

Mojaloop functional extensions

Michael Richards



Areas for discussion



- An ISO 20022 version of Mojaloop
- Currency conversion and foreign exchange



An ISO 20022 version of Mojaloop

Why are we doing this?



- Central banks and market infrastructures are already using ISO 20022 messages
- Global organisations such as the World Bank want to concentrate on ISO 20022-based payment systems
- Existing banks (though not other types of participant) are used to using ISO 20022 messages to support payments

What's the benefit for the Mojaloop community?



- Alignment with an established international standard for payment systems.
- The ability to influence ISO 20022 messaging to align it better with Level One principles.
- The ability to extend the reach of ISO 20022 messaging to new types of participants and jurisdictions.
- Remove some of the roadblocks to Mojaloop entry for scheme operators and participants.

What did we propose for PI 16?



- A switch-hosted ISO version of Mojaloop for one implementation.
- A version of our extensions to existing messages, agreed by the ISO 20022 organisation.
- Potential ISO 20022 solutions to the following issues:
 - Identifier management
 - Currency conversion
 - Authorisation
 - Account relationships for 3PPIs
- A draft Mojaloop ISO 20022 Market Practice Document

Market practice document



- A self-published document
- Describes how to execute use cases in an ISO 20022 Mojaloop
 - Which messages to use
 - Which fields to use/not to use
 - ...and what it means to use them
 - Needs to be *complete*

So it sounds like we're doing OK....?



- Er, sort of...
- We know how to use the ISO 20022 messages to talk Mojaloop in particular cases...
- But that's not the same thing as an ISO 20022 version of Mojaloop

**A (slight) change
of direction**



The Mojaloop message suite



Our original plan was:

- Repurpose a selection of standard ISO 20022 message formats for Mojaloop's particular purposes
- Modify message content where necessary
- Specialise them using a Market Practice Document

Drawbacks



- There were areas where Mojaloop needed coverage, but there were no suitable ISO messages available for use.
- Some of the messages we proposed to use would be understood by the general ISO 20022 community in a sense different from how Mojaloop intended to use them.
- Some of the messages we proposed to use would need considerable specialisation for long-term use in the Mojaloop context
 - Example: directory look-up
- We would still be combining and specialising messages in a way that aligns with Mojaloop's requirements, but which would not necessarily be obvious to parties used to ISO 20022 messages in other contexts.
- We would be asking participants who were not traditional banks to absorb expertise about the format of payments messages which were not necessarily strictly relevant to the Mojaloop system.

An alternative approach



- The existing ISO 20022 data dictionary contains (most of) the structures that Mojaloop needs.
- We use these structures to build a suite of messages appropriate to what Mojaloop is and how it wants to work.
- We accompany these proposals with an ISO 20022 Business Justification to explain them to the ISO 20022 community.
- We explain them to participants using a Market Practice Document, as before.

Advantages and disadvantages



- ✓ All the endpoints required to operate a Mojaloop scheme use members of the same suite of messages.
- ✓ Standard representational techniques (e.g. of a party) can be consistent across messages.
- ✓ Information irrelevant to the Mojaloop payment model is excluded from the message definition, not by the Market Practice Document.
- ✓ External parties will find it easier to understand how to interact with a Mojaloop system.
- ✗ Institutions which already make payments using ISO messages may need to learn a new way of managing payments.
- ✗ Valuable generalisation may be lost.

ISO 20022 Business Justification



Explains:

- The business purpose this message set supports
- The message characteristics we need
- The reasons why we need them
- It's about messages, not endpoints

Business purpose



- Straight through instant payments...
- ...between institutions...
- ...that do not depend on existing relationships between the institutions.

Messages, not endpoints



- ISO 20022 wants to define general forms...
- ...which can then be specialised for particular purposes

An example: identification



- An identification associates an identifier with a participant and with information about the entity identified
- Mojaloop currently defines an identification as a nested structure:
 - FspId
 - PartyIdInfo
 - Party
 - PartyResult
- And uses the structure appropriate to the particular endpoint:
 - FspId in **POST /transfers**
 - PartyIdInfo in **POST /participants**
 - Party in **POST /quotes**
 - PartyResult in **PUT /participants**

The ISO 20022 approach



- Define a single structure
- Specialise its use in particular endpoints...
- Using the Market Practice Document

Message characteristics



- Party identification
- Definition of terms
- Definition of relationships
- Authorisation
- Cryptographic locks
- Idempotency identification
- Additional information

Party identification



- Identifier
 - Type
 - Value
- Optional ancillary information
- Optional status information

Terms



- Define an action which will result in the creation of financial obligations under the rules of a scheme
 - Transfer terms
 - Currency conversion terms
- Contain:
 - Parties
 - Amounts
 - Principal amounts
 - Fees
 - Commission amounts
 - Ancillary information
 - For instance, transaction type

Relationships



- Define a relationship between two institutions in relation to one or more customer identities
- Contain:
 - Identifications
 - Actions
 - Credential definitions

Authorisations



- Used by one institution to delegate customer authorisation for an action to another institution
- Contain:
 - A challenge
 - Definition of terms
 - Authorisation type

Cryptographic locks



- Allow institutions to verify the content of other requests
- Contain:
 - A signature
 - A validity period
 - Optionally, the terms to which the signature relates

Idempotency information



- Used to differentiate instances of messages of the same type
- Contains:
 - A UUID

So, for example...



A quotation contains:

- A required idempotency identifier
 - An optional cryptographic lock
 - A required definition of terms
-
- A quotation request *must not* include a cryptographic lock
 - A quotation acceptance *must* include a cryptographic lock
 - ... but these conditions will form part of the Market Practice Document.

Where are we now?



- A draft Business Justification has been prepared and submitted to the ISO 20022 Payments Group
- Initial feedback has been received
- Feedback is being incorporated into a revised submission

What do we plan for the next PI?



- Business Justification made available for review and comment by the Mojaloop community
- Business Justification approved by ISO 20022 Payments Group
- Draft Market Practice Document
 - Submitted for review by Mojaloop SIGs and CCB
 - Reviewed with potential implementers and other interested parties

Currency conversion and foreign exchange



What did we propose for this PI?



- API definitions agreed.
- Bounded context agreed.
- FXP simulator built and available for sandboxes and hackathons.
- Code build tasks agreed and started.



A further wrinkle...

Can currency conversion be controlled by the switch?



- Advantages:
 - Existing participants don't need to make changes to their applications or operating practices.
 - Problems associated with the existing two-transfer model will be obviated.

Questions:



- How will the switch identify that a transfer requires currency conversion?
- How will the switch interact with an existing FXP?
- How will we ensure that participants see what they expect in the ledgers?
- What about state?
- What about non-repudiation?

Questions:



- How will the switch identify that a transfer requires currency conversion?
 - A database query
 - Issued as part of processing the **POST /quotes** and **POST /transfers** endpoints
 - Since DFSPs will not change their message structures, the new form of notification via the **PUT /parties** response will not be activated...
 - ... but if it is, the switch will prefer it.
 - A configuration item will be used to turn switch-activated currency conversion on or off.

Questions:



- How will the switch interact with an existing FXP?
 - Via an instance of Payment Manager...
 - ... which talks new FXP on the switch side and old FXP on the FXP side

Questions:



- How will we ensure that participants see what they expect in the ledgers?
 - That is:
 - A debit from the payer DFSP and a credit to the FXP in the source currency.
 - A debit from the FXP and a credit to the payee DFSP in the target currency.
 - Instead of:
 - A debit from the payer DFSP and a credit to the FXP in the source currency.
 - A debit from the FXP and a credit to the payer DFSP in the target currency.
 - A debit from the payer DFSP and a credit to the payee DFSP in the target currency.

Questions:



- How will we ensure that participants see what they expect in the ledgers?
 - This will require specialist processing from the switch.

Questions:



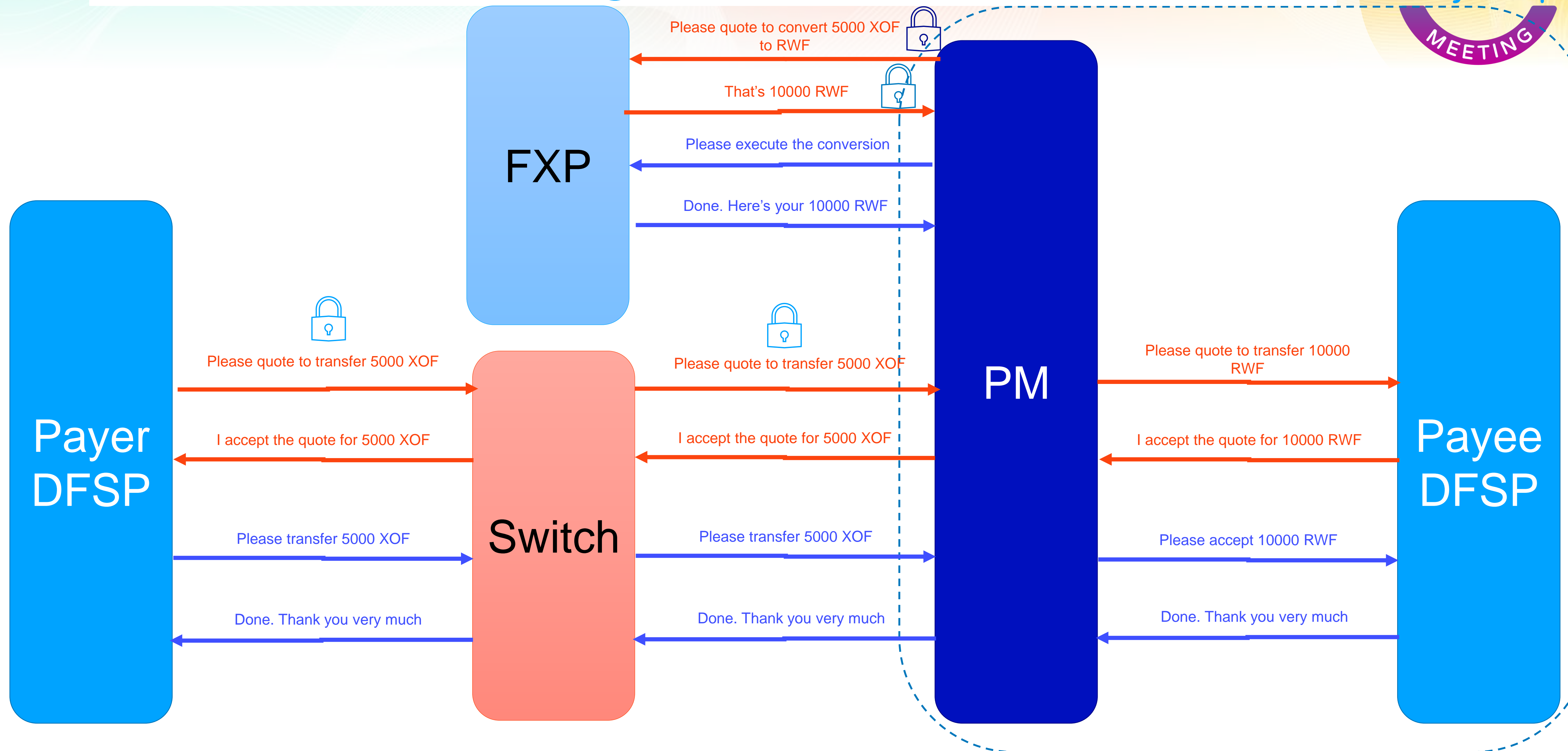
- What about state?
 - The switch will need to store and access
 - Quotations
 - Currency conversion quotations
 - Currency conversion execution requests and responses
 - Transfer execution requests and responses
 - ... as well as maintaining the relations between them.
 - This is (much) more than we would normally ask the switch to do...

Questions:



- What about non-repudiation?
 - The switch will need to generate new messages.
 - It will therefore need to construct the non-repudiation signatures itself.
 - So the trusted originator of quotation and transfer messages will move from being the participant to being the switch.
 - There may be a philosophical objection here...
 - ...on the other hand:
 - The switch already creates and signs error messages
 - We already ask participants to trust the switch, for instance in recording obligations.

There are always alternatives...





Any questions?