**Change Request**

**for the update of ISO 20022 financial repository items**

1. **Origin of the request:**

*A.1 Submitter*:

The Mojaloop Foundation

*A.2 Contact person:*

Michael Richards. Michael.Richards@infitx.com, +44 7785 360009

 *A.3 Sponsors*:

1) Africanenda

2) Comesa Business Council

Contact: Dr. Jonathan Pinifolo, jpinifolo@comesabusinesscouncil.org

1. **Related messages:**

Pacs.008.001 - FIToFICustomerCreditTransfer

Pacs.009.001 - FinancialInstitutionCreditTransfer

New messages to be defined sealing the agreement of terms between the parties for Customer Credit credit transfers and Financial Institution credit transfers.

1. **Description of the change request:**

We want to define new elements in the data dictionary to support the definition of a cryptographic lock which can be attached to the definition of a credit transfer. The reasons for wanting to attach a cryptographic lock are given in detail in CR 1357, which describes the use of the cryptographic lock. The cryptographic lock will be used in the following messages:

* The message which defines the agreed terms of a payment. This is a new message which is the subject of a Business Justification to be submitted to the ISO 20022 Payments SEG.
* The payment execution message (pacs.008).
* The message which defines the agreed terms of a cover request. This is a new message which is the subject of a Business Justification to be submitted to the ISO 20022 Payments SEG.
* The cover request message (pacs.009).

These elements will be defined by a definition analogous to that used in the existing data dictionary for elements such as *Frequency36Choice*, where the creator of the message can choose between different formats for a frequency of payment. In this case, we will allow the creator of the message to choose between different types of cryptographic lock.

The following types of cryptographic lock will be supported in the first instance:

1. An IlpV4Packet. This will be a representation of the data element of an ILP v4 packet, as described [here](https://interledger.org/developers/rfcs/interledger-protocol/). This element will be an encoded string of arbitrary length. The most accurate way of representing this element would be the candidate data element *hexBinary*.
2. A SHA-256 signature created using a private key belonging to the entity that sealed the terms of the payment. This signature will have a fixed length of 32 bytes, and will be represented as a hexadecimal string. The existing data elements which represent hexadecimal encodings of binary strings (e.g. Max32HexBinaryText) are not suitable for this purpose since they support strings of any length up to a maximum. We therefore propose a new data type, whose name will be Exact32HexBinaryText. It will be calqued on the existing Exact1HexBinaryText, and is described in more detail below.

The definition of the proposed new Exact32HexBinaryText data element in MDR format will be as follows:

***Exact32HexBinaryText***

*Definition: Specifies a character string with an exact length of 32 binary bytes (64 hexadecimal text characters).*

*Used for hex binary data only, supports only characters A-F and 0-9.*

*Type: Text*

*Format*

*pattern ([0-9A-F][0-9A-F]){32}*

The name of the proposed data type will be *CryptographicLockChoice*. The definition of the proposed new data type in MDR format will be:

**CryptographicLockChoice**

*Definition*: choice of format for a cryptographic lock which ensures that a payment execution request can only be executed on the terms previously agreed.

.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Or** | **MessageElement*<XML Tag>*** | **Mult.** | **Type** | **Constr. No.** | **Page** |
| {Or | [IlpV4PreparePacket](#_bookmark2601) *<Ilpv4PrprPkt>* | [1..1] | HexBinary |  |  |
| Or} | [Sha256Signature](#_bookmark2605) *<Sh256S>* | [1..1] | Exact32HexBinaryText |  |  |

1. **Urgency of the request:**

It is proposed to include this change request in the next regular maintenance cycle.

1. **SEG/TSG recommendation:**

*This section is not to be taken care of by the submitter of the change request. It will be completed in due time by the SEG(s) in charge of the related ISO 20022 messages or the TSG for changes related to the BAH.*

|  |  |  |
| --- | --- | --- |
| **Consider** | X | **Timing** |
|  | - **Next yearly cycle: 2024/2025**(the change will be considered for implementation in the yearly maintenance cycle which starts in 2024 and completes with the publication of new message versions in the spring of 2025) | X |
|  | - **At the occasion of the next maintenance of the messages**(the change will be considered for implementation, but does not justify maintenance of the messages in its own right – will be pending until more critical change requests are received for the messages) |  |
|  | - **Urgent unscheduled**(the change justifies an urgent implementation outside of the normal yearly cycle) |  |  |
|  | - **Other timing:** |  |

Comments: CR will be reviewed as part of the 2024/2025 maintenance cycle.

|  |  |
| --- | --- |
| **Reject** |  |

Reason for rejection: