

URL example for Payee Presented QR with Token:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/?Tken= Czs7sckkvBpJls4yq9n31j3jeKqNN833

URL example for Payer Presented QR with Token:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/?Tken= Czs7sckkvBpJls4yq9n31j3jeKqNN833

1.3.4.2.Examples of the composition of a QR Code for domestic use:

URL example Payee Presented QR in “Clear Text”:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/Pmt=1&Pid=123&Anm=Telkom company Pty&Tnm=Telkom&Ibn=XK0512120123456789 06&Pcc=1234&Pit=ACH&Ppt=1234&Rmt=1234567890&Cur=EUR&Amt=12.3

URL example for “Proxy”:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/?Pmt=2&Pid=123&Pxt=1&Prx=00383521003760&Pcc=1234&Pit=ACH&Ppt=1234&Rmt=1234567890&Cur=EUR&Amt=12.3

URL example for Payee Presented QR with Token:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/Pmt=3&Pid=123&Tkn=Czs7sckkvBpJls4yq9n31j3jeKqNN833

URL example for Payer Presented QR with Token:

/HTTPS://xyz.qrc.bqk-kos.org/1/i/123/?Pid=123&Tkn= Czs7sckkvBpJls4yq9n31j3jeKqNN833

Annex 2
Diagrams and payment flow

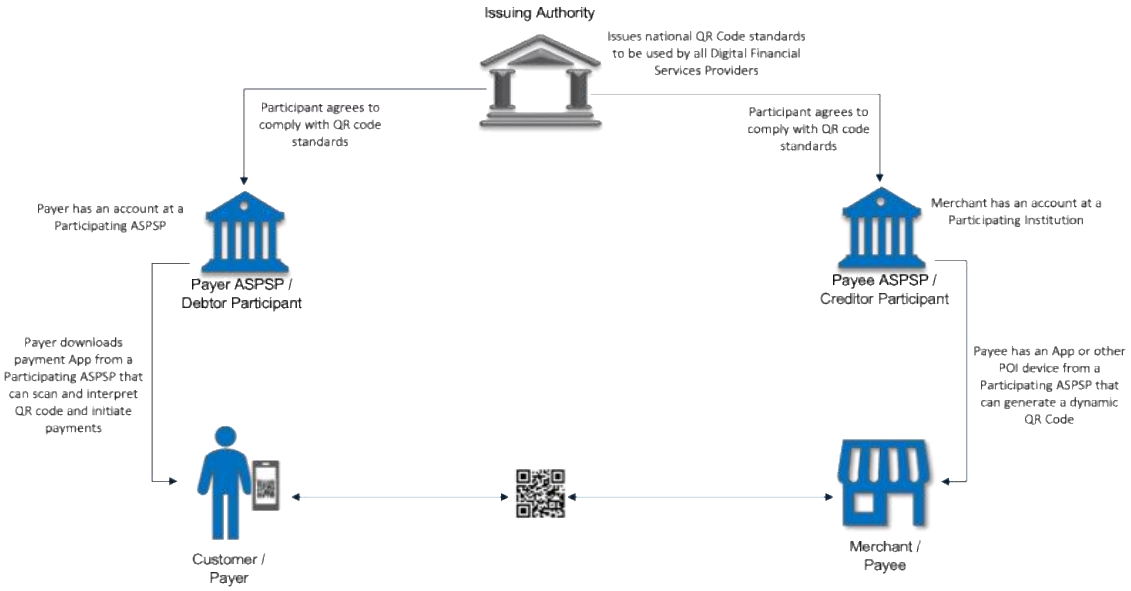

Figure 1: QR Code Standard diagram

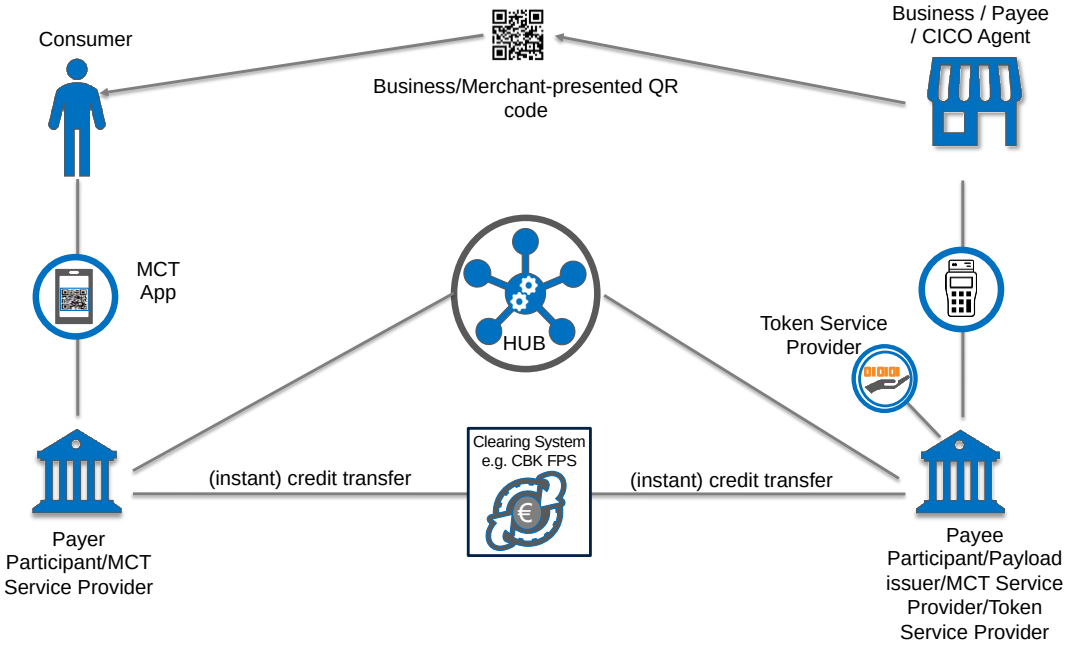

Figure 2: Kosovo QR Code Ecosystem Stakeholders/Actors for Business Presented QR code

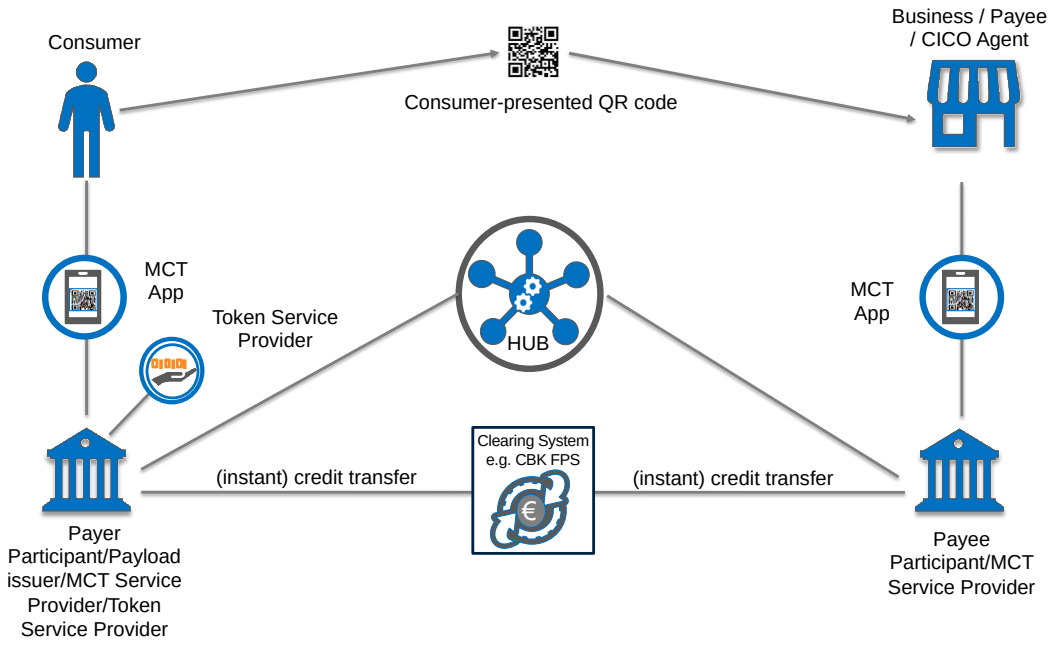

Figure 3: Kosovo QR Code Ecosystem Stakeholders/Actors for Consumer Presented QR code

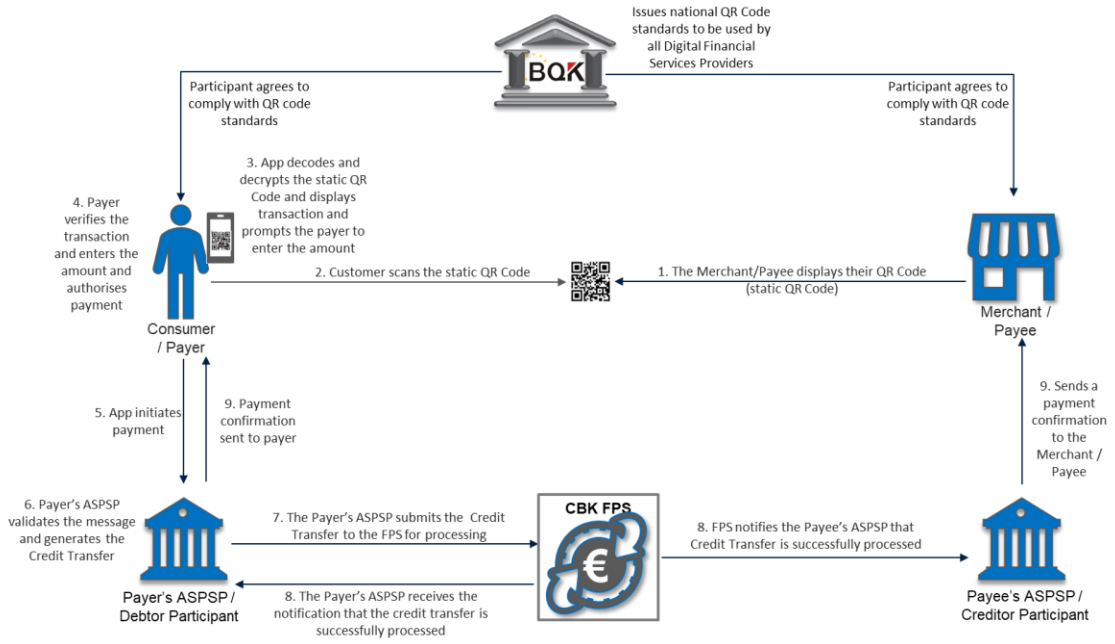

Figure 4: Payee-presented static QR code and payment flow

Step	Description
1	Merchant displays a static QR Code with merchant details which includes the Creditor Participant identification number, Merchant name and account number.
2	Consumer scans QR Code using a mobile application (App).
3	The mobile application decodes the QR code, displays the transaction including the Merchant details and prompts the Consumer to enter the transaction amount.
4	The Consumer verifies the transaction details, enters the amount and authorises the payment.
5	The mobile application initiates the payment sending the payment initiation request to the Debtor Participant.
6	The Debtor Participant validates the message, and checks that the Payer has sufficient funds and generates the credit transfer
7	The Debtor Participant submits the credit transfer to the CBK FPS for processing and clearing
8	The CBK FPS notifies the Debtor and Creditor Participant of the successful processing of the credit transfer and the Consumer and Merchant's accounts are debited and credited respectively
9	The Debtor Participant notifies the Payer that the payment has been processed successfully and the Creditor Participant notifies the Merchant that the funds have been received

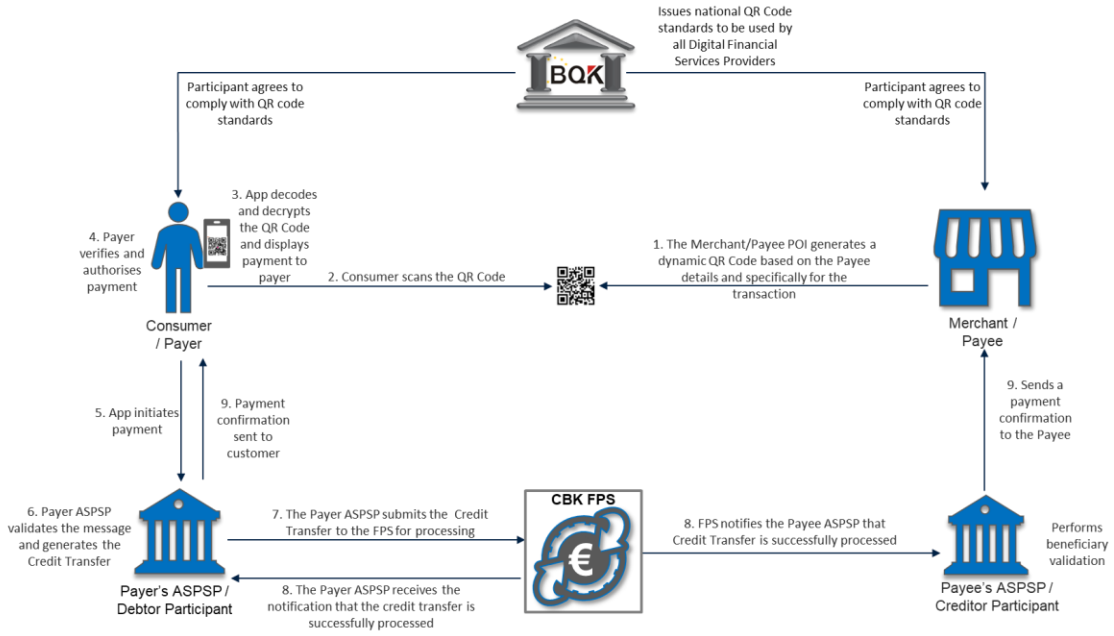

Figure 5: Payee-presented dynamic QR code and Payment Flow

Step	Description
1	Merchant generates and displays a QR Code with merchant and transaction information
2	Consumer scans QR Code using a mobile application
3	The mobile application decodes the QR code, displays the transaction including the Merchant details and transaction amount to the Consumer
4	The Consumer verifies the transaction details and authorises the payment
5	The mobile application initiates the payment sending the payment initiation request to the Consumer's Debtor Participant
6	The Debtor Participant validates the message and checks that the Payer has sufficient funds and generates the credit transfer
7	The Debtor Participant submits the credit transfer to the Kosovo FPS for processing and clearing
8	Once the credit transfer has been processed and cleared by the FPS, the Debtor and Creditor Participants are notified on the outcome of the credit transfer
9	The Debtor Participant notifies the Payer that the payment has been processed successfully and the Creditor Participant notifies the Merchant that the funds have been received