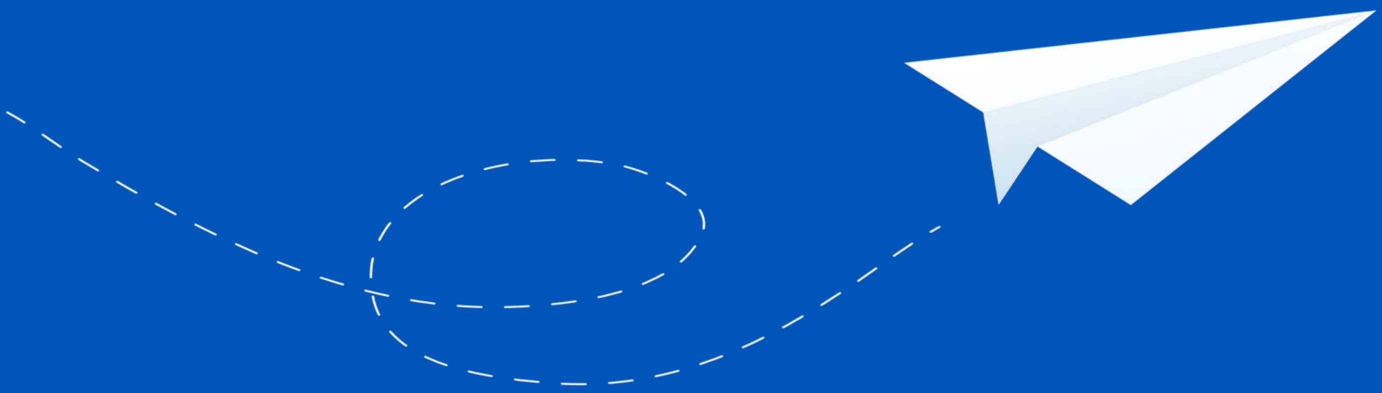
SLOVAK
BANKING
ASSOCIATION

Payment Link Standard

(Payment links and QR codes)



Version: 2.0

Bratislava, 2025-07-17

License grant

Slovak Banking association (hereinafter referred as *„SBA“*) grants to any contributor, developer, implementer, or other interested party of Payment Link Standard (hereinafter referred as *„Standard“*) non-exclusive, royalty free, worldwide copyright license to reproduce, prepare derivative works from, distribute, perform and display, this *„Standard“* solely for the purposes of developing and implementing relevant specification and applications.

Provided that attribution be made to *„SBA“* as the source of the material, but that such attribution does not indicate an endorsement by *„SBA“*.

Disclaimer of warranties and limitation of liability

Permission to use the *„Standard“* is hereby granted under the following conditions:

- that *„SBA“* nor contributors to the *„Standard“* shall have any responsibility or liability whatsoever to any other party from the use or publication of the „Standard“;
- that one cannot rely on the accuracy or finality of the *„Standard“*; and
- that the willingness of *„SBA“* to provide the *„Standard“* does not in any way convey or imply any a responsibility for any product or service developed in accordance with the *„Standard“* and *„SBA“* as well as the contributors to the *„Standard“* specifically disclaim any such responsibility to any party.

Implementation of certain elements of this *„Standard“* may require licenses under third party intellectual property rights, including without limitation, patent rights. „SBA“ and any other contributors to the *„Standard“* are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

This *„Standard“* is provided "as is", "where is" and "with all faults", and *„SBA“* does not makes any representation or warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights (whether or not third parties have been advised, have reason to know, or are otherwise in fact aware of any information), and fitness for a particular purpose (including any errors and omissions in the *„Standard“*).

To the extent permitted by applicable law, neither *„SBA“* nor any contributors to the *„Standard“* shall be liable to any user of the *„Standard“* for any damages (other than direct actual out-of-pocket damages) under any theory of law, including, without limitation, any special damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the *„Standard“*, even if advised of the possibility of such damages.

Document version and history

Version	Release date	Note/ Changes
1.0	2020-06-30	First release of the document
1.1	2020-11-18	Added versioning rules, Added a rule for manipulating the digit zero in the Amount attribute, Addded recommended characters for attributes – Messages and Creditor’s name, Added Annex A and B, Errata.
1.2	2021-04-15	Added slash (/) to the Payment Link, Emphasis on using the Payment Link primarily for sharing peer-to-peer payment instructions, Errata.
1.3.	2025-10-09	Set Creditor’s Name as a mandatory attribute.
2.0	2026-01-01	New version of Payment Link format. Added new form of Payment Link (e.g. QR payment code) Added new chapters: - 4.2 (QR payment code) and - 5 (Implementation guidelines)

Versioning of this document

A normal version number of this document have to take the form X.Y where X represents a Major version and Y a Minor version of this document. Elements X and Y are non-negative integers. Each element have to increase numerically.

Once a versioned document has been released, the contents of that version may not be modified. Any modifications have to be released as a new version.

Version 1.0 defines a final document. The way in which the version number is incremented after this release is dependent on its changes.

Major version have to be incremented if the document has encountered significant and incompatibile changes of specification. The Payment Link specification only contains the Major version number (see chapter 3.3.1 **Error! Reference source not found.**).

Minor version is incremented if new information is introduced to the document or if information is removed from the document (e.g. errata, errors in specifications whithout affecting the comapatibility of the use of Major version).

Notational conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC2119.

Table of content

Foreword

The Slovak Banking Association (hereinafter referred as „*SBA*“) is a key association in Slovakia's financial sector and the sole organisation representing banks' interests in the Slovak republic. One of the association's activity is the development and promotion of common technical standards in the Slovakia's financial sector.

The work of preparing common technical standards is normally carried out through the special working groups. Each association's member has the right to participate on the activities of special working group. In general *SBA*'s standards are voluntary for its members. Participation in the development of the association's technical standards does not imply an obligation of association's members to implement them.

Common technical standards developed by *SBA* are usually opened and free to use. After the approval, each common technical standard is published on the association's websites (e. g. www.sbaonline.sk).

1 Introduction

Payment Link is a simple and flexible way how to instantly request money from another bank client without extensive and expensive implementation on the bank side. The Payment Link is primarily intended for sharing payment instructions in the mobile messaging applications. It can by also used for creating the QR payment code.

The Payment Link concept can be easily described in three steps. In the first step, any payee can create the Payment Link, e.g. in the bank mobile app. Then the Payment Link is distributed to the payer via mobile messaging or email applications, without any connection to the back-end banking interfaces. In the next step, a payment order is generated from the Payment Link in the preferred bank mobile app and it is processed in a standard way with payer’s authorization.

Banks can create a concept similar to Payment Link individually, but the involvement of most banks will bring more benefits to clients. This document has been created to describe a common technical standard for the implementation of Payment Link.

1.1 Document purpose

Payment Link Standard (hereinafter referred as *„Standard“)* provides the information how to implement the Payment Link for any developer, implementer, or other interested party.

The *„Standard“* specifically explains:

- how to use the Payment Link,
- the Payment Link technical specification and recomendations,
- the Payment Link implementation guidelines
- the potential risks arising from the use of the Payment Link and how to mitigate them.

1.2 Terms and definition

For the purposes of this document, the following terms and definition aply.

Term	Meaning
Deep linking	in our case Payment Link leads directly to unsigned payment details in mobile banking application.
ISO 20022	an universal financial industry message scheme.
Open Graph Protocol	a protocol enables any web page to become a rich object in a messaging application.
PAY by square	an QR payment code specification used by banks in Slovakia.
Payee	a person who money is paid to or should be paid to, in our case person who generates and send a Payment Link
Payer	a person who pays, in our case person who clicks on Payment Link, checks the payment details and authorize the payment
Payment Link	a way how to instantly request money from another bank client without implementation on the bank side. Payment Link is not a payment means or payment instruments.
Payment Link Domain	the second level domain name of the Payment Link Website.
Payment Link Standard	a document which describes the implementation of the Payment Link.
Payment Link Website	a common website owned by SBA, which is essential for the functioning of the Payment Link.
Peer-to-peer payment instruction	a payment instruction shared between the Payee and the Payer in the mobile messaging applications.
POI	Point of Interaction is a specific location where a transaction occurs between a customer and a merchant. (e.g.the location where a dynamically generated QR code is presented to the customer, typically on the screen of a cash machine or self-service terminal, enabling the customer to initiate a payment or authentication process using their mobile device).
QR code	Quick Response code is a type of two-dimensional barcode that can store a variety of information, such as URLs, contact details, or text.
SBA	Slovak Banking Association; a key association in Slovakia’s financial sector and the sole organisation representing banks’ interests in Slovakia.
SEPA	Single European Paymnet Area; a payment-integration initiative of the European Union for simplification of bank transfers denominated in euro.
URL	Uniform Resource Locator; a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

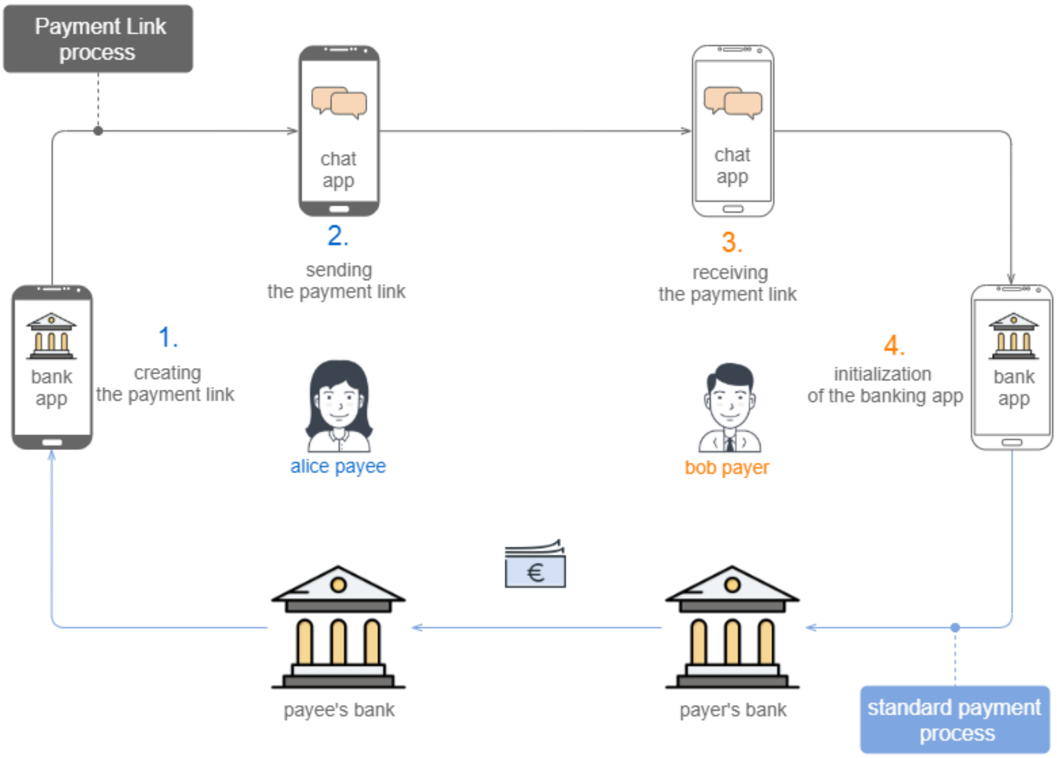
2 How the Payment Link works

The Payment Link is a simple and flexible way how to a payee instantly request money from a payer. It is essentially a URL with encoded payment instruction. Payment instructions through clients can be exchanged betweeen payee and payer in various ways such as:

1. As a standalone payment link or a payment button via email, SMS, messaging application or social media,
2. As a QR payment code (see chapter 4.2 QR Payment Code),
3. Mobile proximity payments (e.g. NFC)[1].

2.1 Usecase 1: Send the payment link viac chat app

This usecase describes sending the Payment Link in the mobile environment, via the messaging applications. The Payment Link Process in this scenario consists of four steps: (1) creating the Payment Link, (2) sending Payment Link, (3) receiving the Payment Link and (4) open the bank application by clicing on link.



Creating the Payment Link

The Payment Link can be created by the Payee in the existing bank applications.

Sending and receiving the Payment Link

In the next steps, the Payee sends the Payment Link to the Payer via the preffered mobile messaging application. Some messaging applications support Open Graph Protocol, therefore the common Payment Link Website will provide basic tags from Open Graph Protocol for a better user experience. Users can share not only the url link, but also the enhanced visualization form of the Payment Link.

Initialization of the banking application

[1] This document currently does not describe the use of this technology in relation to the payment link.

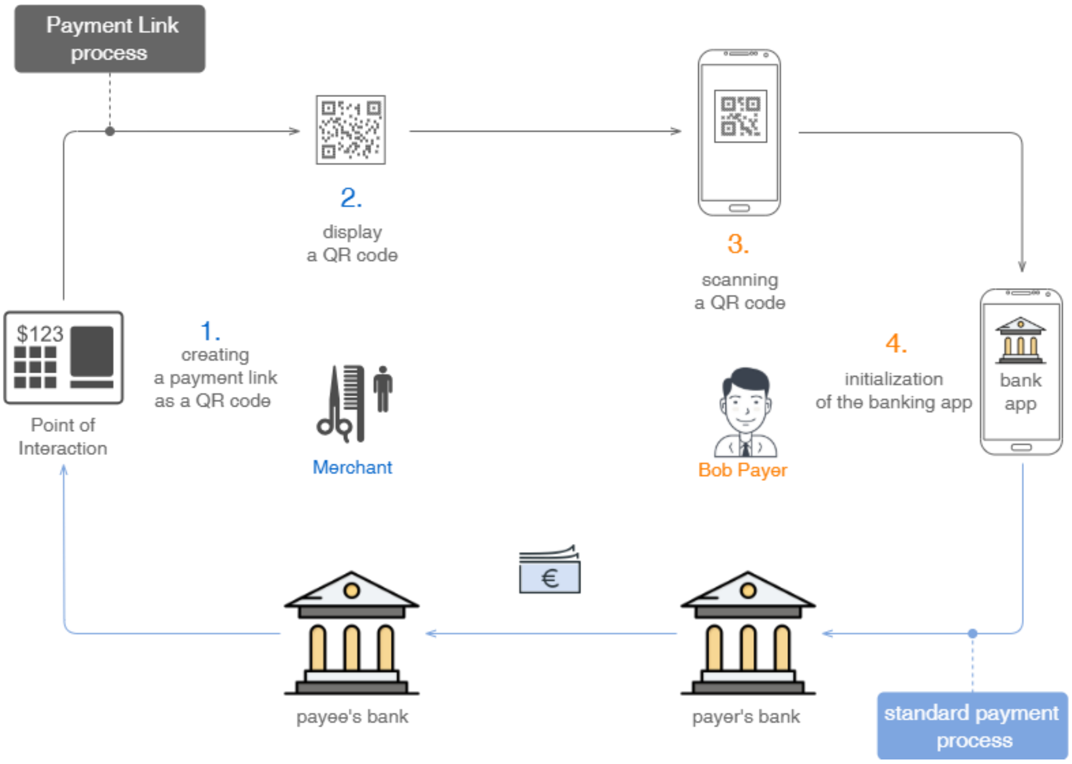
After the clicking on the message with Payment Link, the Payer (thanks the Deep linking) will be automaticly redirected to his bank app, where he will proccess the payment order.

If the Payer has more than one banking app installed on his mobile device, clicking on the message with Payment Link will open a modal window with installed bank apps. Then he will choose preferred app. The Payer can also choose to use the preferred app only once or permanently.

In the next steps, the payment order will be processed in the bank application in the standard way with Payer's authorization.

2.2 Usecase 2: Payment link encoded in a QR code

This usecase describes the payment data excahnage via QR code (e.g. at the Point of Interaction). The Payment Link Process in this scenario consists also of four steps: (1) creating the Payment Link and encoded it into the QR code, (2) then sending or displaying it to the payer, (3) scanning the QR code with Payment Link and (4) Initializating the bank application.



Creating the Payment Link and encoded it into the QR code

The Payment Link is creating by the Merchant and simply encoding it into the QR payment code.

Displaying the QR code at the POI

The QR payment code is displayed to or sent to the Payer (e.g., shown on a screen at the Point of Interaction).

Scanning the QR code

The Payer scans the QR code using their mobile device.

Initialization of the banking application

After the scanning QR code, the Payer will be automaticly redirected to his bank app, where he will proccess the payment order.

If the Payer has more than one banking app installed on his mobile device, Payment Link will open a modal window with installed bank apps. Then he will choose preferred app.

In the next steps, the payment order will be processed in the bank application in the standard way with Payer’s authorization.

3 Payment Link specification

3.1 Principles

The definition of a Payment Link Standard is based on the following principles:

- Payment Link is open standard,
- creating and sending a Payment Link is available to everyone and is not dependent on the banking infrastructure,
- using of the Payment Link for payment is always processed in the Bank's applications on a standard way with authorization,
- the format should be expandable with the possibility of further development within the EU,
- the Internet domain that will be part of the service will be owned by the Slovak banking association
- the „Standard“ supports only SEPA payments (SEPA Credit transfer[2] and SEPA Instant Credit Transfer[3]),
- Payment Link Standard is based on EPC document: Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers[4].

3.2 Format definition

Basic premises of Payment Link Standard:

- It supports only one payment order per Payment Link,
- It uses readable encoding of payment parameters in URL,
- It uses standard URL query string,
- naming convention of the attributes is aligned with the ISO 20022,
- codename names are chosen as short as possible,
- payment formats are in accordance with ISO 20022.

3.2.1 Payment Link syntax

Payment Link consists of a hierarchical sequence of four components:

- scheme,
- authority,
- path,
- query.

```
URI = [scheme]:[//authority][path][?query]
```

[2] SEPA Credit Transfer (SCT)
[3] SEPA Instant Credit Transfer (SCT-Inst)
[4] EPC024-22, version 2.10, from 17 June 2024

Scheme:

- Selected URI scheme for Payment Link Standard is HyperText Transfer Protocol Secure (HTTPS). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, its predecessor, Secure Sockets Layer (SSL).
- Scheme component is followed by a colon (:).

Authority:

- An authority component preceded by two slashes (//).
- Only Host component of Authority is supported.
- The first and second level domain name of the Payment Link Web is represented the following way{PaymentLinkDomain}.

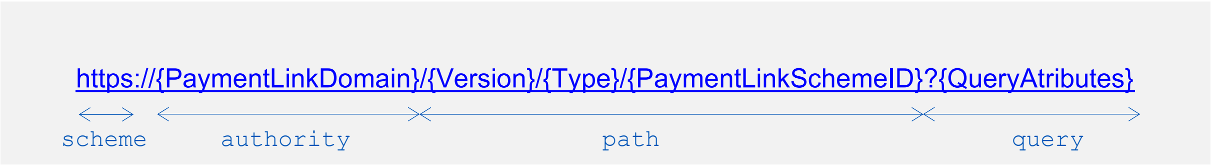
Path:

- A path component, consisting of a sequence of path segments separated by a slash (/).
- Based on implementation experience it is recommend to not end path component with a slash (/).
- The Payment Link Path component consist of three mandatory parts; Version, Type and Payment Link Scheme ID[5] (see chapter 3.3 Path specification).

Query:

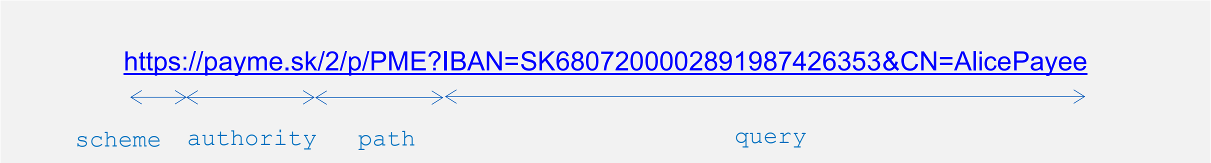
- An query component preceded by a question mark (?), containing a query string of non-hierarchical data. By convention it is a sequence of attribute and =value pairs separated by a delimiter. The commonly used delimiter is an ampersand (&).
- Query component component consists of payment instruction atributes. Payment Link Standard attributes are describe in chapter 3.4 Attributes specification.

Example:



https://{PaymentLinkDomain}/{Version}/{Type}/{PaymentLinkSchemeID}?{QueryAtributes}

Example of payme.sk implementation:

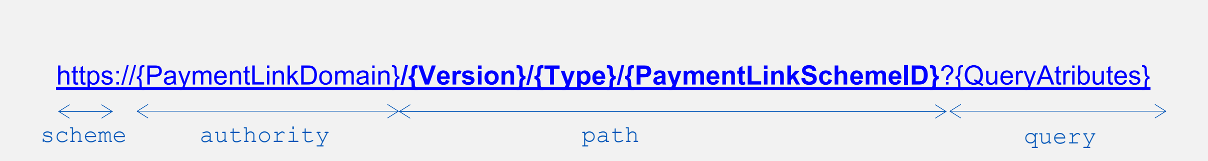


https://payme.sk/2/p/PME?IBAN=SK6807200002891987426353&CN=AlicePayee

[5] In EPC document (EPC 024-22), it is defined as a „Payer MSCT service provider ID“

3.3 Path specification

This section describes three mandatory segments of the Payment Link Path.



https://{PaymentLinkDomain}/**{Version}/{Type}/{PaymentLinkSchemeID}**?{QueryAtributes}

3.3.1 Version

Version of the *„Standard“* is a sequence based versioning and includes only major versions. This sequence is increased when data model of the Payment Link Standard schema is modified to the *„Standard“*. We don't expect more than nine versions of the *„Standard“*, therefore only one character has been reserved for this attribute. Current version of the *„Standard“* is “2”.

3.3.2 Type

The type indicates what kind of payment context is expected. The pre-defined payment context could also determine what kind of query parameters will be allowed or mandatory in the payload. In this version the following coding is supported:

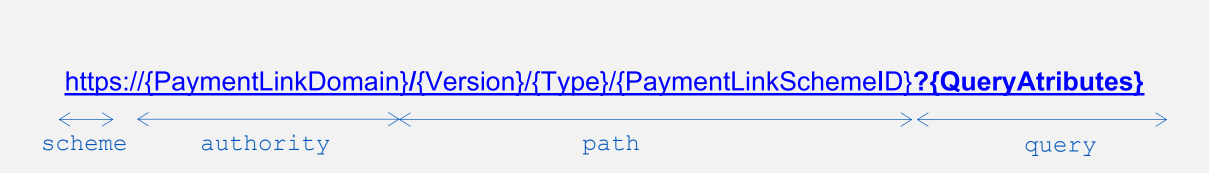
- /m/ for mobile payment at the point of interaction (e.g. via QR code),
- /e/ for e-commerce,
- /q/ for the specific purpose of using a QR code at the point of interaction, when the mandatory parameters (IBAN and Creditor’s Name) are known,
- /p/ person-to-person payment.

In future versions, other type value may be defined.

3.3.3 Payment Link Scheme ID

According to the EPC document, this segment is referred to as the MSCT service provider ID and can be used for routing purposes. In our case, the segment is designated as 'PME' to identify the payme.sk implementation of the Payment Link Standard.

3.4 Attributes specification in Query component


https://{PaymentLinkDomain}/{Version}/{Type}/{PaymentLinkSchemeID}**?{QueryAtributes}**

Payment Link Standard supports attributes listed in following table.

Table 1: List of supported attributes:

Name	Encoded name	Type (max. length*)	Condition	Description
IBAN	IBAN	String (34)	**Mandatory**	International Bank Account Number
Amount	AM	String (9)	*Defined by Type Path component*	Amount of transaction in selected currency. Amount is represented by float number with two digits precesion. The decimal separator is a dot.
Currency code	CC	String (3)	*Defined by Type Path component*	Currency in ISO 4217 Alpha 3 currency code. In version 2 is only “EUR” valid currency code.
Due date	DT	ISODate	*Defined by Type Path component*	Due date in ISO 8601 format YYYYMMDD.
Payment identification	PI	String (35)	*Defined by Type Path component*	Payment identification used as EndToEndId reference.
Message	MSG	String (140)	*Defined by Type Path component*	Message for receipient.
Creditor’s name	CN	String (70)	**Mandatory**	Beneficiary name of the payment receipient.

* max length is defined for data without URL encoding.

Whether the attributes are mandatory or optional depends on the chosen Type Path component (e.g. /m/, /e/, /p/, /q/). Attributes IBAN and Creditor’s name are mandatory in all types. In the following table, the optionality of the parameter is defined according to the type of payment:

Table 2: Condition of Attributes byType and Payment Link scheme Path component:

Type Attributes	/m/	/e/	/q/	/p/
IBAN	Mandatory	Mandatory	Mandatory	Mandatory
Amount	Mandatory	Mandatory	Optional	Optional
Currency code	Mandatory	Mandatory	Optional	Optional
Due date	Omit	Omit	Omit	Optional
Payment identification	Mandatory	Mandatory	Optional	Optional
Message	Optional	Optional	Optional	Optional
Creditor’s name	Mandatory	Mandatory	Mandatory	Mandatory

3.4.1 IBAN

International Bank Account Number (IBAN) is identifier used internationally by financial institutions to uniquely identify the account of a customer. *„Standard“* supports identification of bank account only via IBAN. This attribute is up to 34 characters long string. ISO 20022 defines following pattern for IBAN validation "[A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}".

Name	Abbreviation	Example	Encoded example
IBAN	IBAN	SK68 0720 0002 8919 8742 6353	IBAN=SK6807200002891987426353

3.4.2 Amount

The attribute defines the amount of requested payment in selected currency. Second version of the *„Standard“* supports only Euro currency.

Note:

The „Standard“ does not define a maximum transaction amount, amount is limited only by length of the field (e.g. 9999999 or 999999.99).

Name	Abbreviation	Example	Encoded examaple
Amount	AM	200,30	AM=200.30

3.4.3 Currency code

The attribute defines the currency of requested payment. Second version of the *„Standard“* supports only Euro currency. This attributes use 3 letters payment currency code according ISO 4217.

Name	Abbreviation	Example	Encoded examaple
Currency code	CC	EURO	CC=EUR

3.4.4 Due date

The attribute represents the recommended due date for the requested payment. This attribute is optional and it should be fill only for payment with a future due date. Default value of the Due Date parameter is current bank date.

Implementation recommendations:

If the due date is in the future, the bank should make a payment with a future due date. Processing bank should take into account its own restrictions on the future maturity date (e.g. maximum maturity).

If the message does not contain the due date of payment, the bank should automatically create unsigned payment with the current due date.

If the due date is in the past, the bank should make a payment with the current date as a due date. The bank should decide how to notify the client about the change in due date.

The due date parameter is omitted if the Type Path component has the value /m/, /q/ or /e/.

Name	Abbreviation	Example	Encoded example
Due date	DT	30 April 2025	DT=20250430

3.4.5 Payment identification

The attribute supports unique identification assigned by the initiating party to unambiguously identify the payment transaction. This identification is passed on, unchanged, throughout the entire end-to-end payment chain. In ISO 20022 complexType “PaymentIdentification” and element “EndToEndId” is used to transport this element attribute. Attribute is up to 35 characters long string. This attribute could be mandatory or optional. Condition of this parameter depends on Type Path components (see chapter 5.2)

Note:

In the Slovak Republic up to three payment symbols are used[6]*:*

- *Variable symbol carries payment reference information used for matching the payment to contract or payer. Used coding “/VS” followed by up to 10 digits,*
- *Specific symbol is used by some institutions for further classification of incoming payments. Used coding “/SS” followed by up to 10 digits,*
- *Constant symbol carries payment purpose information. Used for payment classification mostly by Public Sector institutions. Used coding “/KS” followed by 4 digits.*

This field used following format “/VS{0,10}*/SS*{0,10}*/KS*{0,4}*”.*

Implementation recommendations:

It is recommended to use the only characters listed in Annex A. The content of parameter Payment Identifictaion must not start or end with a ‘/’ (single slash) nor should it contain ‘//’ (double slashes).

Name	Abbreviation	Example	Encoded example
Payment identification	PI	/VS2546874464 /SS2019568456 /KS1118	PI=%2FVS2546874464 %2FSS2019568456 %2FKS1118
Payment identification	PI	QR-ab29e346f1d841c8a95a63d857490818	PI=QR-ab29e346f1d841c8a95a63d857490818

3.4.6 Message

Message is additional payment information that the bank delivers to the payee. This attributes is up to 140 characters long string and it is transferred in “Remittance information” element according ISO 20022.

Note:

It is required to ensure that Message entered by client will be encoded to HTML URL. URL encoding converts characters into a format that can be transmitted over the Internet. For example: URLs cannot contain spaces. URL encoding normally replaces a space with a plus (+) sign or with %20. More information about URL encoding find on web: https://www.w3schools.com/tags/ref_urlencode.asp

[6] Additional Optional Service applied in Slovakia to SEPA Credit Transfer

This “Standard” supports space encoding into both “+” and “%20”, banking application should enshure correct decoding of both alternatives. For readability purposes bank applicaton should uses encoding spaces into “+”.

Implementation recommendations:

It is recommended to use the characters listed in Annex A.

Name	Abbreviation	Example	Encoded example
Message	MSG	Thank you for lunch.	MSG=Thank+you+for+lunch.
Message	MSG	Thank you for lunch.	MSG=Thank%20you%20for%20lunch.
Message	MSG	Cafe on the corner, Zilina	MSG=Café+on+the+corner,+Zilina
Message	MSG	Cafe on the corner, Zilina	MSG=Cafe%20on%20the%20corner,%20Zilina

3.4.7 Creditor’s name

The attribute represents the name (first name and surname in the case of individuals, or company name in the case of legal entities) of the party whose account will be credited with the payment. This is a mandatory attribute, limited to a string of up to 70 characters. It is recommended to use normalization rules, including the replacement of national Slovak characters with their standardized ASCII equivalents[7].

Note:

It is required to ensure that this parameter entered by client will be encoded to HTML URL. URL encoding converts characters into a format that can be transmitted over the Internet. For example: URLs cannot contain spaces. URL encoding normally replaces a space with a plus (+) sign or with %20. More information about URL encoding find on web: https://www.w3schools.com/tags/ref_urlencode.asp

This “Standard” supports space encoding into both “+” and “%20”, banking application should enshure correct decoding of both alternatives. For readability purposes bank applicaton should uses encoding spaces into “+”.

Implementation recommendations:

It is recommended to use the characters listed in Annex A.

Name	Abbreviation	Example	Encoded example
Creditor’s name	CN	Alice Payee	CN=Alice+Payee
Creditor’s name	CN	Alice Payee	CN=Alice%20Payee
Creditor’s name	CN	The Best Cafes sro	CN=The+Best+Cafes+sro
Creditor’s name	CN	The Best Cafes sro	CN=The%20Best%20Cafes%20sro

[7] The reason is better readability of the Paymnet Link and a simpler QR payment code.

4 Forms of Pamyent Link

In this section, we describe the ways in which a payment link can be presented or displayed for clients.

4.1 Standalone Paymennt Link

The Payment Link is essentially a URL with an encoded payment instruction. It can be used as a standalone payment link or as a payment button. The payment instruction can thus be sent via email, SMS, messaging app, or social media. Thanks to deep link technology, the payment link in the bank's mobile app can be transformed into a payment order. To ensure the proper functioning of the payment link, the existence of a domain and a website is necessary.

The website (Paymnet Link Website) is needed to provide the Open Graph tags for the better visualization and to convert the Link to the QR payment code. The domain (Payment Link Domain) is needed to define Payment Link syntax and to provide deep linking for automatic redirection to the preferred mobile banking application.

4.1.1 Examples of standalone Payment Link

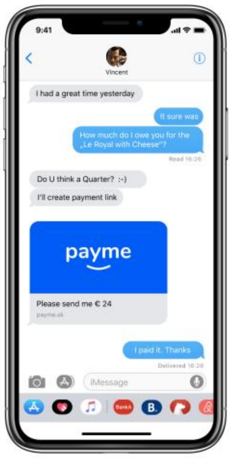
The following examples demonstrate the generation of the Payment Link in the case of payme.sk implementation:

Examples for person-to-person payments:

```
https://payme.sk/2/p/PME?IBAN=SK6807200002891987426353&AM=8.
59&CC=EUR&DT=20280430&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

```
https://payme.sk/2/p/PME?IBAN=SK6807200002891987426353&CN=Al
ice+Payee&AM=8.59&CC=EUR
```

Figure 1: Use of payment link in mobile chat applicatpns



I had a great time yesterday

It sure was

How much do I owe you for the „Le Royal with Cheese"?

Read 16:26

Do U think a Quarter? :-)

I'll create payment link

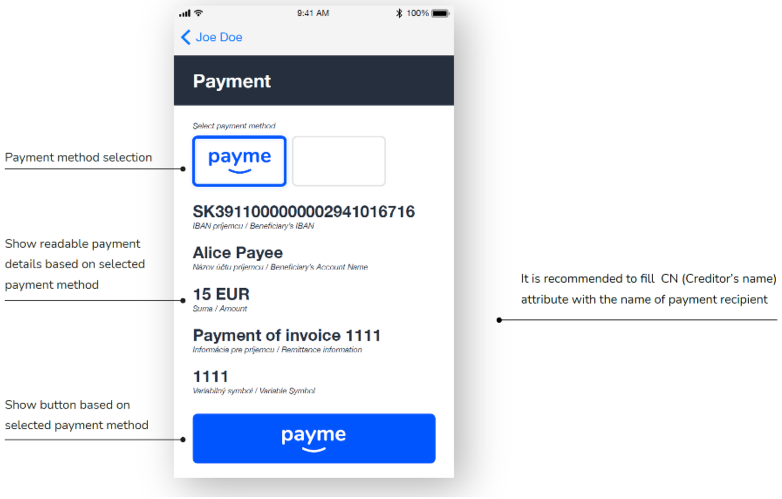
Please send me € 24

payme.sk

I paid it. Thanks

Delivered 16:28

Figure 2: Use of payment link button


9:41 AM
100%
Joe Doe
Payment
Select payment method
payme
SK3911000000002941016716
IBAN príjemcu / Beneficiary's IBAN
Alice Payee
Názov účtu príjemcu / Beneficiary's Account Name
15 EUR
Suma / Amount
Payment of invoice 1111
Informácie pre príjemcu / Remittance information
1111
Variabilný symbol / Variable Symbol
payme

Payment method selection

Show readable payment details based on selected payment method

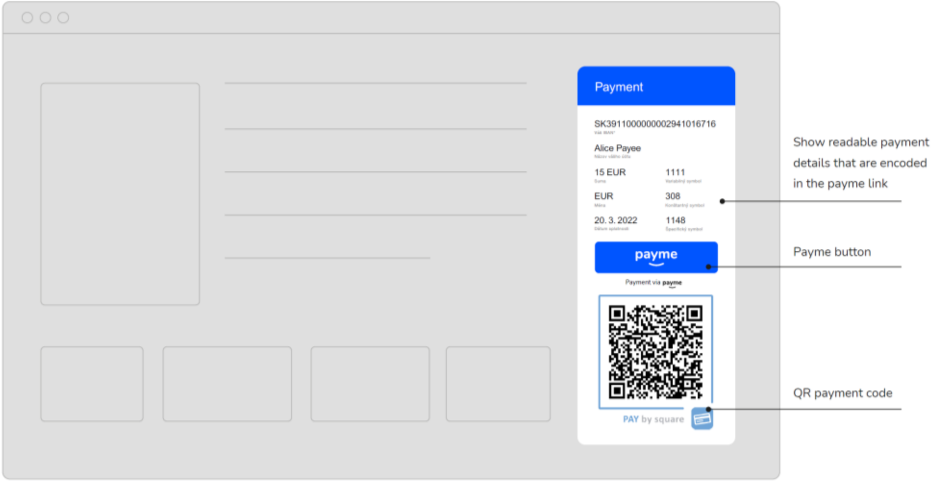
Show button based on selected payment method

It is recommended to fill CN (Creditor's name) attribute with the name of payment recipient

Example for e-commerce payments:

```
https://payme.sk/2/e/PME?IBAN=SK6807200002891987426353&AM=20
0.30&CC=EUR&PI=%2FVS2546874464%2FSS2019568456%2FKS1118&CN=Th
e+Best+e-shops+ltd&MSG=my+e-shop,+Kosice
```

Figure 3: Use of payme in e-commerce



Show readable payment details that are encoded in the payme link

Payme button

QR payment code

4.2 QR payment code

The Payment Link could be also displayed as a QR code. When this QR code is scanned using a smartphone or another device, the user is automatically redirected to the preferred banking mobile application to confirm payment order. QR payment code can be used for a variety of purposes, including invoice payments, charitable donations and also for payments at the Point of Interaction (POI).

4.2.1 Examples of QR code

The following examples demonstrate the generation of the QR code based on Payment Link in the case of payme.sk implementation:

Examples for mobile payments on the POI (e.g. QR payment code):

```
https://payme.sk/2/m/PME?IBAN=SK6807200002891987426353&AM=20
0.30&CC=EUR&PI=QR-
ab29e346f1d841c8a95a63d857490818&CN=The+Best+Cafes+ltd&MSG=C
afe+on+the+corner+Zilina
```

Payment via payme

```
https://payme.sk/2/q/PME?IBAN=SK6807200002891987426353&CN=Th
e+Best+Cafes+td&MSG=Cafe+on+the+corner+Trnava
```

Payment via payme

Example for person-to-person payments as contribution to charity:

```
https://payme.sk/2/q/PME?IBAN=SK6807200002891987426353&CN=Hope+charity
```

5 Recommendations for implementing Payment Link Standard

5.1 Recomended Characters

Recommended character set are listed in the “Standard” Anexes. For key attributes such as Payment Identification (PI), Message (MSG), and Creditor’s Name (CN), it is strongly recommended to use the character set defined in Appendix A. Characters outside the recommended set may be replaced or omitted.

It is also recommended to use normalization rules, including the replacement of national Slovak characters with their standardized ASCII equivalents.

The content of parameter Payment Identifictaion (PI) must not start or end with a ‘/’ (single slash) nor should it contain ‘//’ (double slashes).

5.2 Implementation by Type Path components

This chapter outlines the implementation of Payment Links, which is based on specific path attribute (Type Path component). It is recommended always to use the correct Type Path component, especially for ‘QR payments‘ at the POI (/q/ or /m/).

5.2.1 Type /m/

Primary use: „Dynamic[8] QR payment“ code on the POI

Payment scheme: Always use only SEPA Instant Credit Transfer (SCT Inst)

Payment order editability: Payment order is non-editable in the bank's mobile application

Mandatory attributes:

- IBAN,
- Amount,
- Currency code [EUR],
- Payment identification [ID_transaction],
- Creditor’s name.

Omitted attribute:

- Due date, [Default value is current date].

Optional attributes:

- Message [It is recommended to use this parameter to define the business name and branch location].

[8] A dynamic QR payment code is intended for large merchants. It contains all mandatory information along with the identification of a specific payment (ID Transaction). This QR code cannot be edited by the customer. The merchant verifies the receipt of the payment through a special API service (Push Payment Notification).

5.2.2 Type /e/

Primary use: e-commerce

Payment scheme: Always use only SEPA Instant Credit Transfer (SCT Inst)

Payment order editability: Payment order is non-editable in the bank's mobile application

Mandatory attributes:

- IBAN,
- Amount,
- Currency code [EUR],
- Payment identification,
- Creditor’s name.

Omitted attribute:

- Due date, [Default value is current date].

Optional attributes:

- Message [It is recommended to use this parameter to define the business name and branch location].

5.2.3 Type /q/

Primary use: “Static[9] QR payment code“ at POI. It could be also used for donations.

Payment scheme: Always use only SEPA Instant Credit Transfer (SCT Inst).

Payment order editability: Payment order is editable in the bank's mobile application.

Mandatory attributes:

- IBAN,
- Creditor’s name.

Omitted attribute:

- Due date, [Default value is current date].

Optional attributes:

- Message [It is recommended to use this parameter to define the business name and branch location],
- Amount,
- Currency code [EUR],
- Payment identifications.

[9] A static QR code is primarily intended for small merchants. It contains only mandatory information such as the IBAN and account name. After scanning with a mobile device, the customer then adds the transaction amount and confirms the payment order. The merchant verifies the received payment in their mobile banking.

5.2.4 Type /p/

Primary use: person-to-person payments.

Payment scheme: SEPA Credit Transfer (SCT) or SEPA Instant Credit Transfer (SCT Inst).

Payment order editability: Payment order is editable in the bank's mobile application.

Mandatory attributes:

- IBAN,
- Creditor’s name.

Optional attributes:

- Due date,
- Amount,
- Currency code [EUR],
- Payment identifications,
- Message.

5.3 Implementation for QR payment code

The QR payment code is generated in accordance with ISO/IEC 18004:2024.

The QR payment code utilizes an error correction level of M, which means that 15% of data can be restored if the code is damaged or partially obscured.

The QR code can be scanned using the mobile phone camera, making it accessible and convenient for users. As a backup solution, the QR code can also be scanned from the selected mobile banking application, ensuring flexibility and reliability in various situations.

A comprehensive design manual for using the QR code could be published in a separate document on the SBA websites[10].

[10] e.g. www.sbaonline.sk or payme.sk

6 Risk analysis

6.1 Phishing and fraud

General security preconditions:

- The security of the entire communication depends:
  - on the security and confidentiality of transmission channel used (e.g. messengers, emails, cash machine or self-service terminal),
  - on mechanism of What You See Is What You Sign (WYSIWYS) ensures the semantic content of signed messages is verified by client. Observe before used principle relies on client verification of payment attributes before transaction authorization.
  - standard does not support redirection to internet banking by design
- If attacker is trying to modify the Payment Link URI to different domain:
  - deep linking will fail on smart devices with registered banking application,
  - redirection to fake domain can be successful, it's up to client to check the domain name, security of web protocol and to prevent of provision of bank credentials (1st and 2nd factor) on suspicious redirected pages.
- Payment link data (e.g. IBAN and amount) are susceptible to modify in case of malware infected smart device.

Implementation recommendations:

Deep link processor (eg. banking application) can mitigate this risk by prevention measures: e.g. by showing warning text for unknown, suspicious, untrusted or first time used IBANs, and by applying antimalware technics such as rooted device detection.

6.2 Data integrity

The following deficiencies were found in the analysis:

- Data transmitted in the Payment Link is not protected against modification. The integrity of the transmitted data is not guaranteed. However, since the data are not confidential to the addressee and there is a general presumption that they are known, the deficiency is not serious. In addition, the payment scheme uses exclusively the HTTPS protocol, which to a certain extent guarantees the integrity of the data on the transport layer.
- To improve data integrity in QR payment initialization, the *Verification of Payee* [11](VoP) service validates the recipient's identity based on extracted account details (account number and beneficiary name). This reduces the risk of misdirected payments caused by incorrect or tampered QR data and strengthens overall consistency and trust in the payment process.
- Data transmitted in a Payment Link does not contain a unique NONCE data to prevent MITM, Replay, Relay attacks. Use of NONCE is a standard safety policy. The NONCE task partially replaces the Payment Identification attribute, which serves as a unique transaction identifier as specified. However, this attribute is not mandatory. We recommend introducing a randomly generated NONCE attribute. The *„Standard“* is designed primarily for payment to friend scenarios, so link readability is preferred over unique identification.

[11] Verification of Payee (VoP) is a security measure used in banking to ensure that money is sent to the intended recipient. The legislative framework for Verification of Payee (VoP) primarily revolves around the EU Instant Payments Regulation (EU 2024/886).

6.3 Non-participation

The proposed implementation of the *„Standard“* will work for banks that do not implement the *„Standard“* in their mobile apps. Clients of those banks will be redirected to the central SBA domain where the Payment Link will be displayed in the another QR code (PAY by square) with all payment details in a readable form.

6.4 Service failure

The *„Standard“* is designed in a way that minimizes dependency on the central component in following way:

- definition of the „Standard“ is open and encoding provides application of the request sender,
- Payment Link is interpreted directly in the mobile banking application,
- central component is required mainly for non-participating subjects,
- only mandatory.

6.5 End-user experience

Payment Link brand, logo and visual identity are described in a separate document.

Requirements for the Payment Link Website:

- get information about Payment Link Standard (user description, supported banks, technical specification),
- vizualize clicked Payment Link in readable form,
- provide the Open Graph tags to visualize the Payment Link in mobile messaging applications,
- generate Payment Link form.

6.6 Common reporting

SBA requires reporting on the mothly amount of transactions executed over Payment link standard in order to obtain usage information.

Annexes

A. Recommended characters

Characters outside the recommended set may be replaced or omitted.

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

/	(solidus)
-	(hyphen-minus)
?	(question mark)
:	(colon)
(	(left parenthesis)
)	(right parenthesis)
.	(full stop)
,	(comma)
'	(single quotation)
+	(plus sign)
Space	

Character	ASCII	Unicode
/	47	U+002F
-	45	U+002D
?	63	U+003F
:	58	U+003A
(	40	U+0028
)	41	U+0029
.	46	U+002E
,	44	U+002C
'	39	U+0027
+	43	U+002B
Space	32	U+0020

Bibliography

[1] European Payment Council – SEPA Credit Transfer,

[2] European Payment Council – SEPA Instant Credit Transfer,

[3] European Payment Council – Standardisation of QR-codes for MSCTs, v.2.10,

[4] European Payment Council – Verification of Payee Scheme,

[5] ISO/IEC 18004:2024 – QR code bar code symbology specification,

[6] ISO 20022 – Universal financial industry message scheme,

[7] ISO 4217 – Currency codes,

[8] ISO 8601 – Date and time format,

[9] SBA – Additional Optional Service applied in Slovakia to SEPA Credit Transfer

[10] SBA – PAY by square specifications,

[11] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels,

[12] RFC 2231 – MIME Parameter Value and Encoded Word Extensions,

[13] RFC 3986 – Uniform Resource Identifiers (URI): Generic Syntax,

[14] RFC 5987 – Character Set and Language Encoding for HTTP Header Field Parameters,

[15] Semantic Versioning and Meaningful Manual Version Control for Documents - https://semverdoc.org/semverdoc.html,

[16] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.

Slovak banking association, www.sbaonline.sk, sba@sbaonline.sk