SLOVAK BANKING ASSOCIATION

payme

Payment Link Standard

Version: 2.1

Bratislava, 2026-11-09

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 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 make 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

Ver.	Release	Effective	Note/ Changes
1.0	2020-06-30	2020-06-30	First release of the document
1.1	2020-11-18	2020-11-18	Added versioning rules, Added a rule for manipulating the digit zero in the Amount attribute, Added recommended characters for attributes – Messages and Creditor's name, Added Annex A, Errata.
1.2	2021-04-15	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	2025-10-09	Set Creditor's Name as a mandatory attribute.
2.0	2025-06-15	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)
2.1	2026-11-09	2027-01-01	Added new use cases in chapter 2, Added subdomain support for bank/application routing (Authority component), Added recommendation for using Amount attribute.

Versioning of this document

A normal version number of this document must 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 must increase numerically.

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

The Major version must be incremented if the document has encountered significant and incompatible changes of specification. The Payment Link specification only contains the Major version number (see chapter 3.4.1).

The 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 without affecting the compatibility 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 contents

Foreword **6**

1 Introduction **7**
1.1 Document purpose 7
1.2 Terms and definitions 8

2 How the Payment Link works **9**
2.1 Use case 1: Sending the Payment Link via a chat app 9
2.2 Use case 2: Payment Link encoded in a QR code 10
2.3 Use case 3: Payment Link encoded in an NFC tag 11
2.4 Use case 4: Payment Link with bank-specific routing 12
2.5 Use case 5: Payment Link on an invoice 14
2.6 Use case 6: Payment Link for donations 15

3 Payment Link specification **16**
3.1 Principles 16
3.2 Format definition 16
3.3 Authority specification 18
3.4 Path specification 19
3.5 Attributes specification in Query component 20

4 Forms of Payment Link **25**
4.1 Standalone Payment Link 25
4.2 QR payment code 27

5 Recommendations for implementing Payment Link Standard **29**
5.1 Recommended Characters 29
5.2 Implementation by Type Path components 29
5.3 Implementation for QR payment code 31

6 Risk analysis **32**
6.1 Phishing and fraud 32
6.2 Data integrity 32
6.3 Non-participation 32
6.4 Service failure 33
6.5 End-user experience 33
6.6 Common reporting 33

Annexes **34**
A. Recommended characters 34

Sources **35**

Foreword

The Slovak Banking Association (hereinafter referred as *"SBA"*) is a key association in the Slovakia's financial sector and the sole organisation representing banks' interests in the Slovak Republic. One of the association's activities 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 in the activities of a 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 open 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 method for instantly requesting 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 also be used for creating a 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 the 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 recommendations,
- 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 definitions

For the purposes of this document, the following terms and definitions apply.

Term	Meaning
Biller	in this document, the party that generates a Payment Link and delivers it together with the invoice.
Creditor	a party whose payment account is credited by the payment. The Creditor is identified in the Payment Link by the IBAN and the Creditor's name attributes.
Deep linking	in our case Payment Link leads directly to unsigned payment details in mobile banking application.
ID transaction	a unique identifier of a single transaction assigned by the Merchant or by the terminal. It is carried in the Payment identification (PI).
ISO 20022	a universal financial industry message scheme.
Merchant	in this document, the party that generates a Payment Link and presents it at the Point of Interaction.
Open Graph Protocol	a protocol that enables any web page to become a rich object in a messaging application.
Payee	a person to whom money is paid or should be paid, in our case the person who generates and sends a Payment Link
Payer	a person who pays, in our case person who clicks on Payment Link, checks the payment details and authorizes the payment
Payment Link	a method for instantly requesting money from another bank client without implementation on the bank side. The Payment Link is not a payment means or a payment instrument.
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. cash machine or self-service terminal).
Push Payment Notification Standard	an SBA standard describing the notification of the Creditor, the Merchant or the terminal about a credited payment. It is used where a real-time confirmation of the payment is needed.
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 Euro Payments 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.

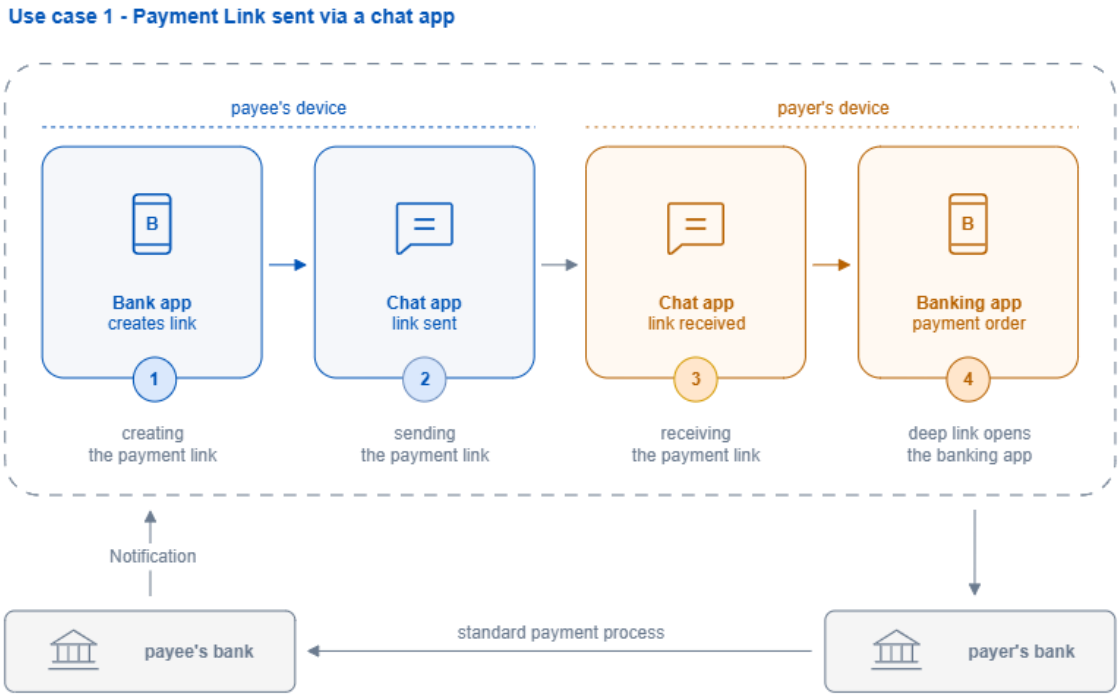
2 How the Payment Link works

The Payment Link is a simple and flexible way for a Payee to instantly request money from a Payer. It is essentially a URL with an encoded payment instruction. Payment instructions can be exchanged between the Payee and the 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).

2.1 Use case 1: Sending the Payment Link via a chat app

This use case describes sending the Payment Link in a mobile environment, via the messaging applications. The process consists of four steps: (1) creating the Payment Link, (2) sending the Payment Link, (3) receiving the Payment Link and (4) opening the banking application by clicking on the link.



Creating the Payment Link

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

Sending and receiving the Payment Link

In the next steps, the Payee sends the Payment Link to the Payer via the preferred 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, but also the enhanced visualization form of the Payment Link.

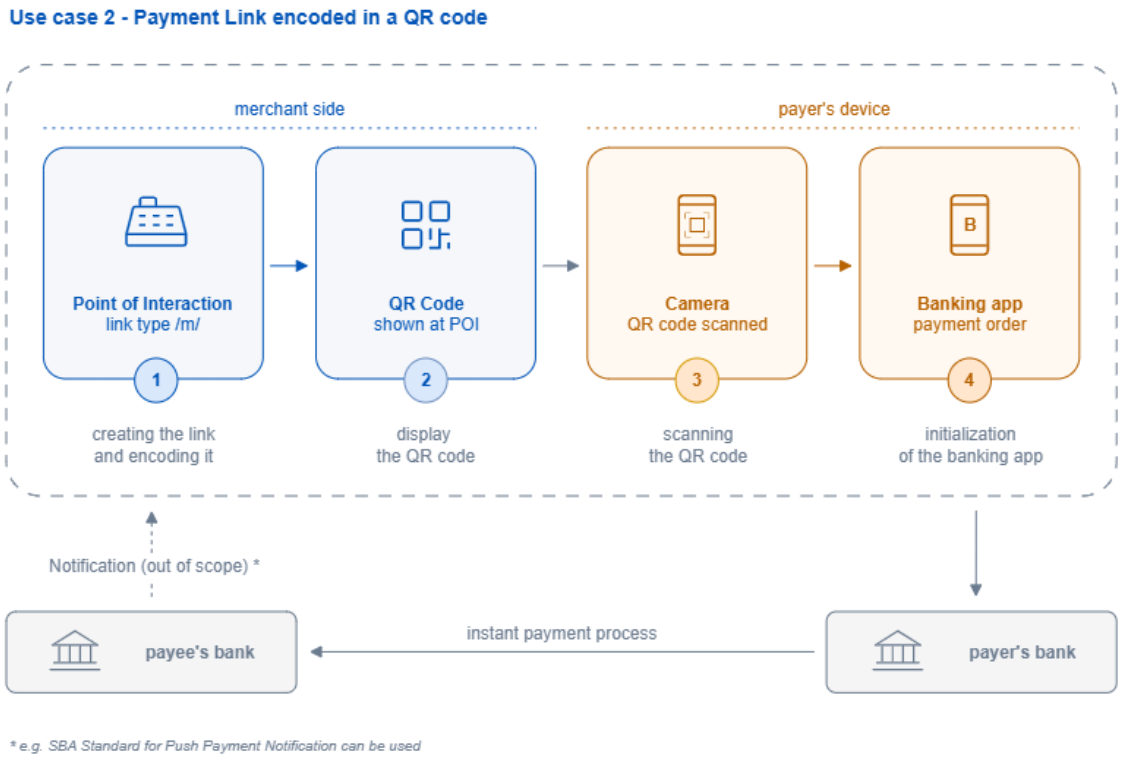
Initializing the banking application

Thanks to deep linking, clicking the Payment Link opens a banking application capable of handling it. If more than one such application is installed on the Payer's mobile device, the

mobile operating system asks the Payer to select one[1]. The banking application retrieves the payment data from the Payment Link and displays the payment order for the Payer's review. The order is then processed through the banking application's standard payment process, including the Payer's authorization.

2.2 Use case 2: Payment Link encoded in a QR code

This use case describes the payment data exchange via QR code at the Point of Interaction. The process involves: (1) creating the Payment Link and encoding it into a QR code, (2) then sending or displaying it to the payer, (3) scanning the QR code with Payment Link and (4) initializing the banking application.



Creating the Payment Link and encoding it into a QR code

The Payment Link is created by the Merchant and encoded into a QR 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.

[1] In this case, this behaviour is platform dependent. Android allows the Payer to select from all applications registered for the Payment Link and to set the selection as one-time or permanent. iOS does not offer such an application chooser: where more than one banking application claims the same Payment Link domain, the operating system does not prompt the Payer to select an application.
This limitation is relevant only when the Payment Link is opened from a message, a hyperlink or a web page. For the QR payment code (Usecase 2) and the NFC tag (Usecase 3), the Payer initiates the scan or the tap from within the banking application of their choice, so the application that will process the payment order is already determined,

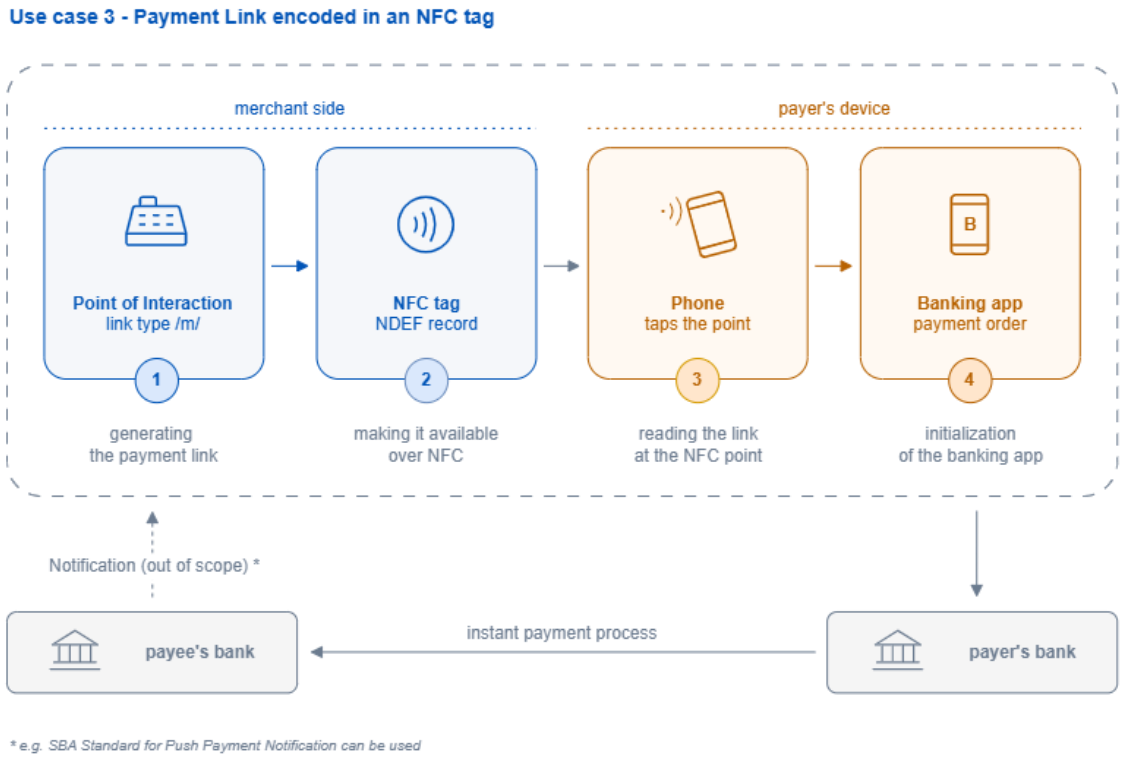
Initializing the banking application

After scanning the QR payment code, the Payment Link is opened in a banking application capable of handling it. Depending on the operating system and device configuration, the link may be opened in the default application, or the Payer may be asked to select an application capable of handling the link. The banking application retrieves the payment data from the Payment Link and displays the payment order for the Payer's review The order is then processed through the banking application's standard payment process, including the Payer's authorization.

Note: Notification of the Merchant about the credited payment is out of scope of this Standard. Where the terminal needs a real-time confirmation before releasing the goods or the service, the notification may be provided by the SBA Standard for Push Payment Notification[2].

2.3 Use case 3: Payment Link encoded in an NFC tag

This use case describes payment at self-service terminals, such as a parking meter, a ticket machine or a vending machine, where the Payment Link is transmitted to the Payer's mobile device via NFC (Near Field Communication). The terminal exposes the Payment Link using the mobile payment Type /m/. The process consists of four steps: (1) generating the Payment Link with the current transaction data, (2) making the Payment Link available over NFC, (3) reading the Payment Link with the mobile device, and (4) initializing the banking application.



Generating the Payment Link

The Payment Link is generated by the Merchant's terminal based on the current transaction data, such as the payment amount, currency, payment reference and Payee identification. The generated Payment Link uses the mobile Payment Link type (/m/).

[2] https://www.sbaonline.sk/projekt/standard-sluzby-notifikacie/

Making the Payment Link available via NFC

The terminal stores the Payment Link in an NFC Data Exchange Format (NDEF) URI record or text and makes it available through its NFC interface. The Payment Link made available through NFC shall correspond to the transaction currently displayed or selected on the terminal.

Reading the Payment Link

The Payer places or holds their NFC-enabled mobile device near the terminal's NFC interaction point. The mobile device reads the Payment Link from the NFC record.

Initializing the banking application

After the Payment Link has been read from the NFC tag, the mobile operating system opens it in a banking application capable of handling it. The banking application retrieves the payment data from the Payment Link and displays the payment order for the Payer's review. The order is then processed through the banking application's standard payment process, including the Payer's authorization.

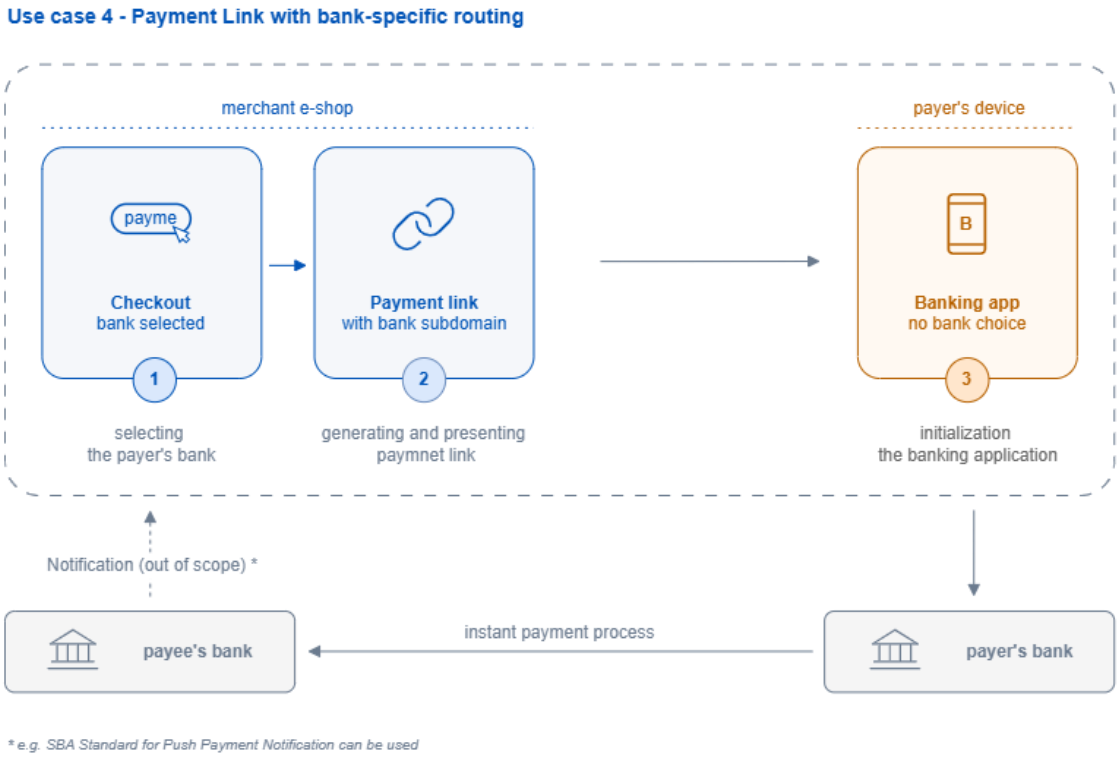
Note: Notification of the Merchant or the terminal about the credited payment is out of scope of this Standard. Where the terminal needs a real-time confirmation before releasing the goods or the service, the notification may be provided by the SBA Standard for Push Payment Notification[3].

2.4 Use case 4: Payment Link with bank-specific routing

This use case describes an online checkout in which the Payer's bank is already known, so that the Merchant can address the Payment Link to a bank-specific subdomain and route the Payer directly to the correct banking application.

Because the bank is selected before the Payment Link is generated, the bank-selection step on the Payer's device is not needed. This scenario uses the e-commerce Type /e/ and the bank-specific subdomain of the Authority component (see chapter 3.3.2). The process consists of three steps: (1) selecting the Payer's bank at checkout, (2) generating and presenting the Payment Link addressed to the bank-specific subdomain and (3) initializing the banking application.

[3] https://www.sbaonline.sk/projekt/standard-sluzby-notifikacie/



Selecting the Payer's bank at checkout

During checkout, the Payer selects payment method and specifies the bank holding the payment account, choosing from a list of supported banks presented by the Merchant.

Generating and presenting the Payment Link

The Merchant's e-commerce system then generates a Payment Link of the e-commerce type (/e/), containing the order data. The Authority component of this Payment Link uses the bank-specific subdomain assigned to the bank the Payer selected (see chapter 3.3.2). The Payment Link is then presented to the Payer as a “payme” button or hyperlink.

Initializing the banking application

Because the Payment Link is addressed to the bank-specific subdomain, the mobile operating system opens the selected bank's banking application directly. The banking application retrieves the payment data from the Payment Link and displays the payment order for the Payer's review. The order is then processed through the banking application's standard payment process, including the Payer's authorization.

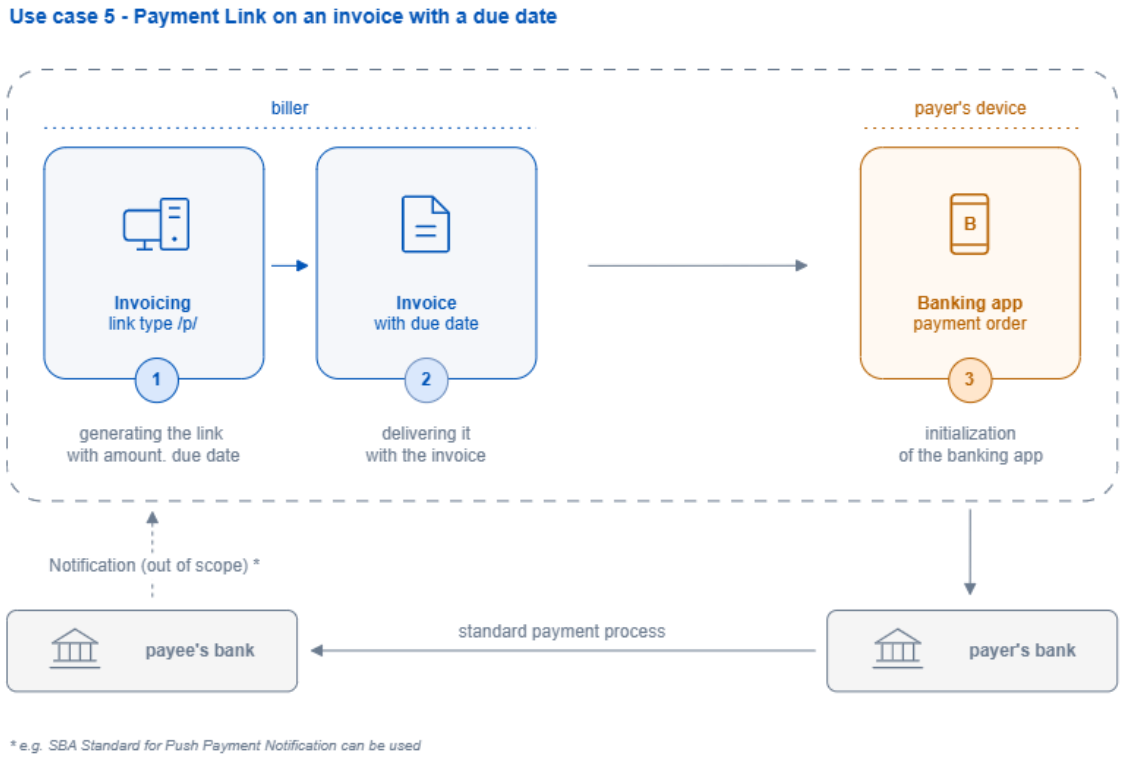
Note: Notification of the Merchant about the credited payment is out of scope of this Standard. Where the e-commerce system needs to confirm the payment before completing the order, the notification may be provided by the SBA Standard for Push Payment Notification[4].

[4] https://www.sbaonline.sk/projekt/standard-sluzby-notifikacie/

2.5 Use case 5: Payment Link on an invoice

This use case describes deferred invoice payments, where the Biller sends a clickable link or QR code with a future due date, using the person-to-person Type /p/ and the Due Date (DT) attribute.

The process consists of three steps: (1) generating the Payment Link with the amount and due date, (2) delivering it with the invoice, and (3) initializing the banking application and scheduling the payment.



Generating the Payment Link with the amount and due date

The Biller generates a Payment Link of the type (/p/) containing the IBAN and name of the Creditor, the invoiced amount, the currency, the payment identification used on the invoice and the Due Date (DT) attribute set to the due date stated on the invoice.

Delivering it with the invoice

The Payment Link is delivered to the Payer together with the invoice. In an electronic invoice it is placed as a clickable “payme” link or button; on a printed or PDF invoice it is placed as a QR payment code next to the payment details, so that the Payer can initiate the payment by scanning it. Both forms may be used on the same invoice.

Initializing the banking application

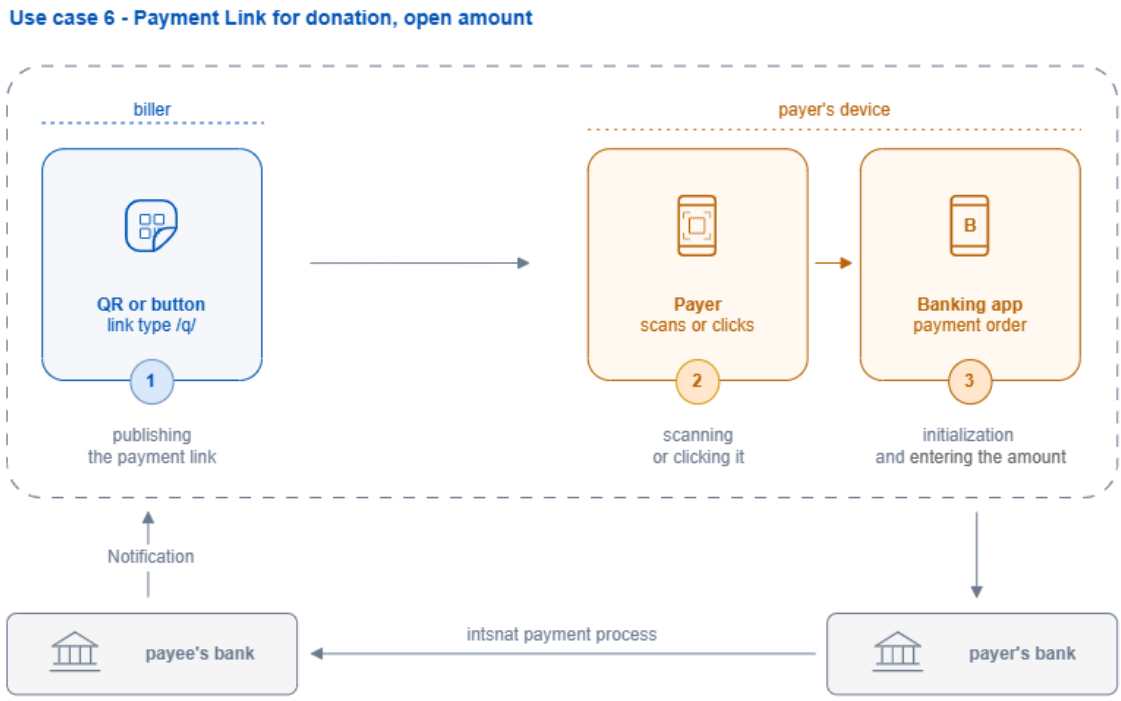
The Payer clicks the Payment Link or scans the QR payment code and the payment order is opened in a compatible banking application with the data prefilled from the Payment Link, including the due date. The Payer may execute the payment immediately or, where scheduled payments are supported by the banking application, schedule it for the due date carried in the DT attribute. The order is then processed through the banking application's standard payment process, including the Payer's authorization.

Note: Notification of the Biller about the credited payment is out of scope of this Standard. Where the Biller needs to reconcile the invoice in real time, the notification may be provided by the SBA Standard for Push Payment Notification.

2.6 Use case 6: Payment Link for donations

This use case describes an open payment request for charitable donations, where the Creditor is fixed but the amount is left optional for the Payer, using Type /q/.

The Creditor publishes a “payme” link, QR code or button for example on a poster, a website or a printed leaflet, using the Type /q/, in which the IBAN and Creditor's Name are mandatory while the amount is optional. The process consists of three steps: (1) publishing the Payment Link, (2) scanning or clicking it, and (3) initializing the banking application and entering the amount.



Publishing the Payment Link

The Creditor generates a Payment Link of the payment type (/q/) in which the IBAN and the Creditor's Name are mandatory. The Amount attribute can be omitted so that it can be defined by the Payer.

Scanning or clicking it

If the Payment Link is published in printed form, the Payer scans the QR payment code with the mobile device camera or with the banking application. If it is published in electronic form, the Payer clicks the “payme” link or button and the mobile operating system opens the Payment Link in a compatible banking application.

Initializing the banking application

The banking application retrieves the Creditor's data from the Payment Link and presents the payment order to the Payer. Because the Amount attribute is not contained in the Payment Link, the amount field remains empty and the Payer enters the amount of the donation. The order is then processed through the banking application's standard payment process, including the Payer's authorization.

3 Payment Link specification

3.1 Principles

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

- The Payment Link is an open standard,
- Creating and sending a Payment Link is available to everyone and is not dependent on the banking infrastructure,
- A payment initiated from the Payment Link is always processed in the bank's applications in a standard way with authorization,
- The “Standard” supports only SEPA payments (SEPA Credit transfer[5] and SEPA Instant Credit Transfer[6]),
- Payment Link Standard is based on EPC document: Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers[7].

- 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.

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,
- The naming convention of the attributes is aligned with ISO 20022,
- The encoded attribute names are kept 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]
```

[5] SEPA Credit Transfer (SCT)
[6] SEPA Instant Credit Transfer (SCT-Inst)
[7] 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 (//), containing the Payment Link Website domain, optionally extended with a subdomain identifying the Payer's bank and application (see chapter 3.3 Authority specification).

Path:

- A path component, consisting of a sequence of path segments separated by a slash (/).
- Based on implementation experience it is recommended not to end the path component with a slash (/).
- The Payment Link Path component consists of three mandatory parts: Version, Type and Payment Link Scheme ID[8] (see chapter 3.4 Path specification).

Query:

- A query component preceded by a question mark (?), containing a query string of non-hierarchical data. By convention it is a sequence of attribute=value pairs separated by a delimiter. The commonly used delimiter is an ampersand (&).
- The Query component consists of payment instruction attributes. The Payment Link Standard attributes are described in chapter 5 Attributes specification.

Example:

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

scheme authority path query

Examples of payme.sk implementation:

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

scheme authority path query

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

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

3.3 Authority specification

This section defines the rules for the Authority component of the Payment Link URI. It consists of the general rules for the Host component and an optional extension supporting bank-specific subdomains.



3.3.1 General rules

The Authority component shall contain only the Host component as defined in RFC 3986.

By default, the Host consists of the second-level domain of the Payment Link Website in the format: {PaymentLinkDomain} (e.g. payme.sk), referred to as the generic Authority format.

3.3.2 Bank-specific Authority extension

This section defines an optional extension of the Authority component by introducing bank-specific subdomains.

Bank-specific subdomains are intended for scenarios where the payer's bank is already known at the time the Payment Link is generated[9], for example during an e-commerce checkout where the payer has already selected their bank. In such cases, the Payment Link may directly identify the target bank, eliminating the bank selection step and improving the overall user experience. The Authority component may optionally include one or two additional subdomain levels:

https://**[{App}.]{Bank}.**{PaymentLinkDomain}/{Version}/{Type}/{PaymentLinkSchemeID}?{QueryAttributes}

Subdomain definition rules:

- {Bank} segment must uniquely identify the participating bank using a textual identifier, which may be the bank's officially registered second-level domain name, as commonly used for the bank's Internet banking services.
- {App} segment **may** be used only if the bank provides more than one application supporting the Payment Link Standard. If the bank provides only one application, the {App} segment **must not** be present.
- The value of the {App} segment **shall be** defined by the participating bank.
- If both subdomains are used, their order **must** be {App}.{Bank}.{PaymentLinkDomain}.
- The introduction of subdomains **does not modify** the definition of {PaymentLinkDomain}.
- The use of bank-specific subdomains is **optional** and **does not affect** the Path or Query components of the Payment Link.

[9] See use case in chapter 2.4 Use case 4: Payment Link with bank-specific routing

Implementation recommendation:

- Each subdomain must provide an association file that enables secure deep linking between the subdomain and the corresponding mobile banking application (e.g. Digital Asset Links or Apple App Site Association).
- Banking applications must support the generic Authority format ({PaymentLinkDomain}). Support for bank-specific subdomains is optional.
- The operator of the Payment Link Website must ensure valid DNS records and TLS certificates for all supported subdomains.
- The creator of a Payment Link should be aware that that there is no guarantee that a payment link addressed to a bank-specific subdomain will be processed by another banking application. Whether such a link is processed by another bank (application) depends solely on that bank's decision and implementation. For payment QR codes, it is therefore strongly recommended to use the generic Authority format ({PaymentLinkDomain}) instead of a bank-specific subdomain.

Example without bank identification:

```
https://payme.sk/2/p/PME?IBAN=SK6807200002891987426353&AM=8.59&CC=EUR&D
T=20280430&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

Example with bank-specific routing:

```
https://bank.payme.sk/2/p/PME?IBAN=SK6807200002891987426353&AM=8.59&CC=E
UR&DT=20280430&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

Example with bank-specific application routing:

```
https://bankapp.bank.payme.sk/2/p/PME?IBAN=SK6807200002891987426353&AM=8.5
9&CC=EUR&DT=20280430&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

3.4 Path specification

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



3.4.1 Version

Version of the *"Standard"* uses sequence-based versioning and includes only Major versions. The sequence is incremented when the data model of the Payment Link Standard is modified. No more than nine versions of the "Standard" are expected; therefore, only one character is reserved for this segment. Current version of the *"Standard"* is "2".

3.4.2 Type

The type indicates what kind of payment context is expected. The pre-defined payment context also determines which query parameters are allowed or mandatory in the payload. In this version, the following values are 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/ for person-to-person payments.

In future versions, other Type values may be defined.

3.4.3 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.

3.5 Attributes specification in Query component



Payment Link Standard supports the attributes listed in the 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 the transaction in the selected currency. The amount is represented as a decimal number with two decimal places. The decimal separator is a dot.
Currency code	CC	String (3)	*Defined by Type Path component*	ISO 4217 Alpha 3 currency code. In version 2, "EUR" is the only 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 the recipient.
Creditor's name	CN	String (70)	**Mandatory**	Name of the beneficiary (payment recipient).

* 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/). The IBAN and Creditor's name attributes 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 by Type 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

3.5.1 IBAN

International Bank Account Number (IBAN) is an identifier used internationally by financial institutions to uniquely identify the account of a customer. *The “Standard” supports identification of the bank account only via the IBAN.* This attribute is a string of up to 34 characters. ISO 20022 defines the 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

3.5.2 Amount

The attribute defines the amount of the requested payment in the selected currency. The second version of the “Standard” supports only the euro.

Note:

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

Implementation recommendations:

The amount should be represented as a decimal number with exactly two fractional digits. The decimal separator is a dot (.).

Name	Abbreviation	Example	Encoded example
Amount	AM	200.30	AM=200.30

3.5.3 Currency code

The attribute defines the currency of requested payment. The second version of the "Standard" supports only the euro. This attribute uses the three-letter currency code defined in ISO 4217.

Name	Abbreviation	Example	Encoded example
Currency code	CC	EUR	CC=EUR

3.5.4 Due date

The attribute represents the recommended due date for the requested payment. This attribute is optional and it should be filled in only for payments with a future due date. The default value of the Due date attribute is the current bank date.

Implementation recommendations:

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

If the Payment Link does not contain a due date, the bank should automatically create an unsigned payment order with the current due date.

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

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

Name	Abbreviation	Example	Encoded example
Due date	DT	30 April 2028	DT=20280430

3.5.5 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, the complexType "PaymentIdentification" and the element "EndToEndId" are used to carry this attribute. The attribute is a string of up to 35 characters. It may be mandatory or optional; the condition depends on the Type Path component (see chapter 5.2).

Note:

In the Slovak Republic up to three payment symbols are used[10]:

- *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 uses the following format "/VS{0,10}/SS{0,10}/KS{0,4}".

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

Implementation recommendations:

It is recommended to use only the characters listed in Annex A. The content of the Payment identification attribute 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

3.5.6 Message

The Message is additional payment information that the bank delivers to the Payee. The attribute is a string of up to 140 characters and is carried in the "Remittance information" element in accordance with ISO 20022.

Note:

The Message entered by the client must be URL-encoded. 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. For more information about URL encoding, see: https://www.w3schools.com/tags/ref_urlencode.asp

This "Standard" supports space encoding into both "+" and "%20", banking applications should ensure correct decoding of both alternatives. For readability, banking applications should encode spaces as "+".

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=Cafe+on+the+corner,+Zilina
Message	MSG	Cafe on the corner, Zilina	MSG=Cafe%20on%20the%20corner, %20Zilina

3.5.7 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[11].

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

Note:

This parameter entered by the client must be URL-encoded. 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. For more information about URL encoding, see:

https://www.w3schools.com/tags/ref_urlencode.asp

This "Standard" supports space encoding into both "+" and "%20", banking applications should ensure correct decoding of both alternatives. For readability, banking applications should encode spaces as "+".

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

4 Forms of Payment Link

This section describes the ways in which a Payment Link can be presented or displayed to clients.

4.1 Standalone Payment Link

The Payment Link is essentially a URL with an encoded payment instruction. The Payment Link can be used as a standalone clickable URL or a payment button. The payment instruction can thus be sent via email, SMS, messaging app, or social media.

When clicked on a smart device with a registered banking application, deep link technology automatically transforms the URI 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 (Payment Link Website) is needed to provide the Open Graph tags for the better visualization and to convert the Link into a 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:

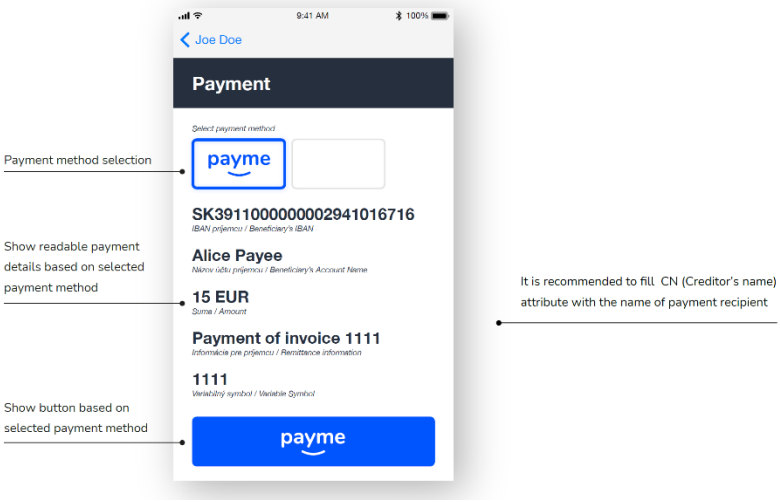
```
https://payme.sk/2/p/PME?IBAN=SK6807200002891987426353&AM=8.59&CC=EUR&DT=20280430&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

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

Figure 1: Use of payment link in mobile chat applications



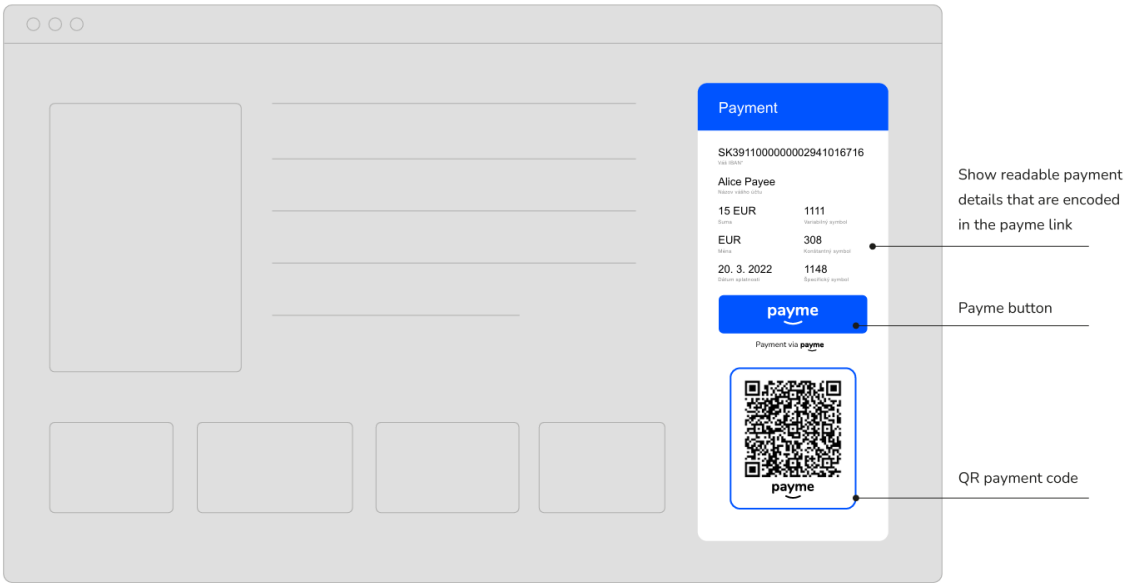
Figure 2: Use of payment link button



Example for e-commerce payments:

https://payme.sk/2/e/PME?IBAN=SK6807200002891987426353&AM=200.30&CC=EUR&PI=%2FVS2546874464%2FSS2019568456%2FKS1118&CN=The+Best+e-shops+ltd&MSG=my+e-shop,+Kosice

Figure 3: Use of payme in e-commerce



4.2 QR payment code

The Payment Link can also be 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 the 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=200.30&CC=EUR&PI=QR-ab29e346f1d841c8a95a63d857490818&CN=The+Best+Cafes+ltd&MSG=Cafe+on+the+corner+Zilina
```



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

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 Recommended Characters

Recommended character sets are listed in the “Standard” Annexes. For key attributes such as Payment Identification (PI), Message (MSG), and Creditor’s Name (CN), it is strongly recommended to use the standard ASCII character set defined in Annex 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 the Payment identification (PI) attribute 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 a 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/).

To ensure clarity across all implementation scenarios, the table below maps the use cases defined in chapter 2 to their respective Type Path components:

ID	Use Case	Recommended Type Path	Key Attribute Constraints
1	Chat App P2P	/p/ (Person-to-Person)	IBAN & CN mandatory; AM, CC, MSG optional. Editable amount.
2	QR at POI	/m/ or /q/	/m/ requires fixed AM & PI; /q/ allows optional AM for static QR. Always use SEPA Instant (SCT Inst).
3	NFC Terminal	/m/ (Mobile POI)	Always use SEPA Instant (SCT Inst). Non-editable payment order.
4	E-commerce	/e/ (E-commerce)	Requires bank-specific subdomain routing. Non-editable amount.
5	Deferred Invoice	/p/ (Person-to-Person)	Supports Due Date (DT) attribute in YYYYMMDD format.
6	Open Donations	/q/ (Static QR)	IBAN & CN mandatory; Amount (AM) omitted/optional.

5.2.1 Type /m/

Primary use: "Dynamic[12] 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].

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[13] 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:

[12] 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).

[13] 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.

- 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 identification.

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 identification,
- 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[14].

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

6 Risk analysis

6.1 Phishing and fraud

Security relies on WYSIWYS (What You See Is What You Sign) verification by the client before authorization. Deep linking prevents unauthorized redirection on devices with registered banking applications.
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 the What You See Is What You Sign (WYSIWYS) mechanism, which ensures that the semantic content of the signed message is verified by the client. The observe-before-use principle relies on the client verifying the payment attributes before authorizing the transaction.
  - the “Standard” does not support redirection to internet banking by design.
- If an attacker tries to modify the Payment Link URI to point to a different domain:
  - deep linking will fail on smart devices with registered banking application,
  - redirection to a fake domain may be successful; it is up to the client to check the domain name, security of web protocol and to avoid providing bank credentials (1st and 2nd factor) on suspicious redirected pages.
- Payment link data (e.g. IBAN and amount) are susceptible to modification on a malware-infected smart device.

Implementation recommendations:

The deep link processor (e.g. the banking application) can mitigate this risk by preventive measures, e.g. by showing a warning for unknown, suspicious, untrusted or first time used IBANs, and by applying anti-malware techniques such as rooted-device detection.

6.2 Data integrity

The following deficiencies were found in the analysis:

- HTTPS protects the transmission when a URI is loaded over the network. It does not provide protection for the authenticity or integrity of payment link parameters embedded in QR codes, NFC codes, messages, or other distribution channels.
- To improve data integrity in QR payment initialization, the Verification of Payee (VoP) service validates the recipient’s identity based on extracted account details (IBAN and Creditor's Name) before transaction authorization. This reduces the risk of misdirected payments caused by incorrect or tampered QR data and ensures alignment with EU Instant Payments Regulation (2024/886).

6.3 Non-participation

The “Standard” also works for clients of banks that have not implemented it in their mobile applications. In such cases the Payment Link is opened on the Payment Link Website, where it is displayed in a readable form together with a QR payment code that can be scanned in any banking application supporting QR payments.

6.4 Service failure

The Standard minimizes dependency on central components in the following ways:

- The definition of the Standard is open, and encoding is performed entirely by the request sender's application without real-time backend API calls;
- The Payment Link is interpreted directly by the target mobile banking application on the client's device using native OS deep-linking mechanisms;
- The central component (Payment Link Website) is required solely for non-participating subjects (to render a fallback QR codes or Open Graph metadata);
- Only mandatory parameters encoded within the URL query string are required for the banking application to construct a valid SEPA payment order, ensuring full offline processing capability at the Point of Interaction without real-time backend API dependencies.

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),
- visualize the clicked Payment Link in a readable form,
- provide the Open Graph tags to visualize the Payment Link in mobile messaging applications,
- generate Payment Link form.

6.6 Common reporting

To monitor the adoption and performance of the Standard, participating banks shall provide monthly statistical reporting to the SBA by the 15th calendar day of the following month. The reporting shall be provided in the template and through the channel agreed within the relevant SBA working group, and shall include:

- Total volume and value: Total number of initiated transactions and total cumulative monetary volume (in EUR).
- Breakdown by Payment Type: Aggregated metrics categorized by Type Path components (/m/, /e/, /q/, /p/).
-
- Note: All reported statistical data must be anonymized and aggregated in compliance with applicable data privacy and GDPR regulations.

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

Sources

[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] Phosphor Icons,

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

[11] SBA – Standard for Push Payment Notification,

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

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

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

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

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

[17] 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

payme

Slovak Banking Association, www.sbaonline.sk, sba@sbaonline.sk