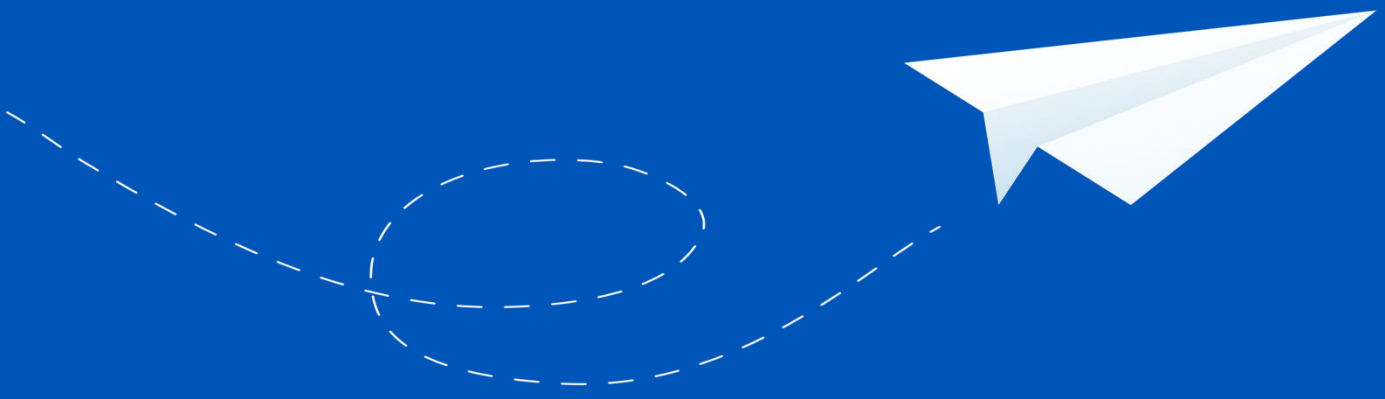
SLOVAK BANKING ASSOCIATION

Payment Link Standard



Version: 1.3

Bratislava, 2025-07-16

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.

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 3.3.1.1 Version)

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

Table of Figures

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 peer-to-peer payment instructions in the mobile messaging applications.

Unlike the planned Request-To-Payment solutions[1], the Payment Link does not use a connection directly to the back-end banking interfaces and supports the transfer of payment information only.

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 potential risks arising from the use of the Payment Link and how to mitigate them.

[1]E. g. Multi-Stakeholder Group on Request-To-Pay or Request-To Pay by PAY.UK

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.
Request-to-pay	the set of operating rules and technical elements (including messages) that allow a Payee (or creditor) to claim an amount of money from a Payer (debtor) for a specific transaction.
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 instantly request money from another bank client. It is a simplified type of Request-to-Pay without a direct connection to the back-end banking interfaces. There is therefore no need for an extensive and expensive implementation by the banks.

The existence of a common *„Standard“*, a common website and a domain is essential for the functioning of the Payment Link. The common “Standard” (Paymnet Link Standard) describes the rules for creating the Payment Link (see chapter 3 Payment Link specification). The common 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. Domain (Payment Link Domain) is needed to define Payment Link syntax and to provide deep linking for automatic redirection.

The Payment Link described in this document is intended especially for sharing peer-to-peer payment instructions. Risk analysis in chapter 4 concerns only that usage of Payment Link. Using the Payment Link any other way is not prohibited, but it requires to prepare an extended risk analysis and potentially extension of the existing Standard to new usecases.

„Standard“ covers two use cases for sharing peer-to-peer payments instructions:

(1) baseline scenario for sending and receiving the Payment Link in the mobile environment,

(2) extended scenario for sending and receiving the Payment Link in desktop environment.

2.1 Baseline scenario

The baseline scenario 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.

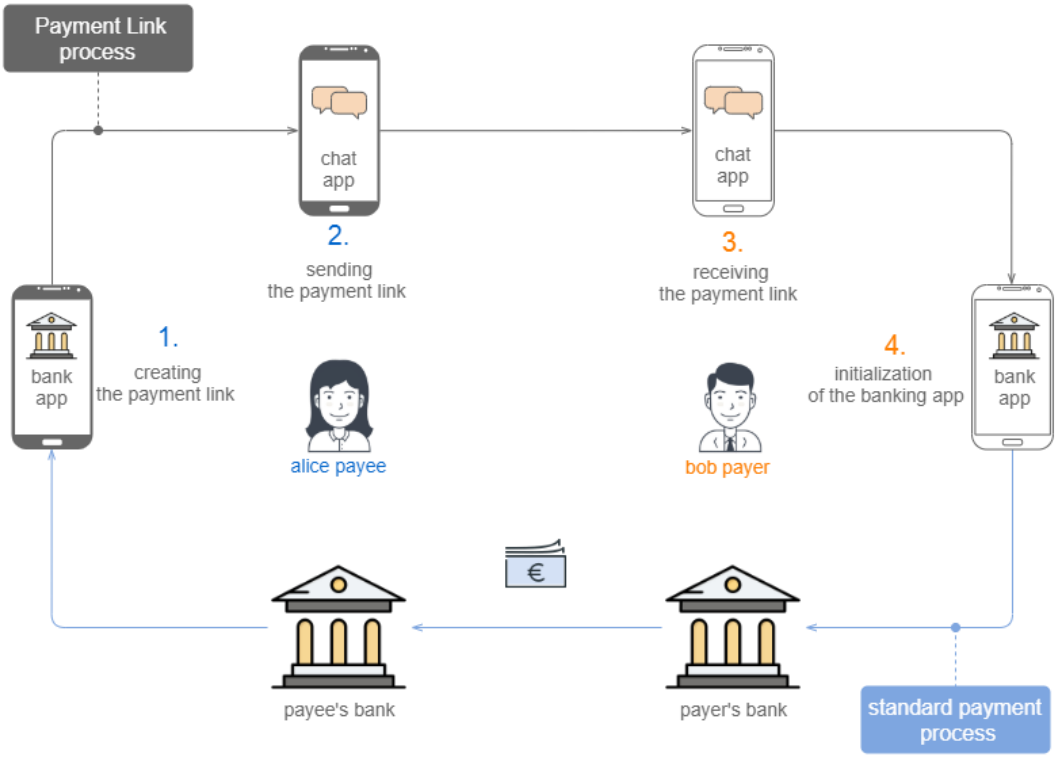


Figure 1: Baseline scenario

Creating the Payment Link

The Payment Link can be created by the Payee in the existing bank applications. For a better user experience, it can be created directly in the mobile messaging applications, through the so called „third party apps“ (e. g. iMessage Extension).

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

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 Extended scenario

The extended scenario describes sending (receiving) the Payment Link in the desktop environment, for example via the email. The Payment Link Process in this scenario consists also of four steps: (1) creating the Payment Link, (2) sending the Payment Link, (3) receiving the Payment Link and (3) open the Payment Link Website with QR payment code.

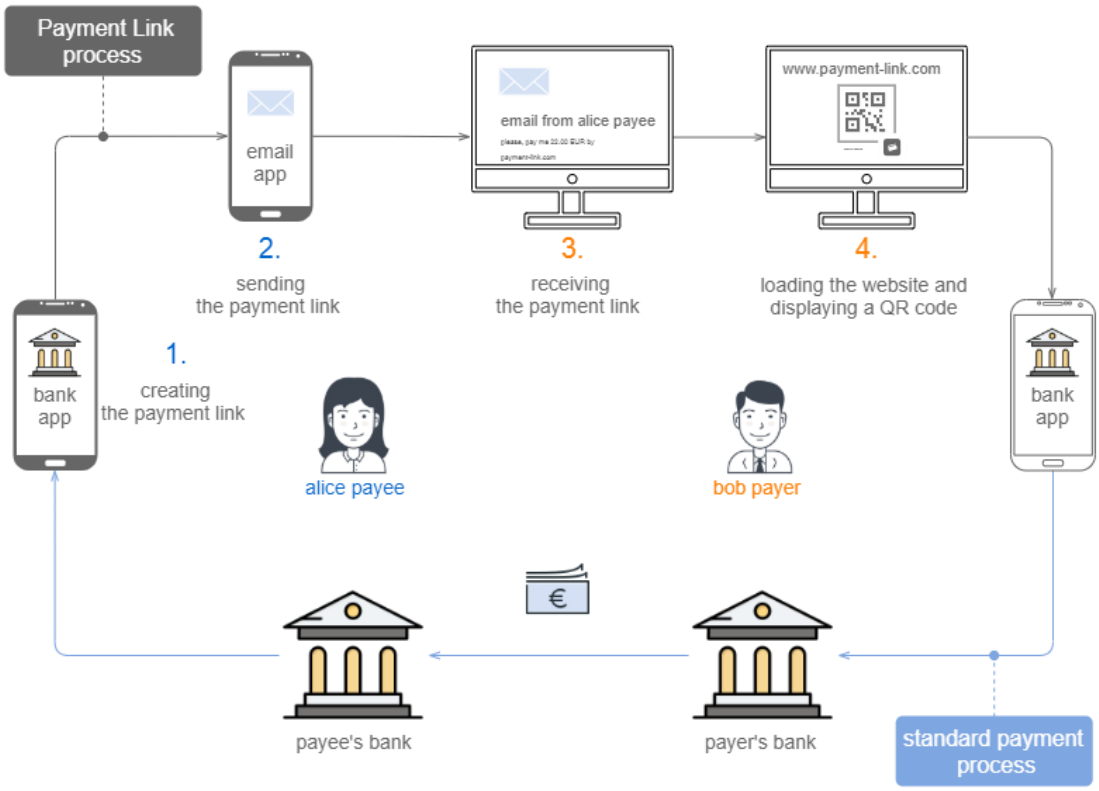


Figure 2: Extended scenario

Creating the Payment Link

The Payment Link is created by the Payee in the same way as in the Baseline scenario.

Sending and receiving the Payment Link

In the nexts steps, the Payee sends the Payment Link to the Payer for example via the email.

Loading the Payment Link Website and displaying a QR payment code

After the clicking on the Payment Link in the email, the Payer will be redirected to the Payment Link Website with payment data and QR payment code (PAY by square).

The Payer can scan QR code and use PAY by square functionality available in his bank app or can copy payment data and then create a payment order in the internet banking.

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

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]
```

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 optional authority component preceded by two slashes (//). The authority component options is not used in the Payment Link Standard.

Path:

- A path component, consisting of a sequence of path segments separated by a slash (/).
- Based on implementation experience it is recommend to end path component with a slash (/).
- The second level domain name of the Payment Link Web is represented the following way{PaymentLinkDomain}
- If the standard will be extended with another payment products, for each of them new a domain will be created.

Query:

- An optional 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 (&).
- Payment Link Standard attributes are describe in chapter 3.3 Attributes specification.

Example of Payment Link syntax:

```
https://{PaymentLinkDomain}?V=1&IBAN=SK6807200002891987426353&AM=2
00.30&CC=EUR&DT=20201205&PI=%2FVS2546874464%2FSS2019568456%2FKS111
8&MSG= Thank+you+for+lunch.&CN=Alice+Payee
```

Example of payme.sk implementation:

```
https://payme.sk/?V=1&IBAN=SK6807200002891987426353&AM=200.30&CC=E
UR&DT=20201205&PI=%2FVS2546874464%2FSS2019568456%2FKS1118&MSG=
Thank+you+for+lunch.&CN=Alice+Payee
```

3.3 Attributes specification

Payment Link Standard supports attributes listed in following table.

Table 1: List of supported attributes:

Name	Encoded name	Type (max. length*)	Condition	Description
Version	V	String(1)	Mandatory	Major version of the „Standard“. Starting with “1”.
IBAN	IBAN	String(34)	Mandatory	International Bank Account Number
Amount	AM	String(9)	Mandatory	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)	Mandatory	Currency in ISO 4217 Alpha 3 currency code. In version 1 is only “EUR” valid currency code.
Creditor’s name	CN	String(70)	Mandatory	Beneficiary name of the payment receipient.
Due date	DT	ISODate	Optional	Due date in ISO 8601 format YYYYMMDD.
Payment identification	PI	String(35)	Optional	Payment identification used as EndToEndId reference.
Message	MSG	String(140)	Optional	Message for receipient.

* max length is defined for data without URL encoding.

3.3.1 Further details and examples

3.3.1.1 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 e.g.: new attribute is added 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 “1”.

Name	Abbreviation	Example	Encoded example
Version	V	1	V=1

3.3.1.2 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	SK6807200002891987426353	IBAN=SK6807200002891987426353

3.3.1.3 Amount

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

This attribute can be “0” in cases requested payment amount is not known, in such cases as donations.

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

3.3.1.4 Currency code

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

Note:

This attribute is mandatory, even though the first version of „Standard“ allows to use only one currency code EUR.

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

3.3.1.5 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.

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.

Name	Abbreviation	Example	Encoded example
Due date	DT	5. December 2020	DT=20201205

3.3.1.6 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 is optional.

Note:

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

- *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}”.

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

3.3.1.7 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

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.

3.3.1.8 Creditor’s name

The attributes represents name (first name and surname in case of individual persons or company name) of the party whose account will be credited with the payment. This is optional attribute up to 70 characters long string.

Implementation recommendations:

If the creditor's name is filled in the requested payment message, this name should be used in initiated payment.

If the creditor's name is empty in the requested payment message, the bank should use its own methods to insert this information (e.g. to ask the client to enter creditor's name, or use the client contacts directory).

It is recommended not to use the characters listed in Annex B.

Name	Abbreviation	Example	Encoded example
Creditor's name	CN	Alice Payee	CN=Alice+Payee
Creditor's name	CN	Alice Payee	CN=Alice%20Payee

3.3.1.9 Attributes examples

Table 2: List of attributes examples:

Payment structure	Abbreviation	Example	URL Encoding
*Version	V	1	V=1
*IBAN	IBAN	SK6807200002891987426353	IBAN=SK6807200002891987426353
Amount	AM	200,30	AM=200.30
*Currency	CC	Euro	CC=EUR
Creditor's name	CN	Alice Payee	CN=Alice+Payee
Due date	DT	20201205	DT=20201205
Payment identification	PI	/VS2546874464 /SS2019568456 /KS1118	PI=%2FVS2546874464 %2FSS2019568456 %2FKS1118
Message	MSG	Thank you for lunch.	MSG=Thank+you+for+lunch.

"*" mandatory payment attributes.

Examples shows how to generate standard link:

```
https://{PaymentLinkDomain}?V=1&IBAN=SK6807200002891987426353&AM=200.30&CC=EUR&DT=20201205&PI=%2FVS2546874464%2FSS2019568456%2FKS1118&MSG=Thank+you+for+lunch.&CN=Alice+Payee
```

```
https://{PaymentLinkDomain}?V=1&IBAN=SK6807200002891987426353&AM=200.30&CC=EUR&MSG=Thank+you+for+lunch&CN=Alice+Payee.
```

```
https://{PaymentLinkDomain}?V=1&IBAN=SK6807200002891987426353&AM=0&CC=EUR&CN=Alice+Payee
```

Examples of payme.sk implementation:

```
https://payme.sk/?V=1&IBAN=SK6807200002891987426353&AM=200.30&CC=E
UR&DT=20201205&PI=%2FVS2546874464%2FSS2019568456%2FKS1118&MSG=Than
k+you+for+lunch.&CN=Alice+Payee
```

```
https://payme.sk/?V=1&IBAN=SK6807200002891987426353&AM=200.30&CC=E
UR&MSG=Thank+you+for+lunch&CN=Alice+Payee
```

```
https://payme.sk/?V=1&IBAN=SK6807200002891987426353&AM=0&CC=EUR&CN
=Alice+Payee
```

4 Risk analysis

4.1 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),
  - 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.

4.2 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.
- 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.

4.3 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 QR code (PAY by square) with all payment details in a readable form.

4.4 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.

4.5 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 + QR payment code (PAY by square),
- provide the Open Graph tags to visualize the Payment Link in mobile messaging applications,
- generate Payment Link form.

4.6 Common reporting

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

Annexes

A. Recommended characters

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

B. Not allowed characters

& (ampersand)
< (left brace)
> (right brace)
" (double quotation)

Bibliography

[1] ISO 20022 - Universal financial industry message scheme

[2] PAY by square specifications

[3] RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels

[4] RFC 2231 - MIME Parameter Value and Encoded Word Extensions

[5] RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax

[6] RFC 5987 - Character Set and Language Encoding for HTTP Header Field Parameters

[7] Request to pay (pay.uk)

[8] Request-to-Pay Specifications for a standardisation framework, Version 1.0 (EPC)

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

[10] https://en.wikipedia.org/wiki/HTTPS

[11] https://en.wikipedia.org/wiki/Single_Euro_Payments_Area

[12] https://en.wikipedia.org/wiki/URL

[13] https://www.w3schools.com/

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