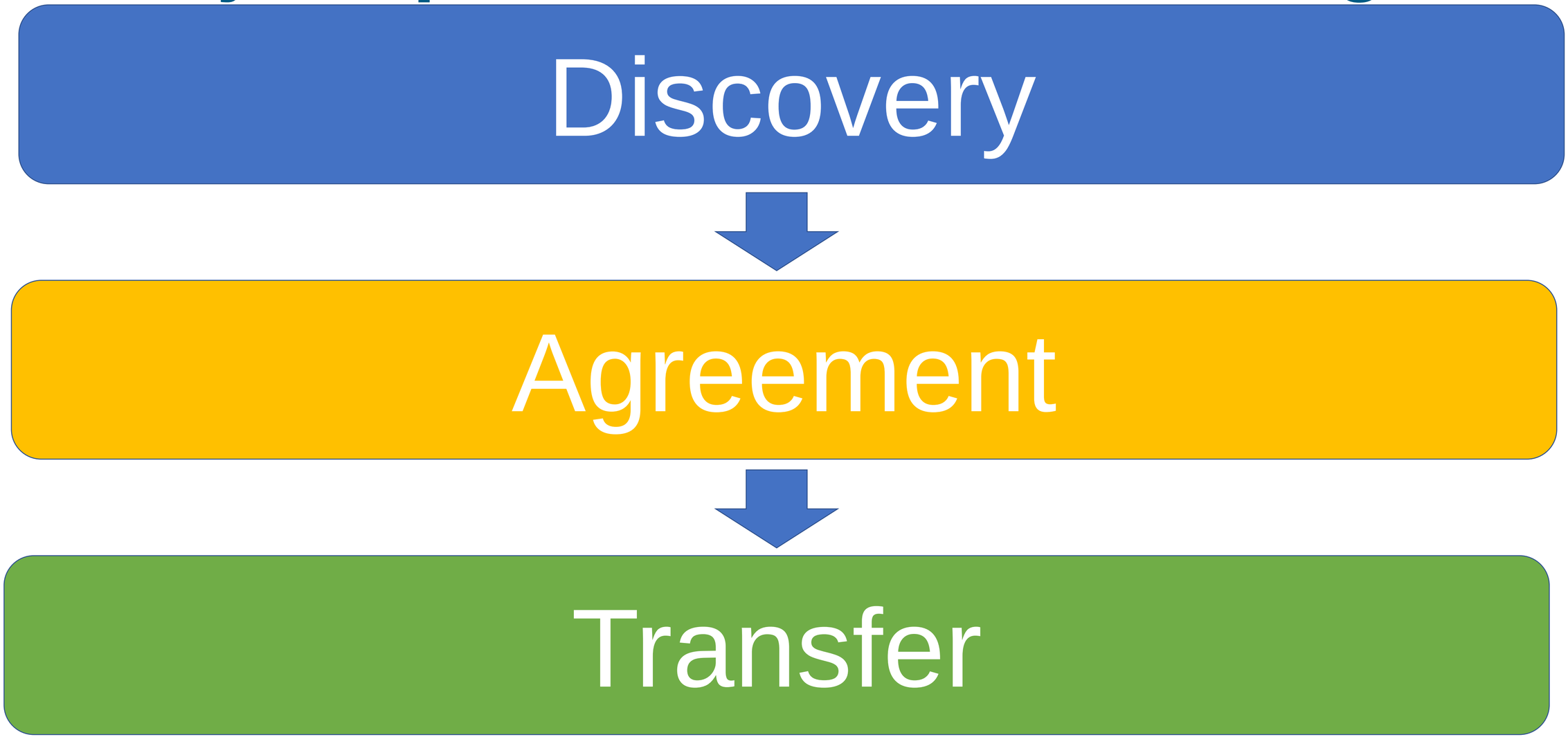
mojaloop

Anatomy of a Mojaloop Transfer

mojaloop

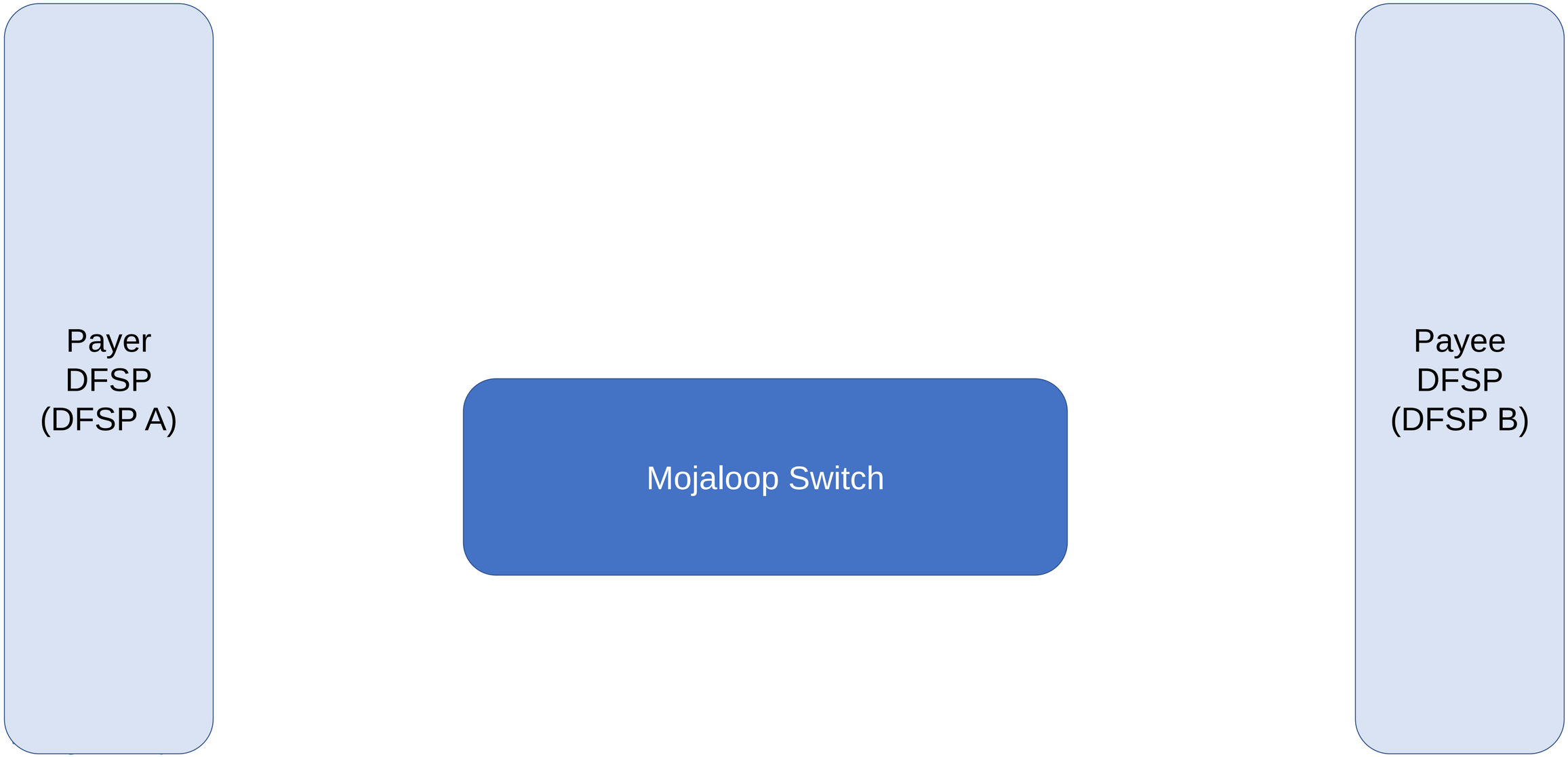
A Mojaloop Transfer has three stages:



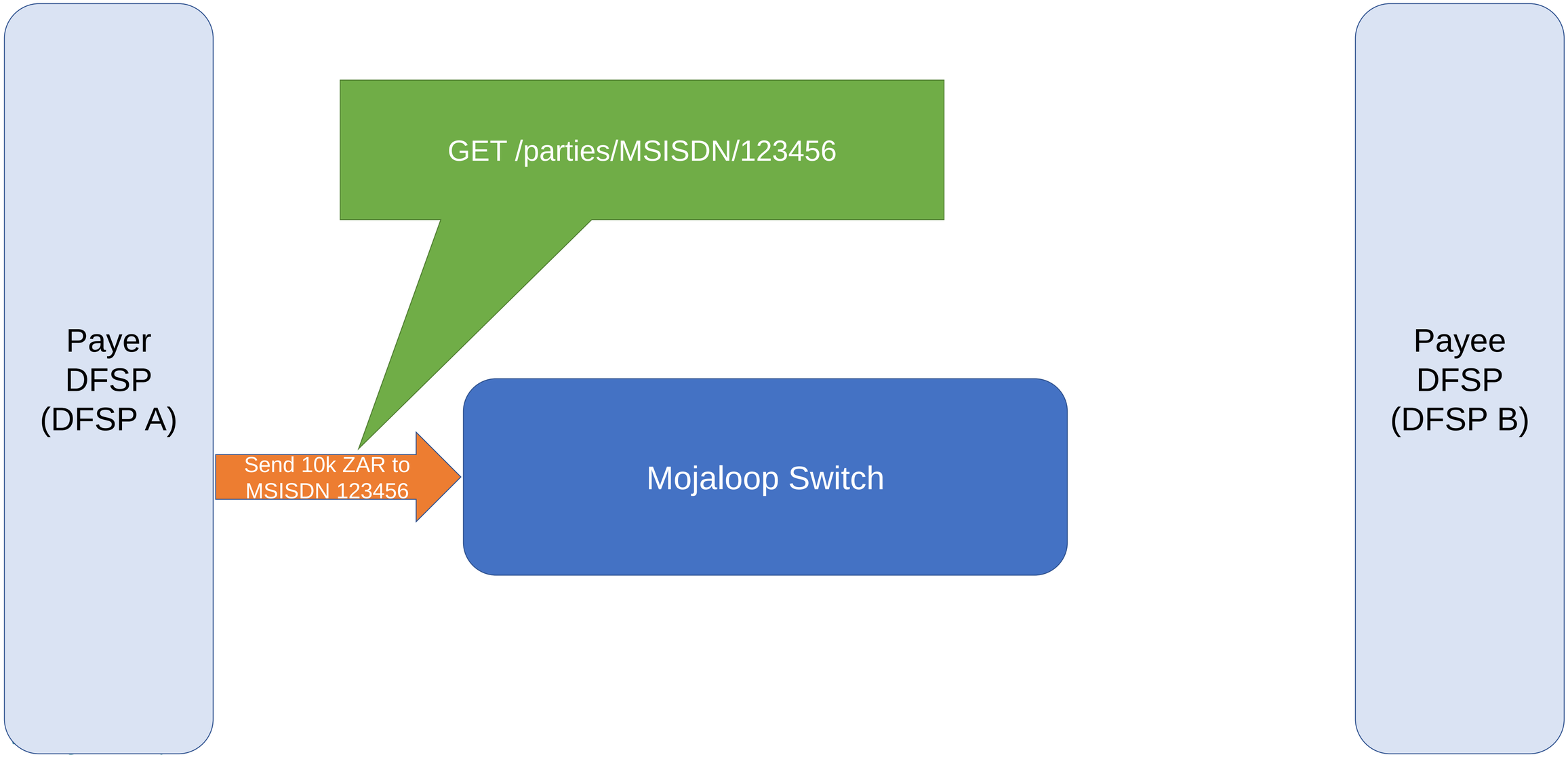
The three stages

- In the *discovery* phase:
  - The payer's DFSP identifies the owner of the identifier to which the payer wants to transfer funds;
  - The payee's DFSP provides information that the payer can use to check that they are sending to the account intended.
- In the *agreement* phase:
  - The payer's DFSP exposes the details of the proposed transaction
  - The payee's DFSP confirms that the payee's account can receive the proposed transfer
  - The payee's DFSP defines the terms under which the transfer will be accepted
  - The payee's DFSP puts a cryptographic lock and an expiry date on the transfer terms
- In the *transfer* phase:
  - The payer's DFSP and the switch reserve funds so that they can't be spent twice.
  - The payee's DFSP confirms that the transfer conforms with the terms agreed.
  - The payee's DFSP provides the switch and the payer's DFSP with a cryptographic key which confirms that the transfer has completed.
  - The payee's DFSP completes the transfer to the payee's account
  - The payer's DFSP removes the funds from the payer's account
  - The switch records the transfer for use by the settlement service

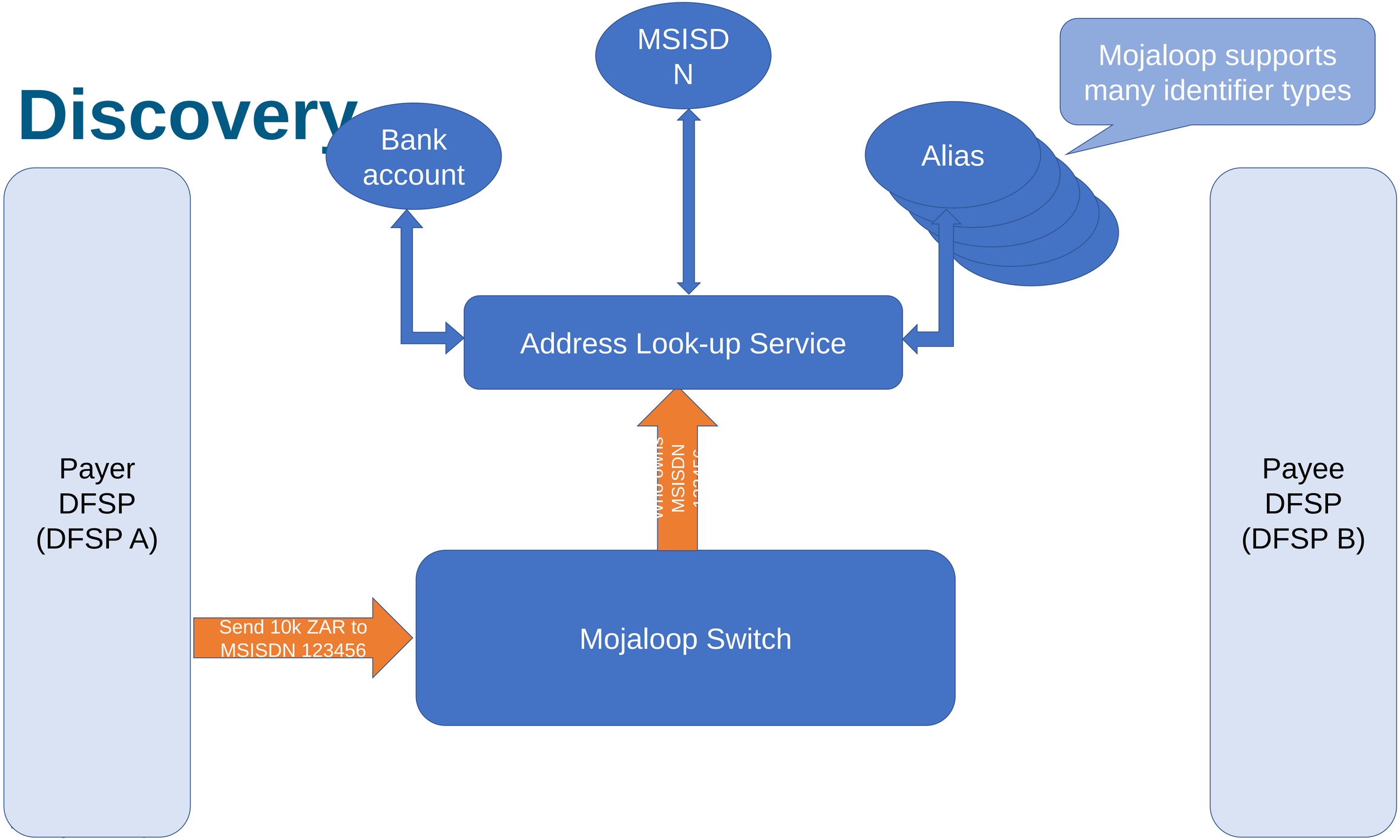
The transfer model



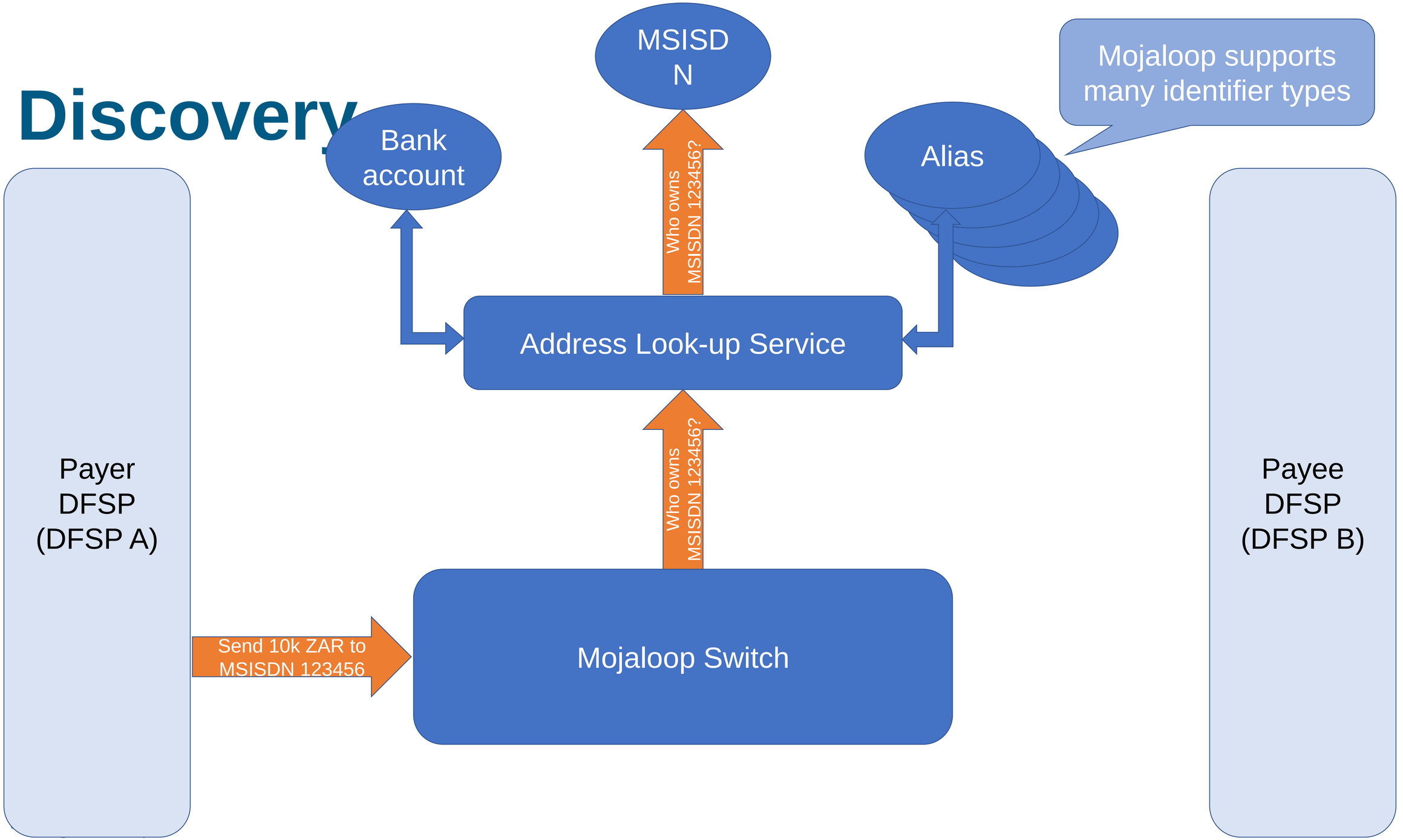
Discovery


Payer
DFSP
(DFSP A)
GET /parties/MSISDN/123456
Send 10k ZAR to
MSISDN 123456
Mojaloop Switch
Payee
DFSP
(DFSP B)

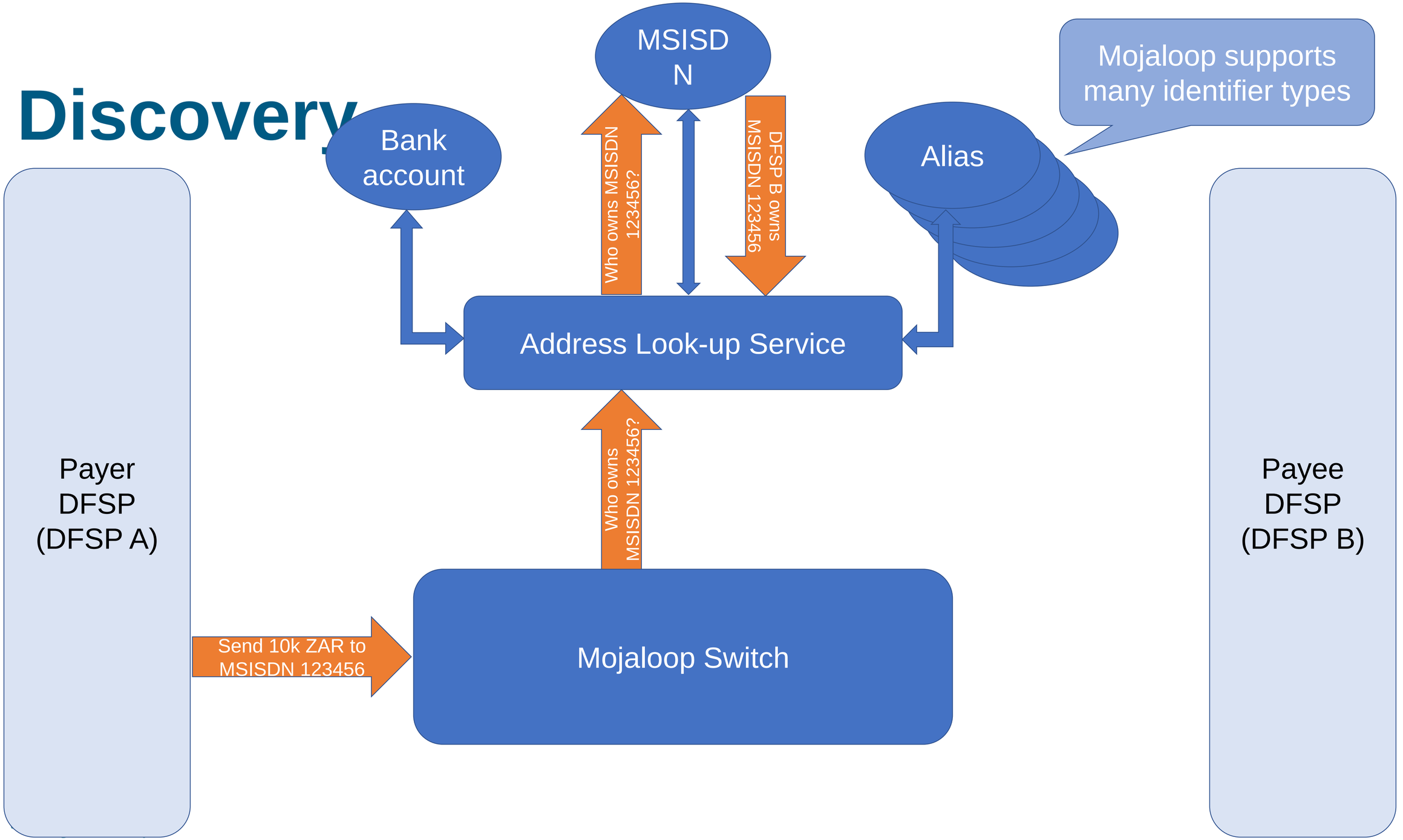
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Address Look-up Service
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Who owns MSISDN
Send 10k ZAR to MSISDN 123456
Mojaloop Switch

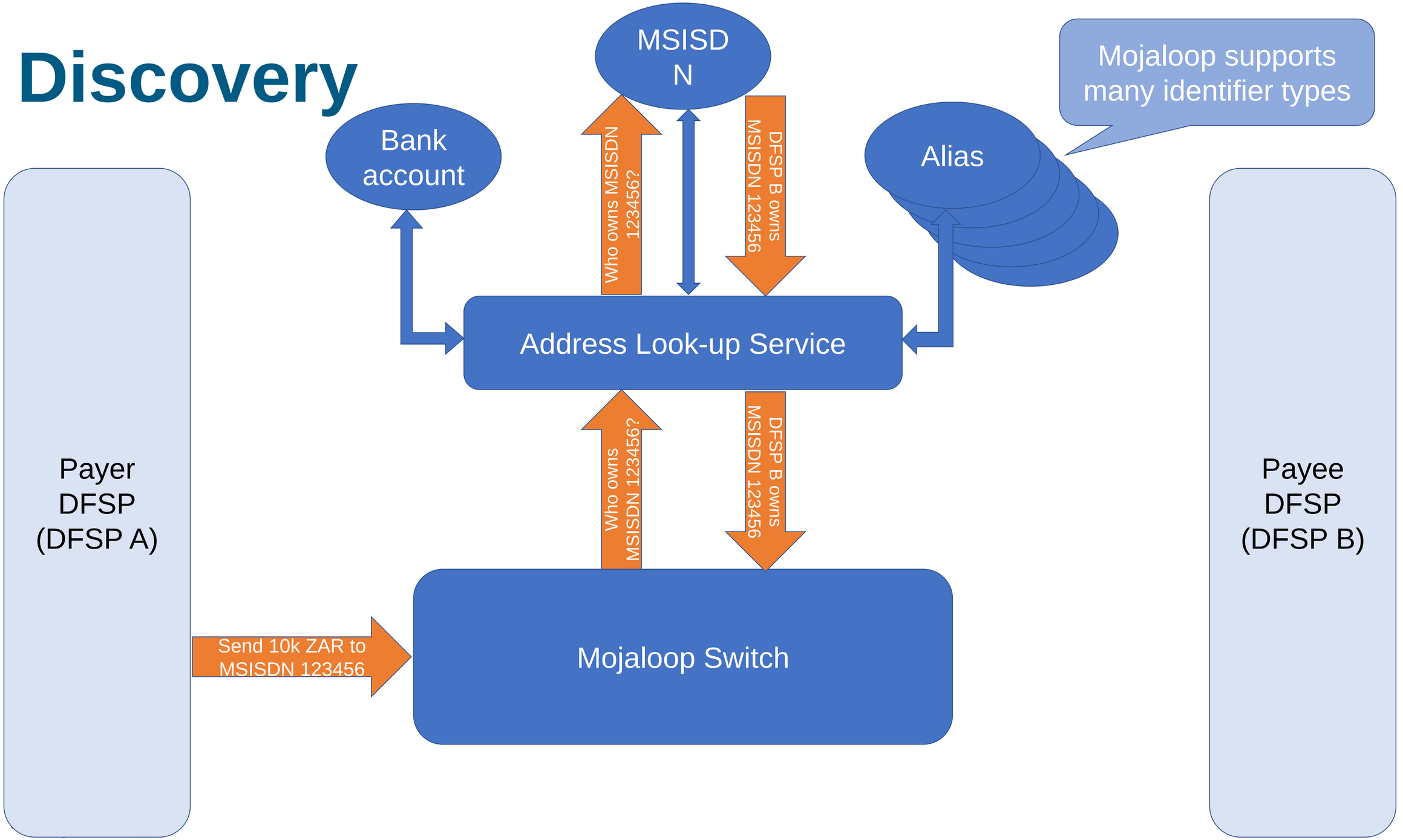
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
Address Look-up Service
Who owns MSISDN 123456?
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Send 10k ZAR to MSISDN 123456
Mojaloop Switch

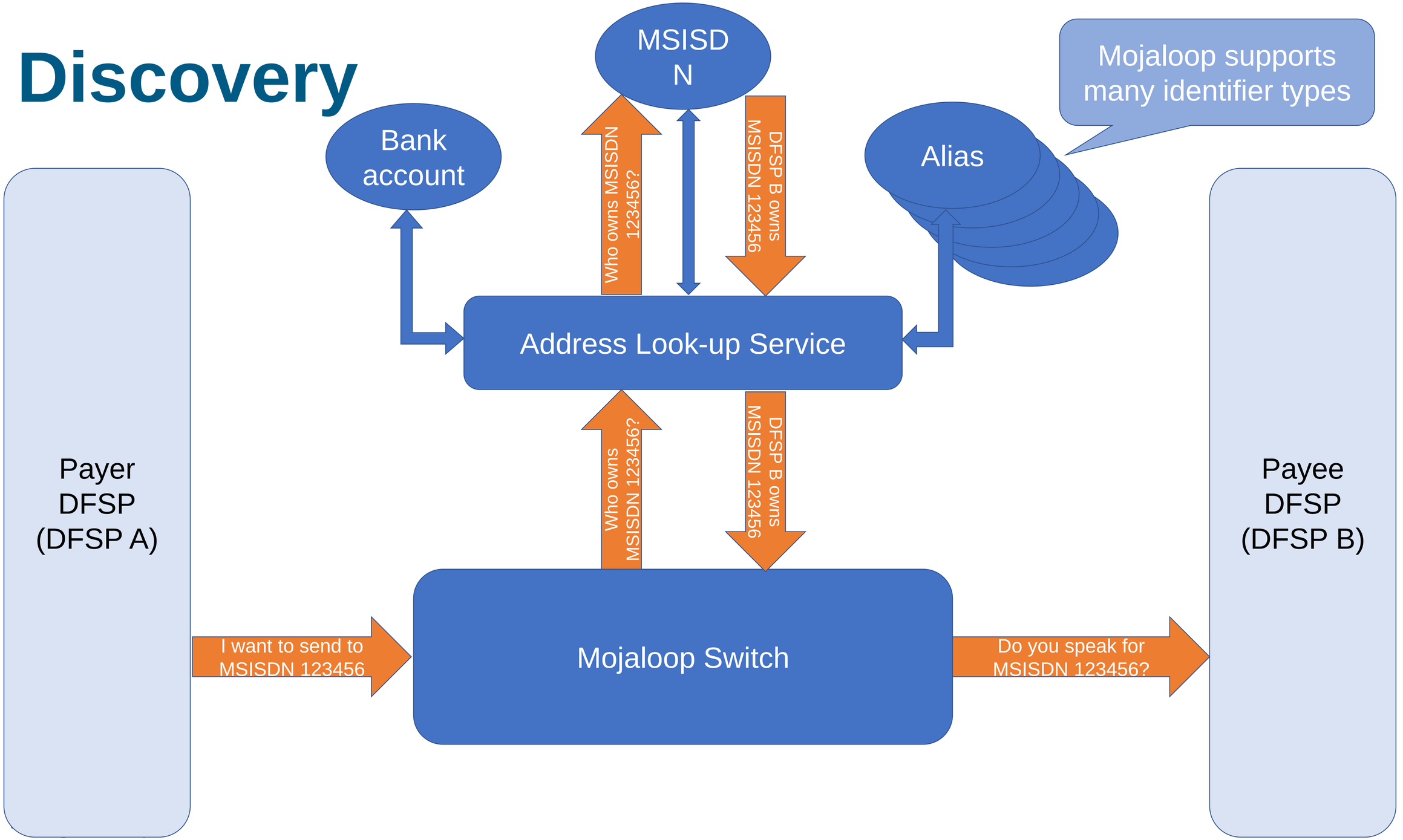
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Send 10k ZAR to MSISDN 123456
Mojaloop Switch

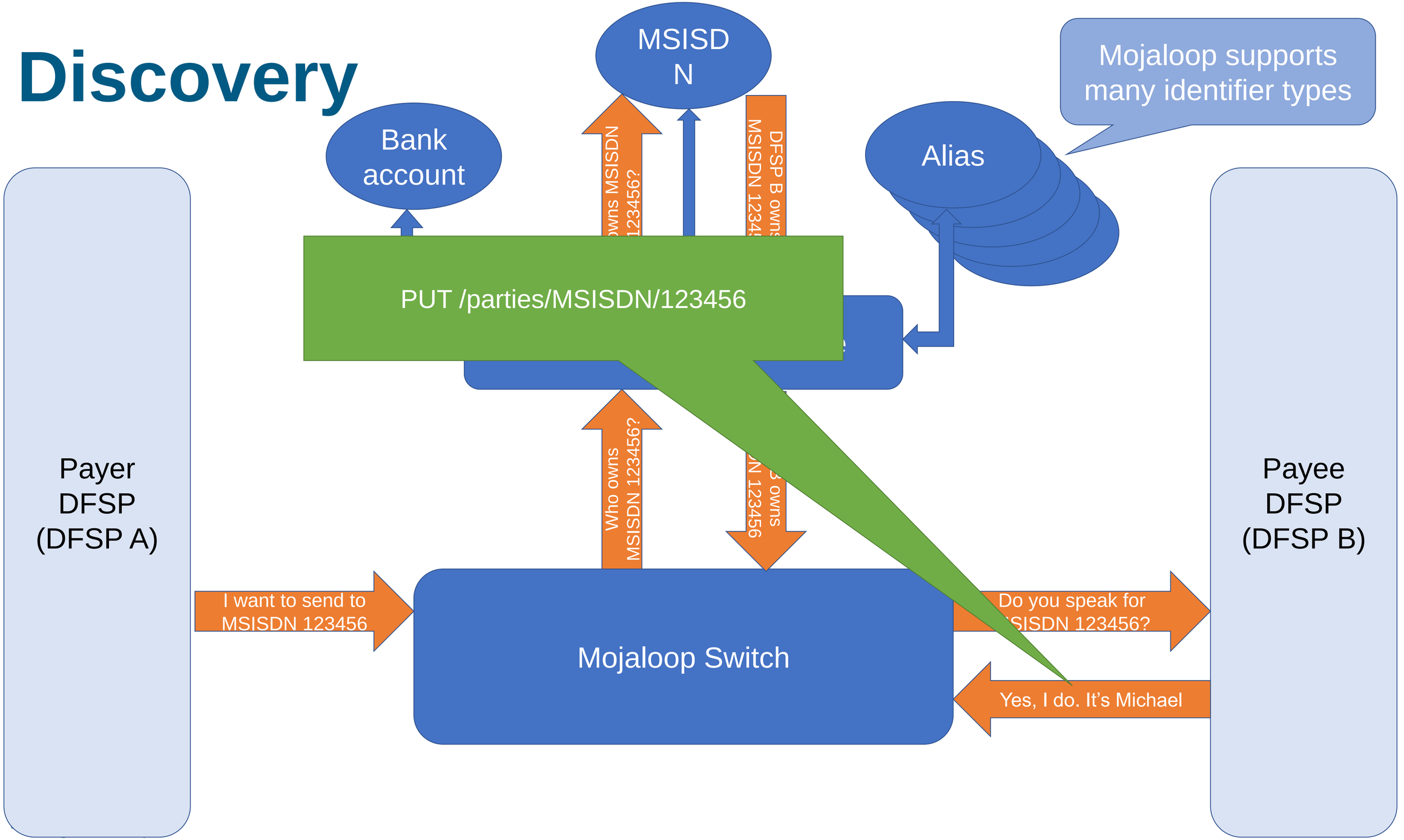
Discovery


MSISD N
Bank account
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Alias
Mojaloop supports many identifier types
Address Look-up Service
Payer DFSP (DFSP A)
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Payee DFSP (DFSP B)
Send 10k ZAR to MSISDN 123456
Mojaloop Switch

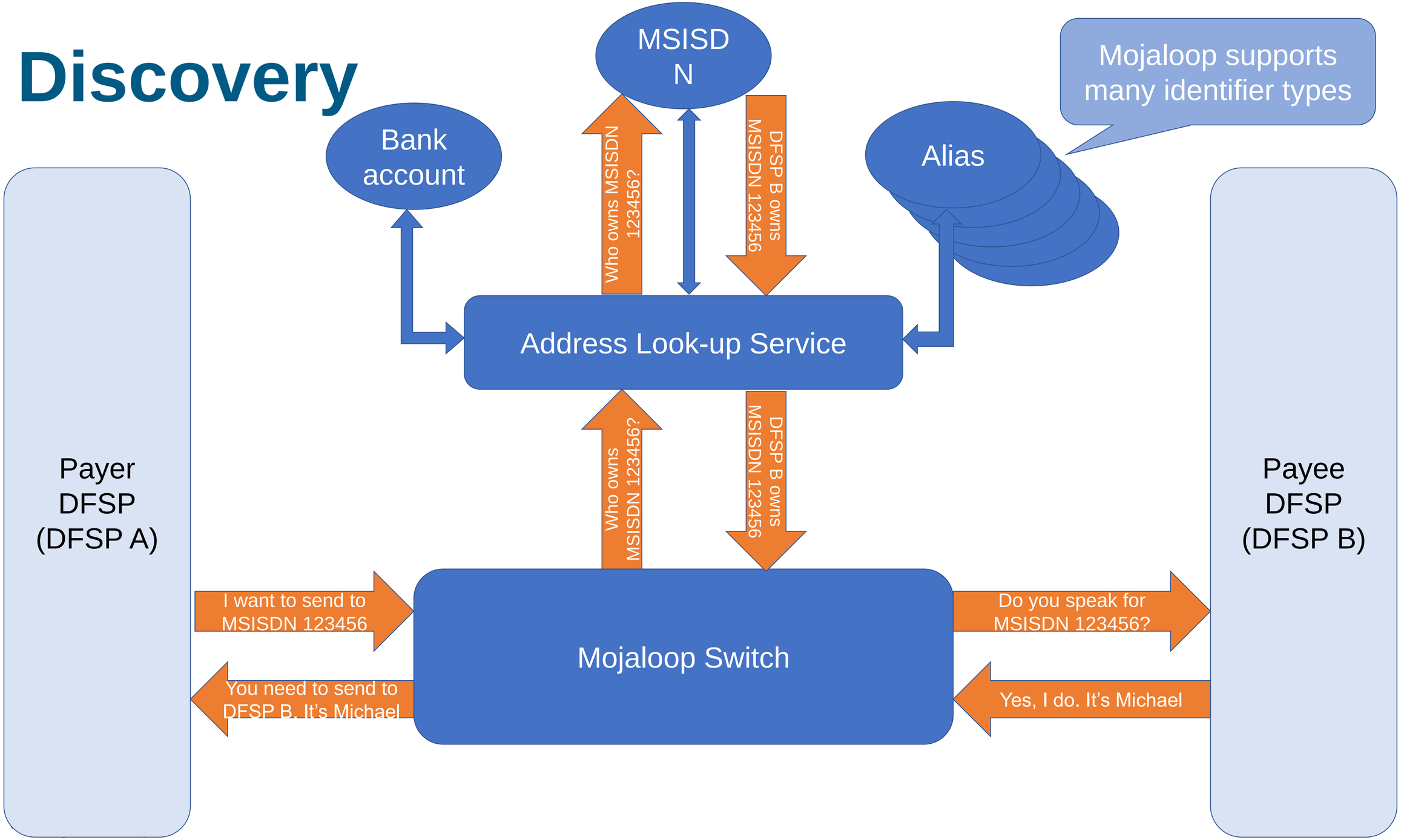
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Payer DFSP (DFSP A)
I want to send to MSISDN 123456
Mojaloop Switch
Do you speak for MSISDN 123456?
Payee DFSP (DFSP B)

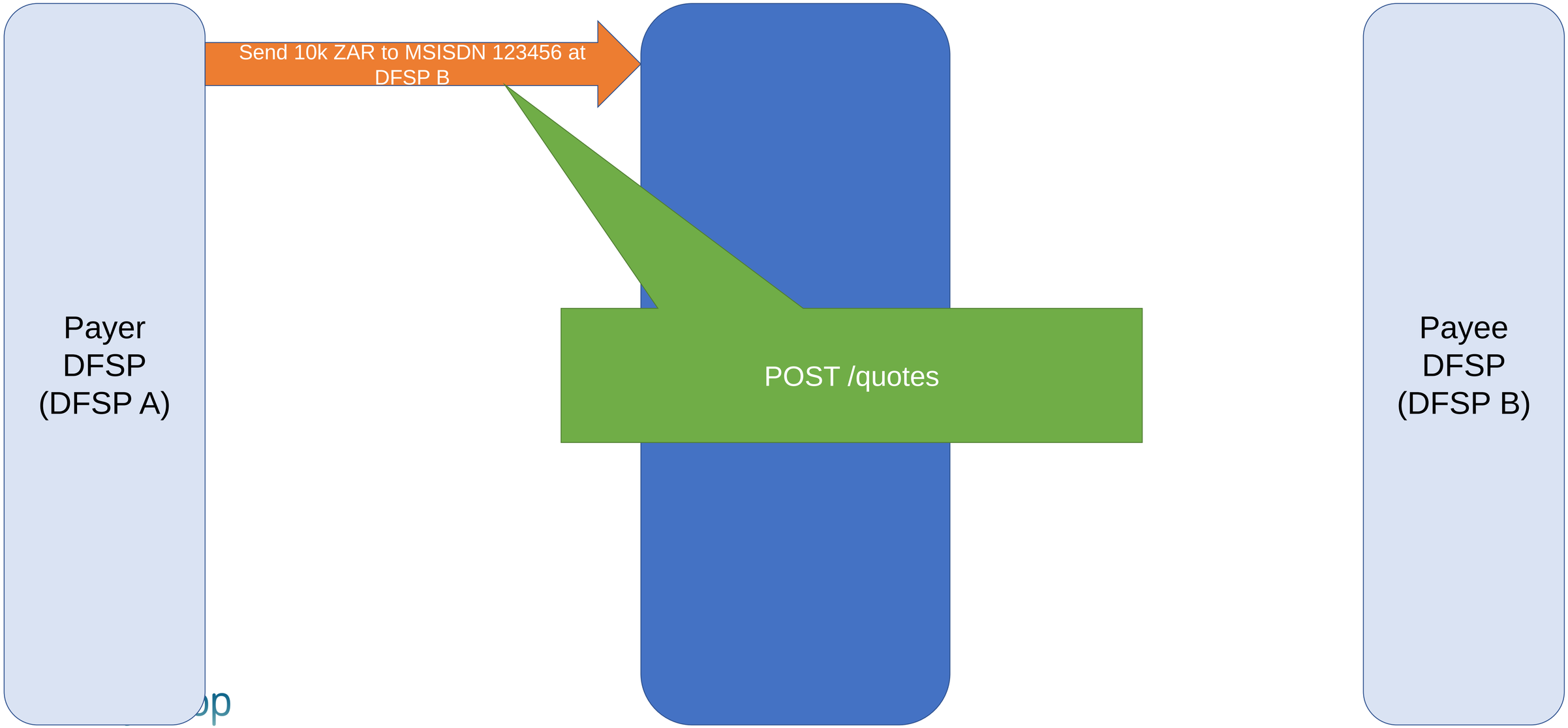
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
PUT /parties/MSISDN/123456
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
I want to send to MSISDN 123456
Do you speak for MSISDN 123456?
Yes, I do. It's Michael
Mojaloop Switch

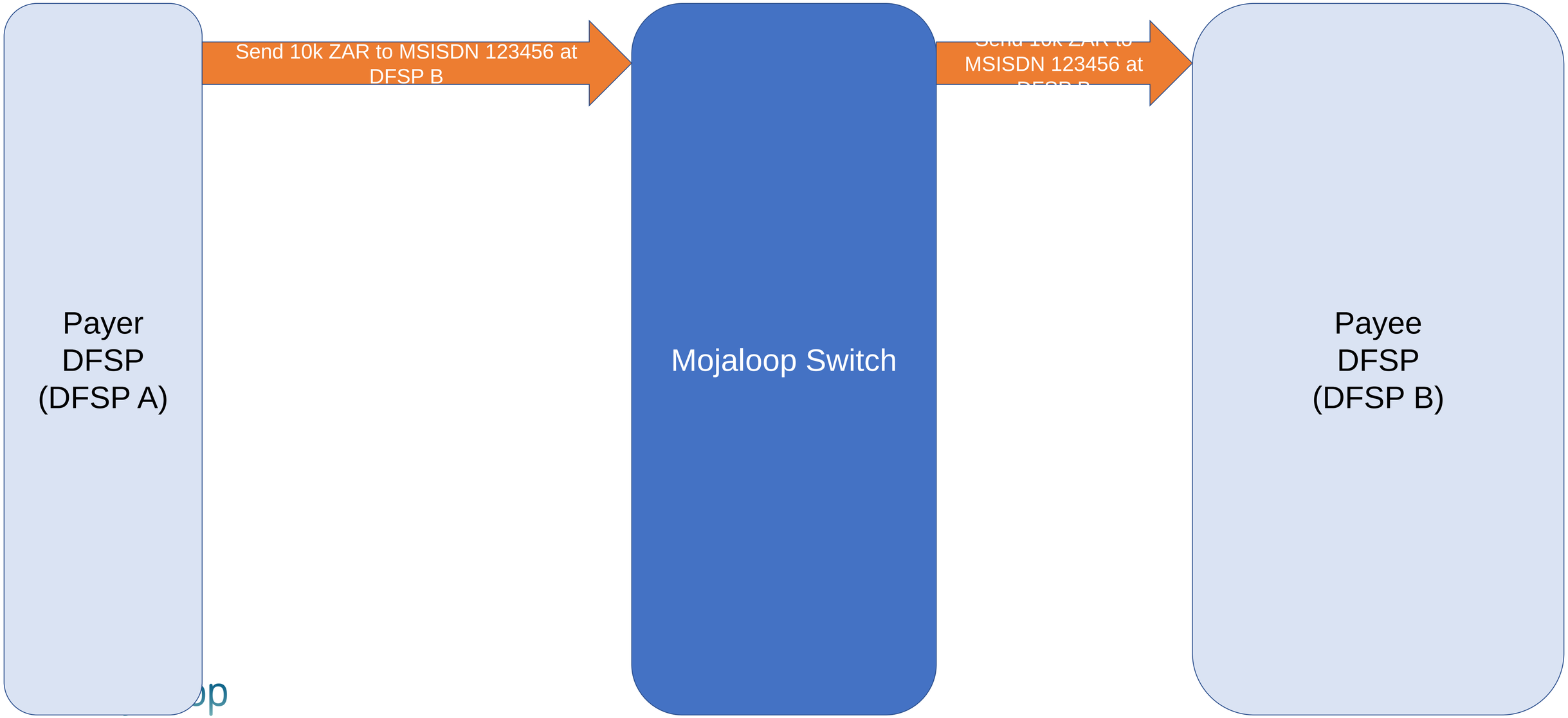
Discovery


MSISDN
Mojaloop supports many identifier types
Bank account
Alias
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
Address Look-up Service
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Who owns MSISDN 123456?
DFSP B owns MSISDN 123456
I want to send to MSISDN 123456
Do you speak for MSISDN 123456?
Mojaloop Switch
You need to send to DFSP B. It's Michael
Yes, I do. It's Michael

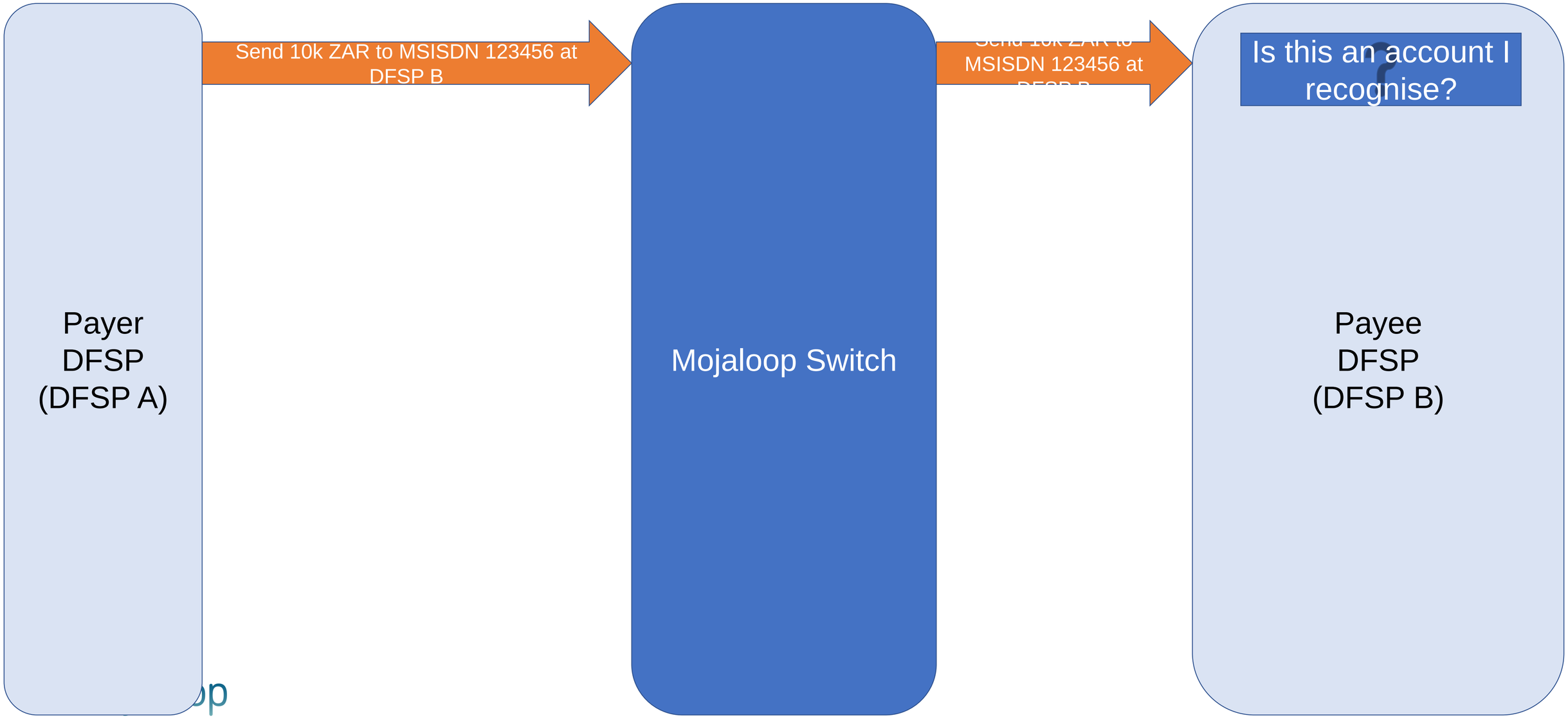
Agreement


Send 10k ZAR to MSISDN 123456 at DFSP B
POST /quotes
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)

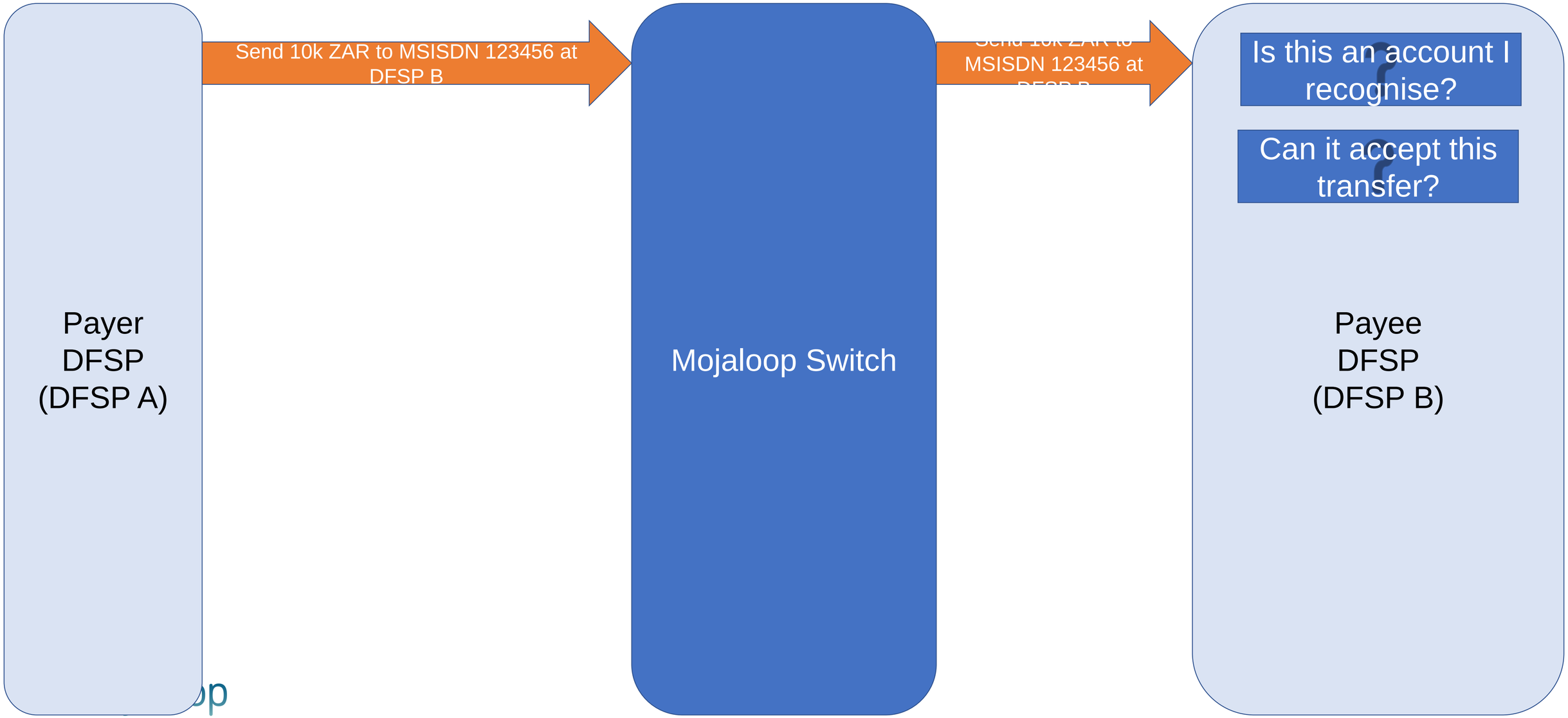
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
MSISDN 123456 at
Payee
DFSP
(DFSP B)

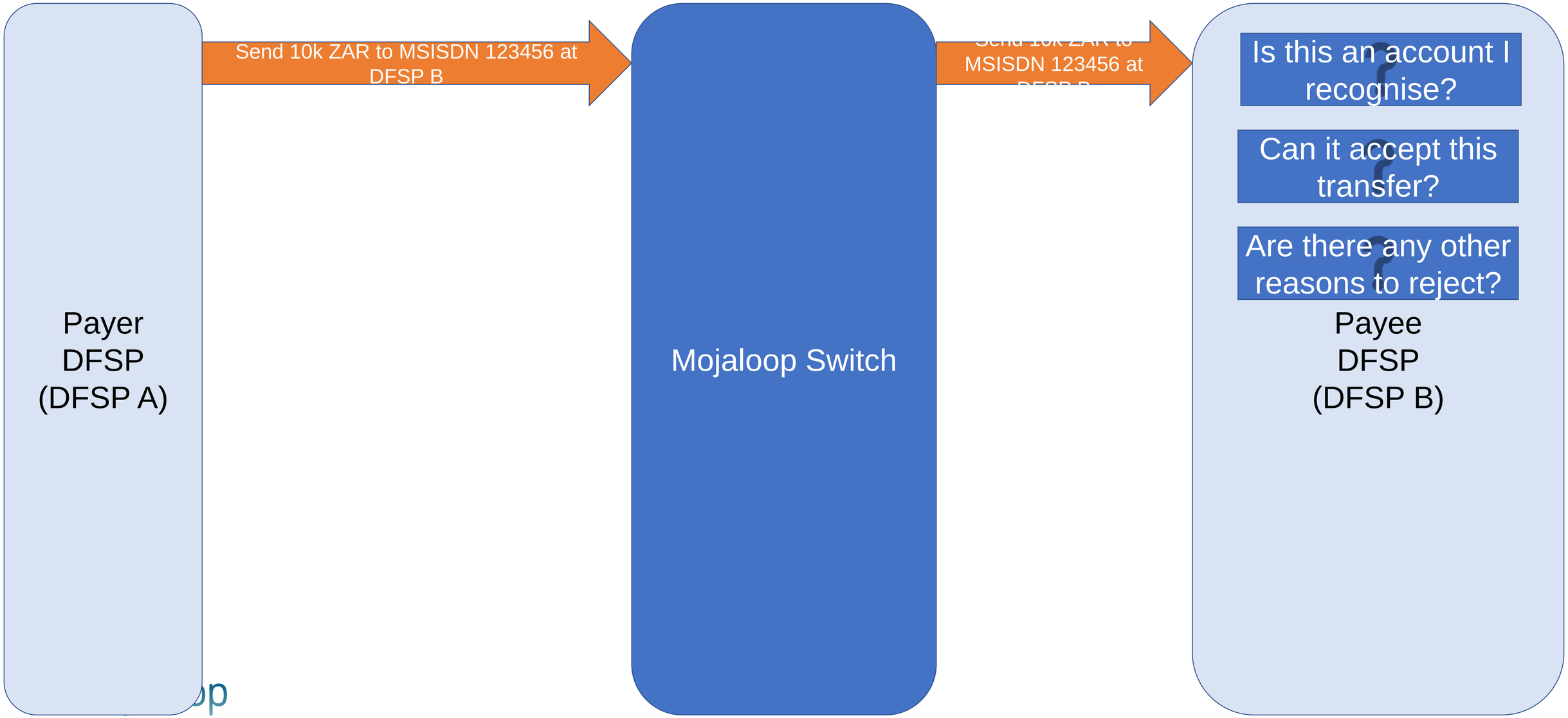
Agreement


Send 10k ZAR to MSISDN 123456 at DFSP B
Send 10k ZAR to MSISDN 123456 at
Is this an account I recognise?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

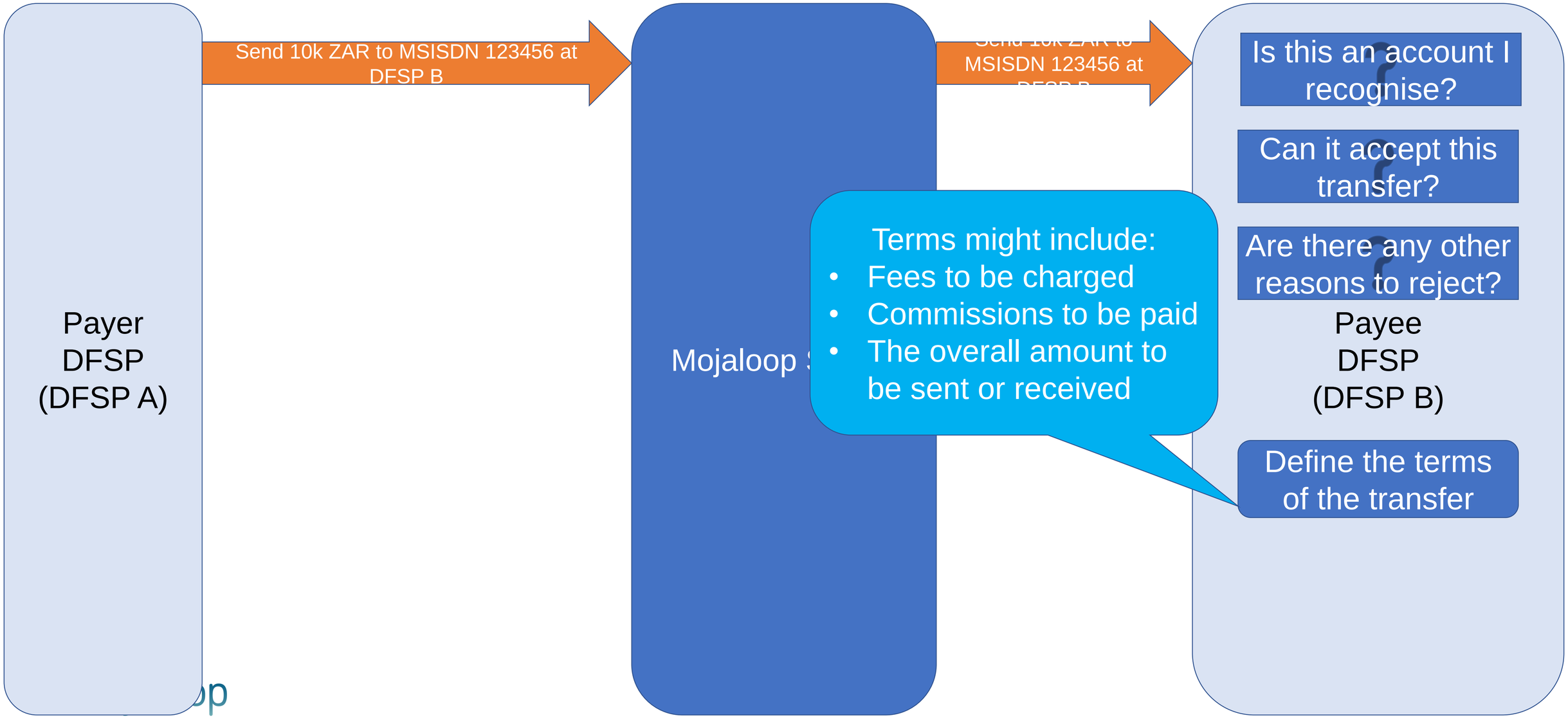
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
Send 10k ZAR to MSISDN 123456 at
Is this an account I recognise?
Can it accept this transfer?
Payee
DFSP
(DFSP B)

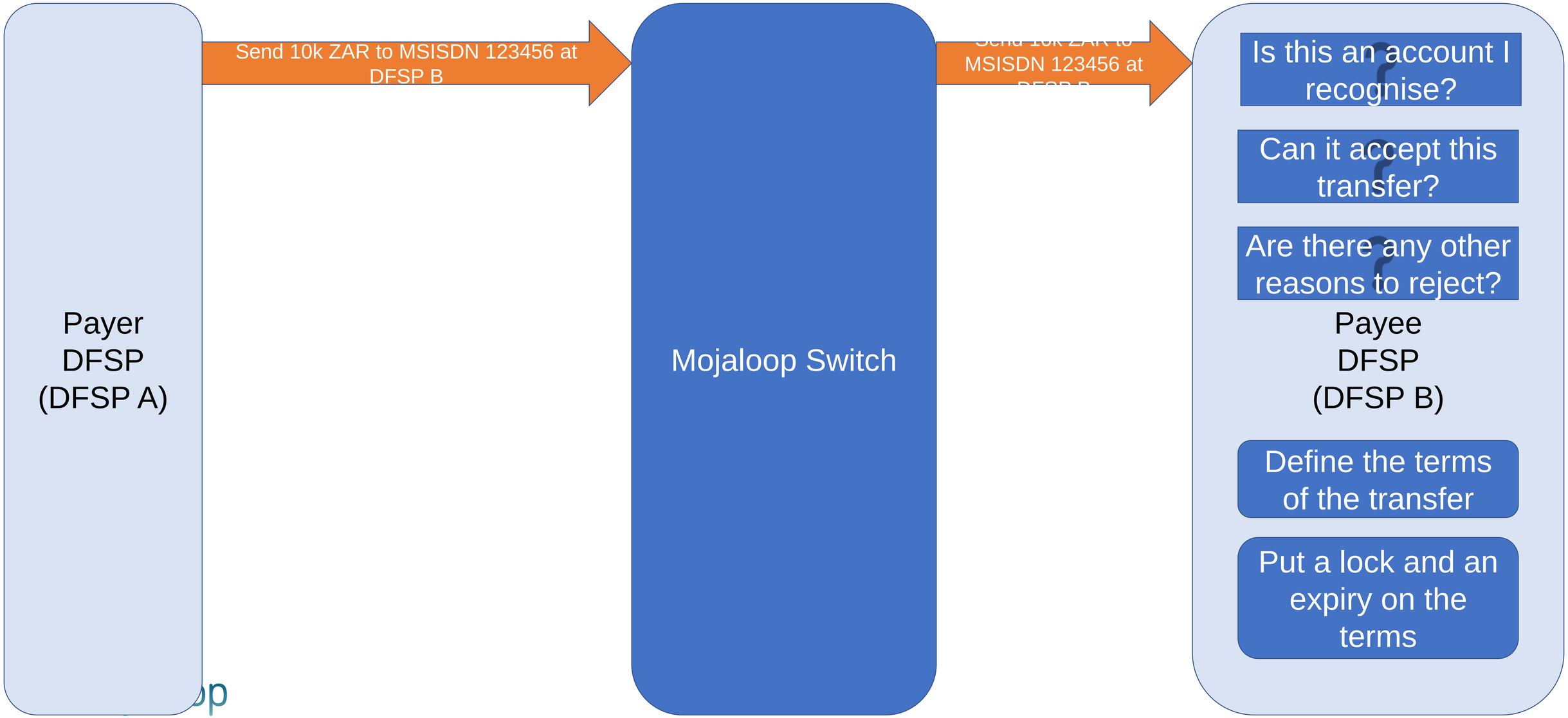
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
Send 10k ZAR to MSISDN 123456 at
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)

Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop
Send 10k ZAR to MSISDN 123456 at
Terms might include:
• Fees to be charged
• Commissions to be paid
• The overall amount to be sent or received
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)
Define the terms of the transfer

Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
Send 10k ZAR to MSISDN 123456 at
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)
Define the terms of the transfer
Put a lock and an expiry on the terms

Mojaloop security considerations

- Mojaloop messages are exchanged over the open internet
- They are protected by three separate mechanisms
- Each mechanism manages a different level of security

Mechanism 1: MTLS

- Mojaloop uses certificate-based MTLS.
- Each message transmitted is encrypted using a shared key.
- It can only be decrypted by another organisation in possession of the shared key.
- This applies to all Mojaloop messages

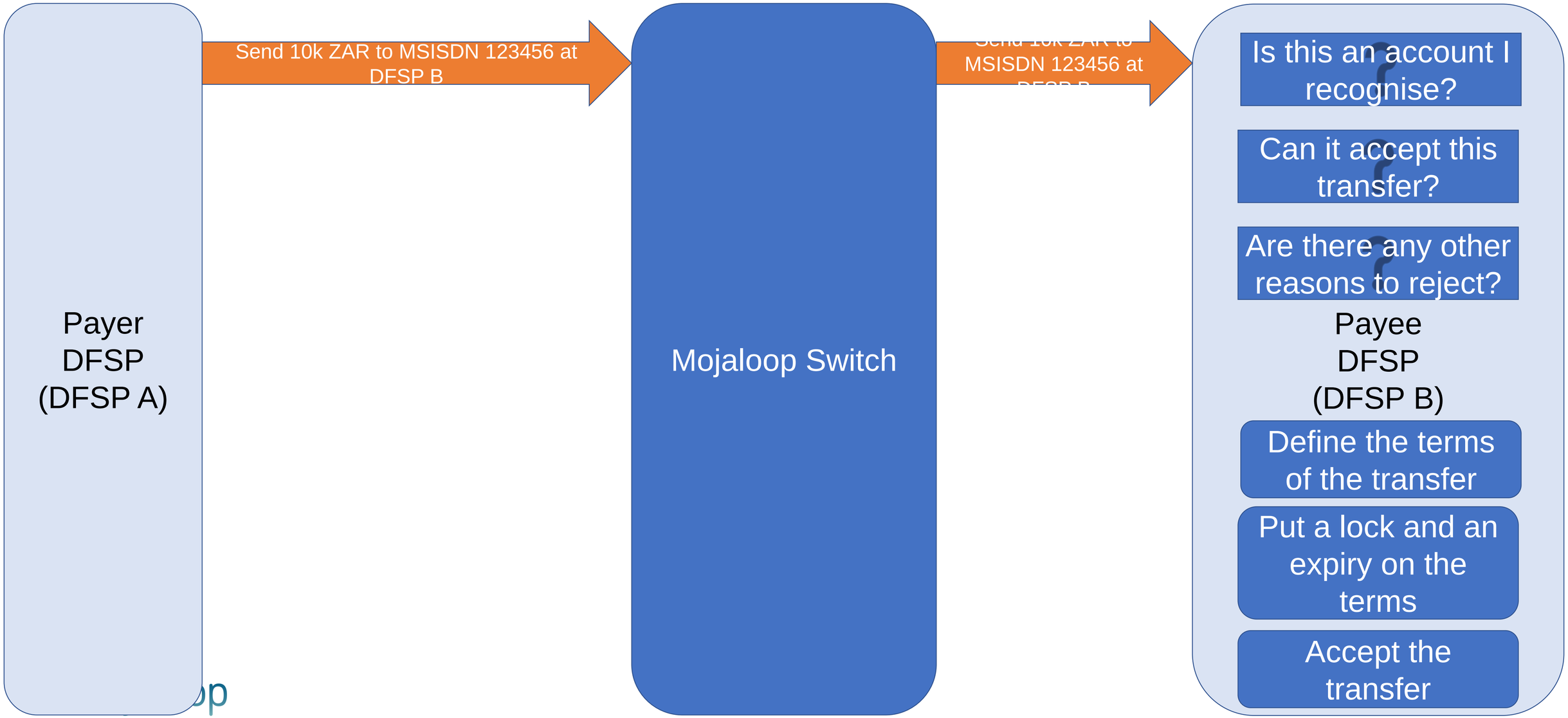
Mechanism 2: Non-repudiability

- The standard for non-repudiability is JWS
- The sender of a message signs its content using a private key.
  - Key fields of the header are signed
  - The entire body of the message is signed
- The signature is transmitted as part of the message header
- The recipient compares the signature with a signature generated using the sender's public key, and confirms that they match.
- All Mojaloop messages are signed *except for* the original discovery request.

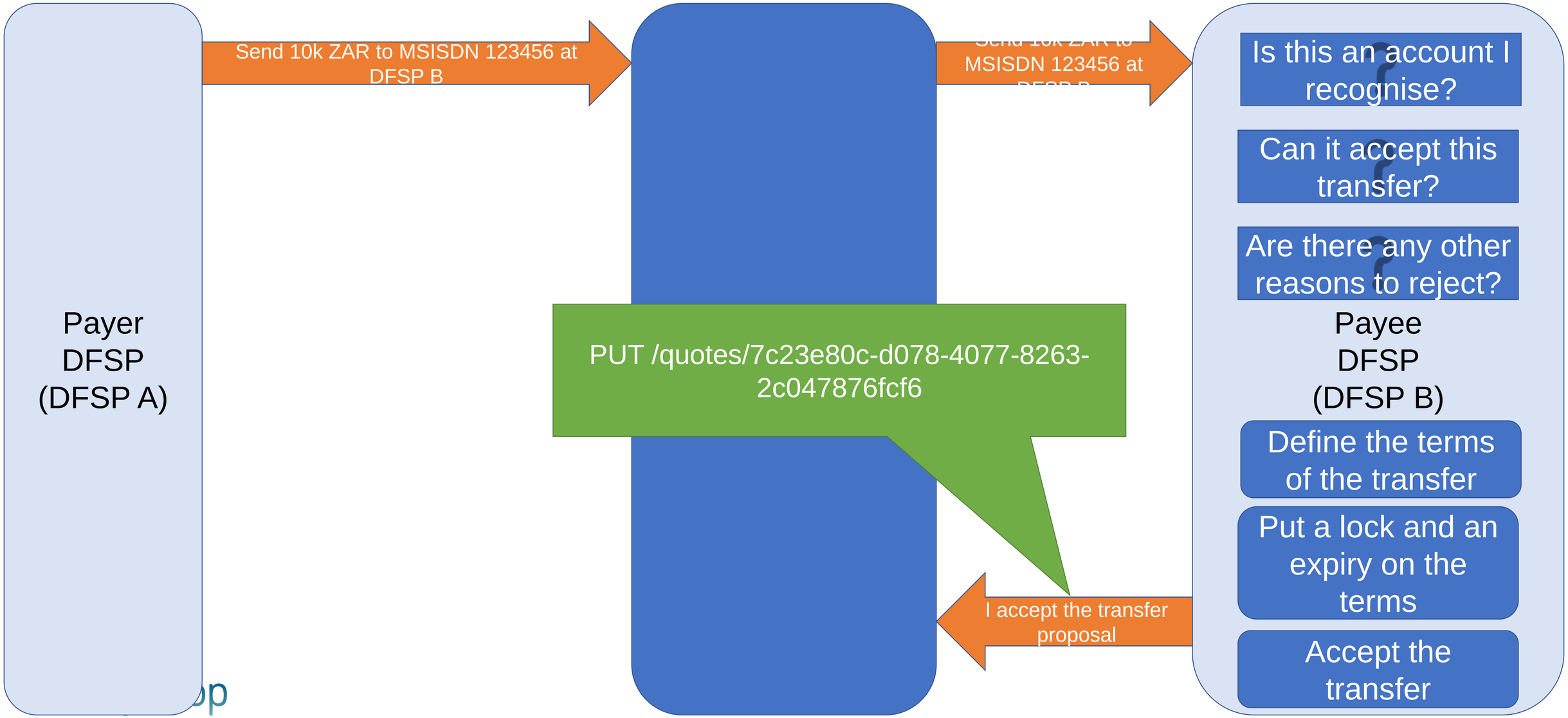
Mechanism 3: two-phase commit

- Uses the Interledger Protocol (ILP)
- The payee DFSP signs the agreed content of the transfer using a private key.
- It passes the resulting signature (the *fulfilment*) through a public one-way hash
- The hashed result (the *condition*) is returned to the payer DFSP.
- The payer DFSP and the switch retain the condition as they reserve funds during the transfer process.
- When the payee DFSP accepts the transfer, it returns the fulfilment to the switch and the payer DFSP.
- They can then pass the fulfilment through the same one-way hash and check the result.
- Since the response is verifiably from the payee (thanks to non-repudiability,) the other parties can be confident that the transfer has been completed successfully

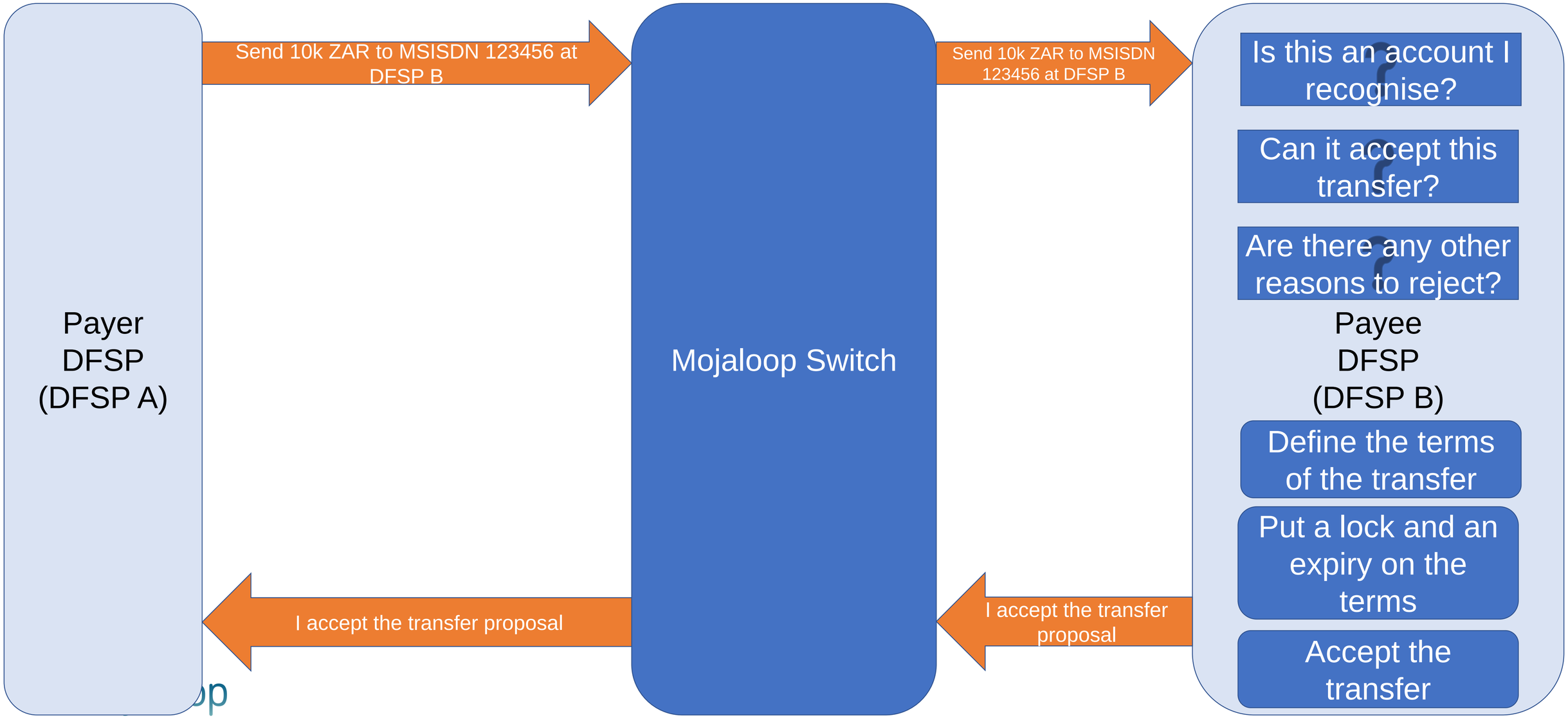
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
Send 10k ZAR to MSISDN 123456 at
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)
Define the terms of the transfer
Put a lock and an expiry on the terms
Accept the transfer

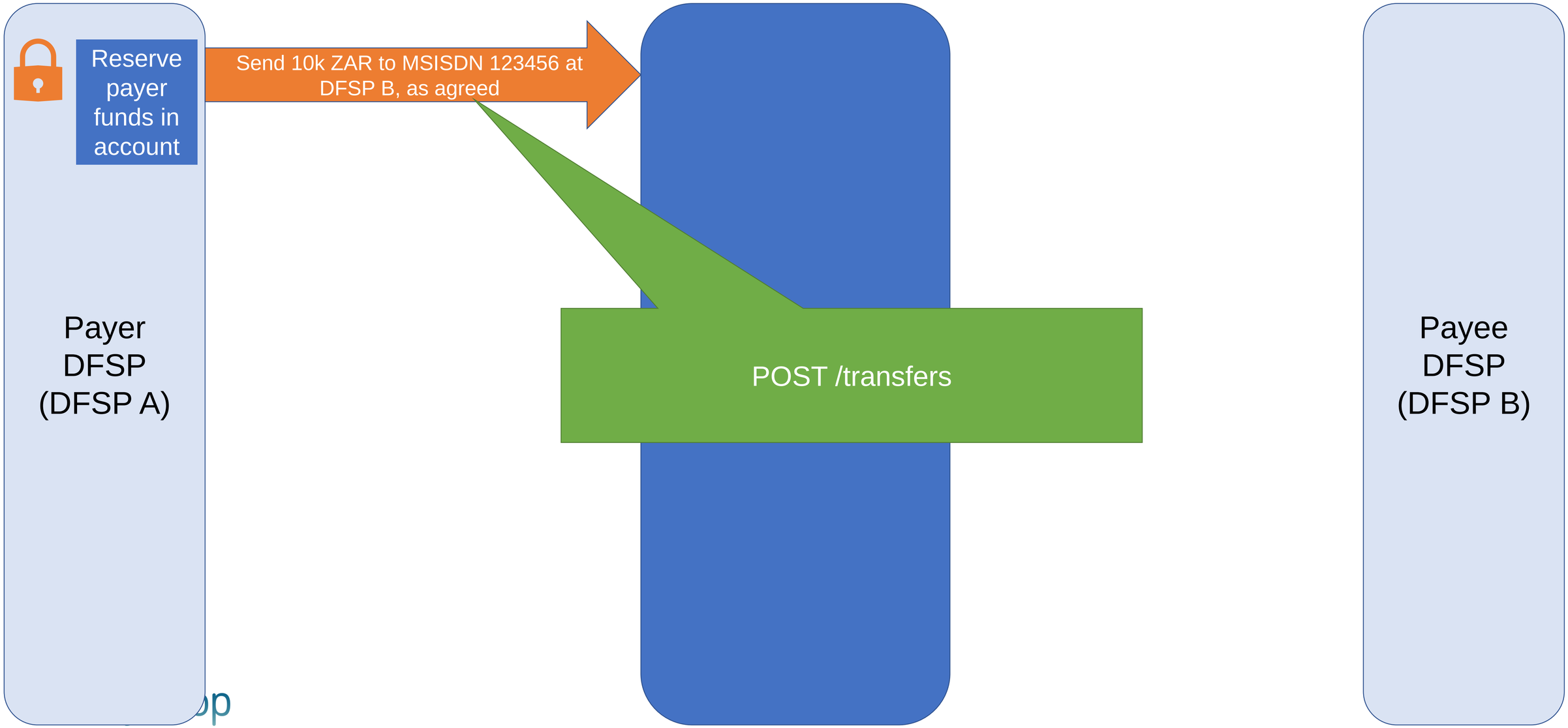
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Send 10k ZAR to MSISDN 123456 at
PUT /quotes/7c23e80c-d078-4077-8263-2c047876fcf6
I accept the transfer proposal
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)
Define the terms of the transfer
Put a lock and an expiry on the terms
Accept the transfer

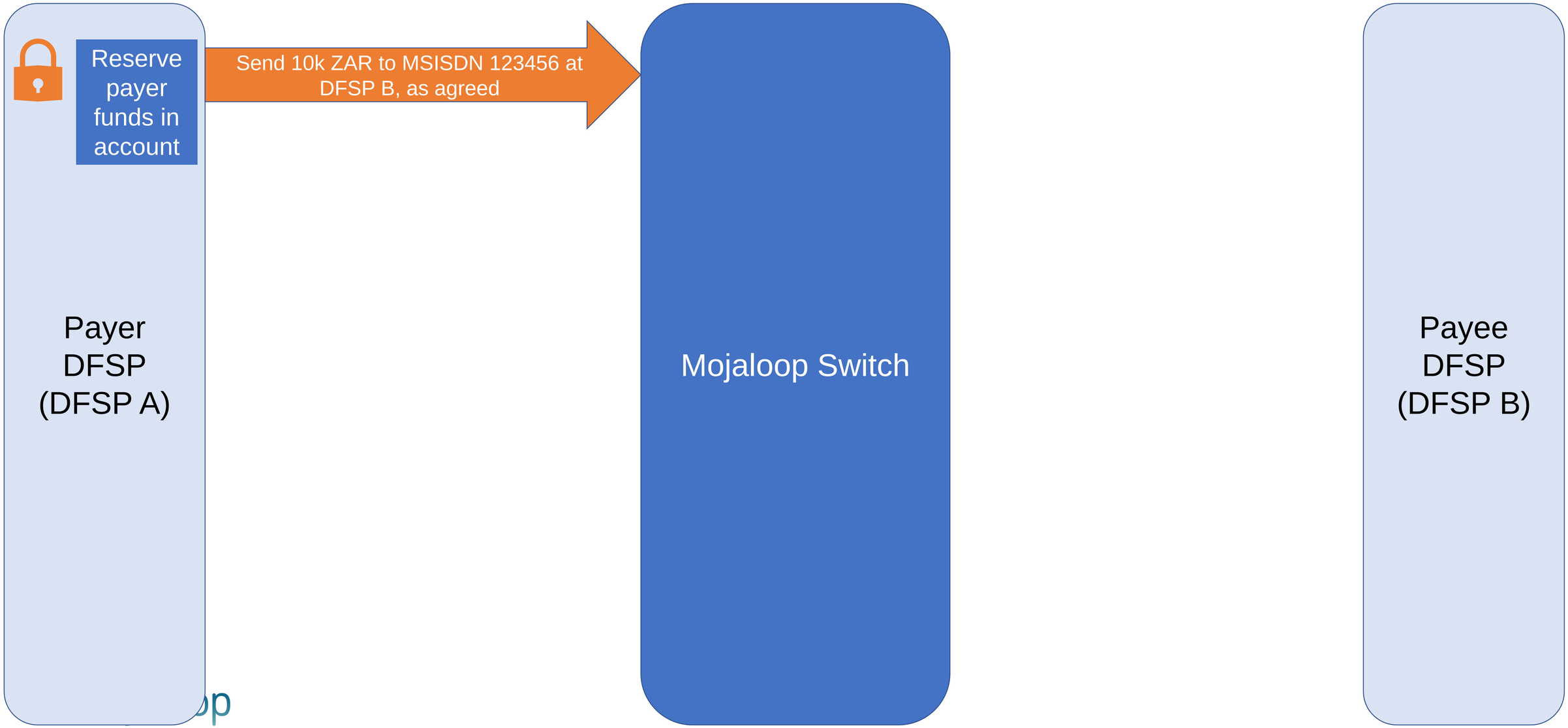
Agreement


Payer
DFSP
(DFSP A)
Send 10k ZAR to MSISDN 123456 at DFSP B
Mojaloop Switch
Send 10k ZAR to MSISDN 123456 at DFSP B
Is this an account I recognise?
Can it accept this transfer?
Are there any other reasons to reject?
Payee
DFSP
(DFSP B)
Define the terms of the transfer
Put a lock and an expiry on the terms
Accept the transfer
I accept the transfer proposal
I accept the transfer proposal

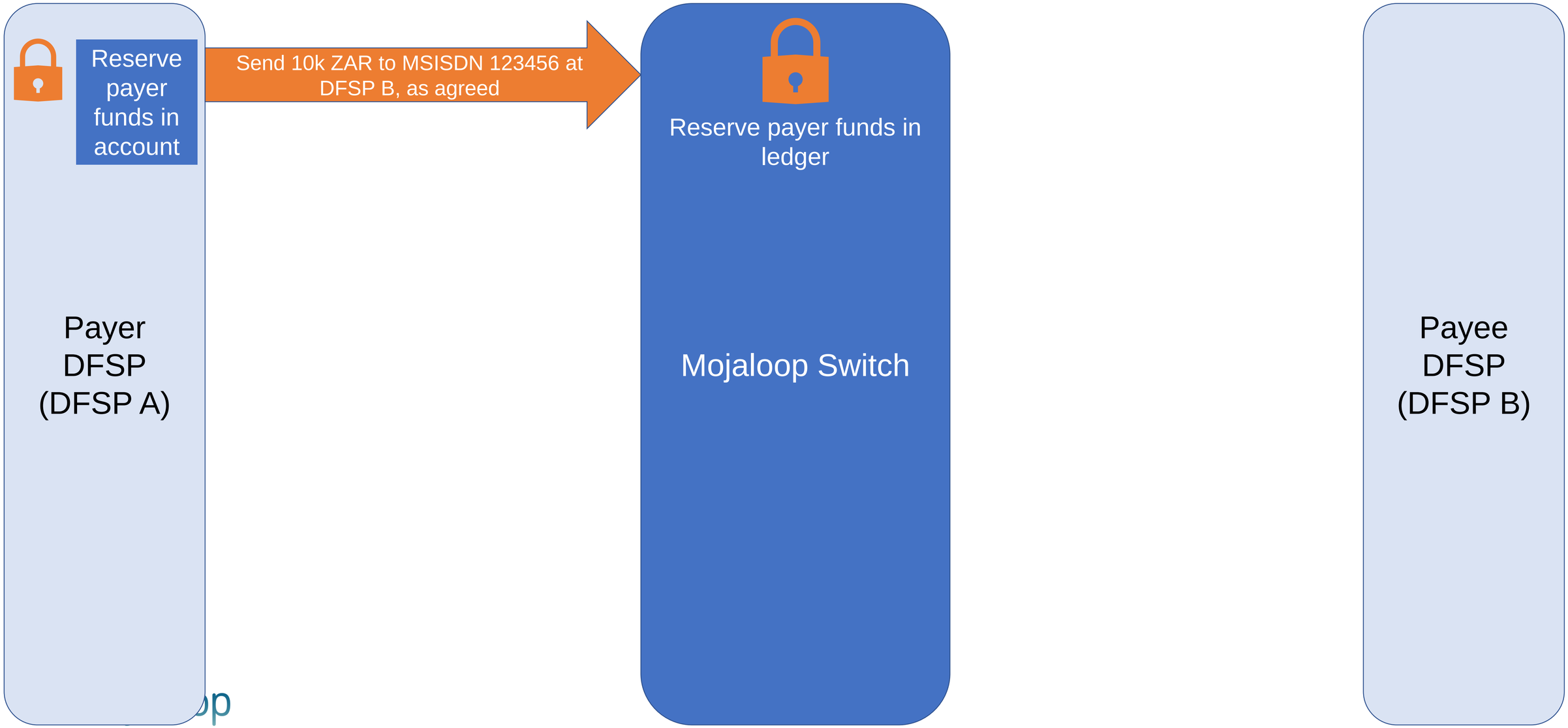
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
POST /transfers
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)

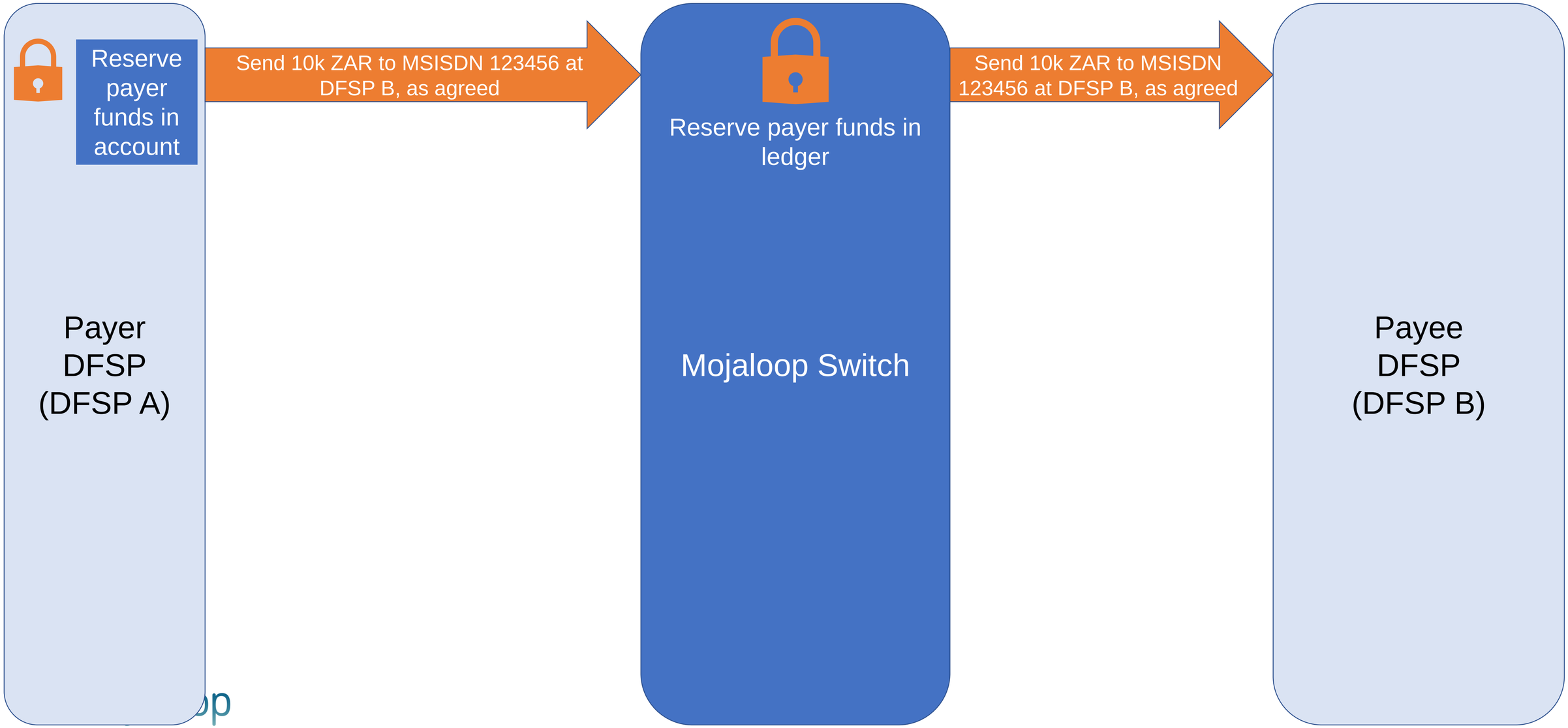
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

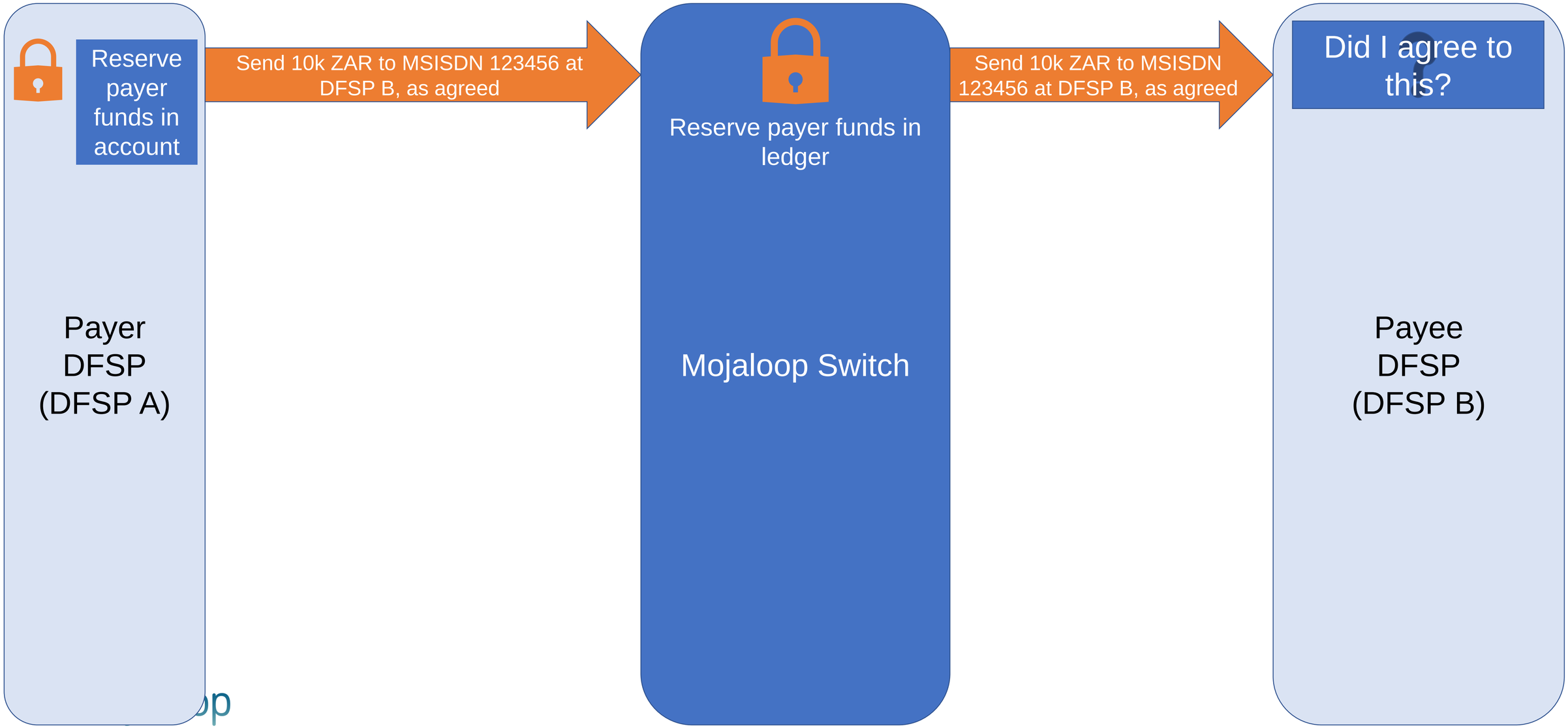
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

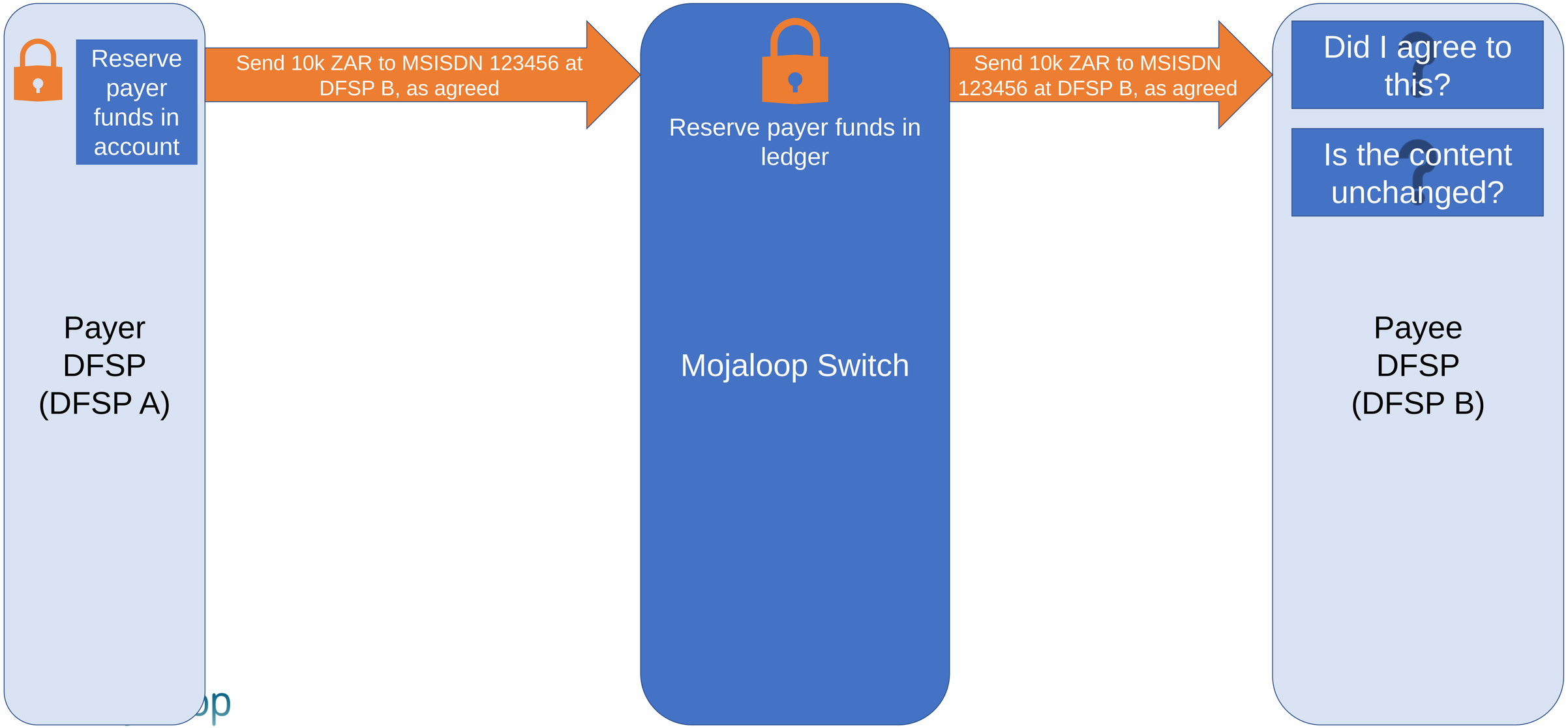
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

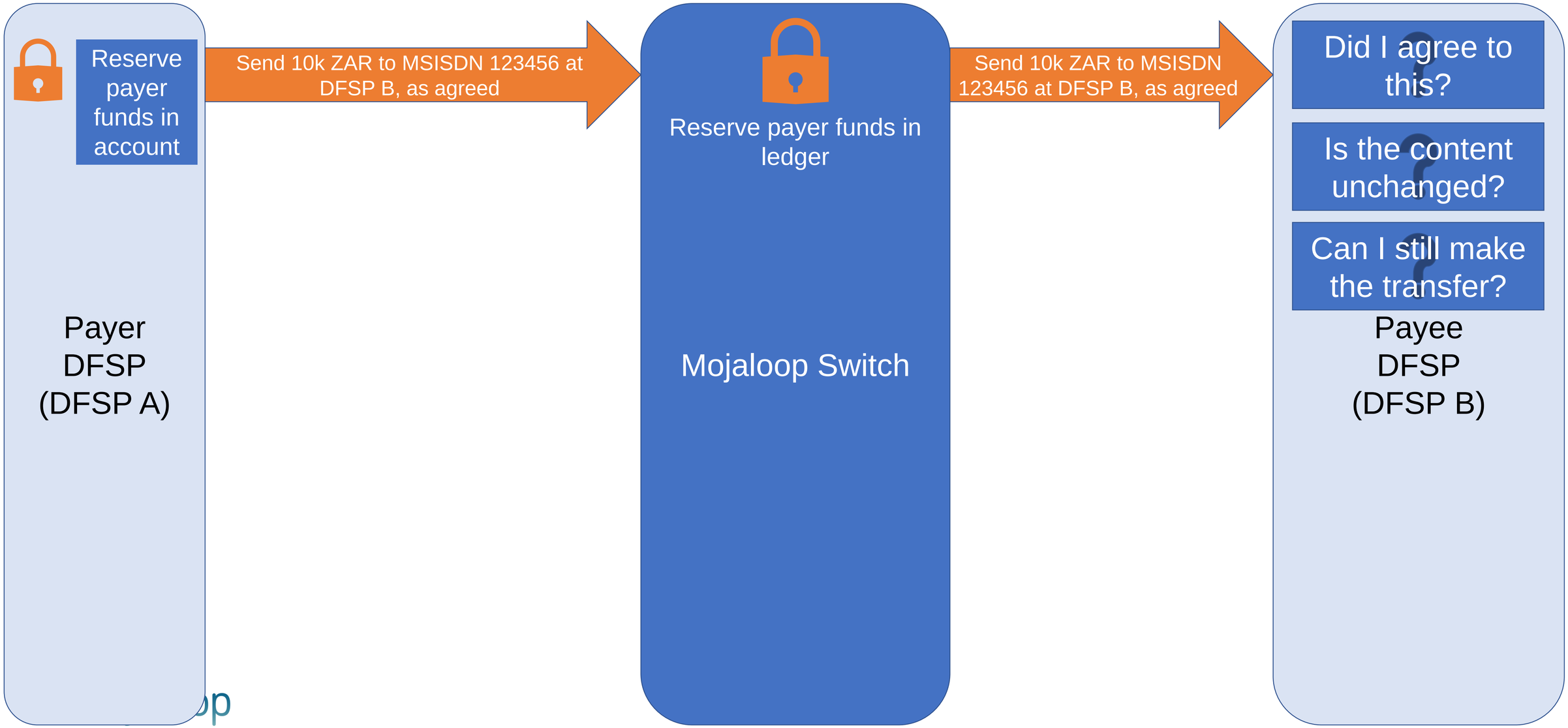
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

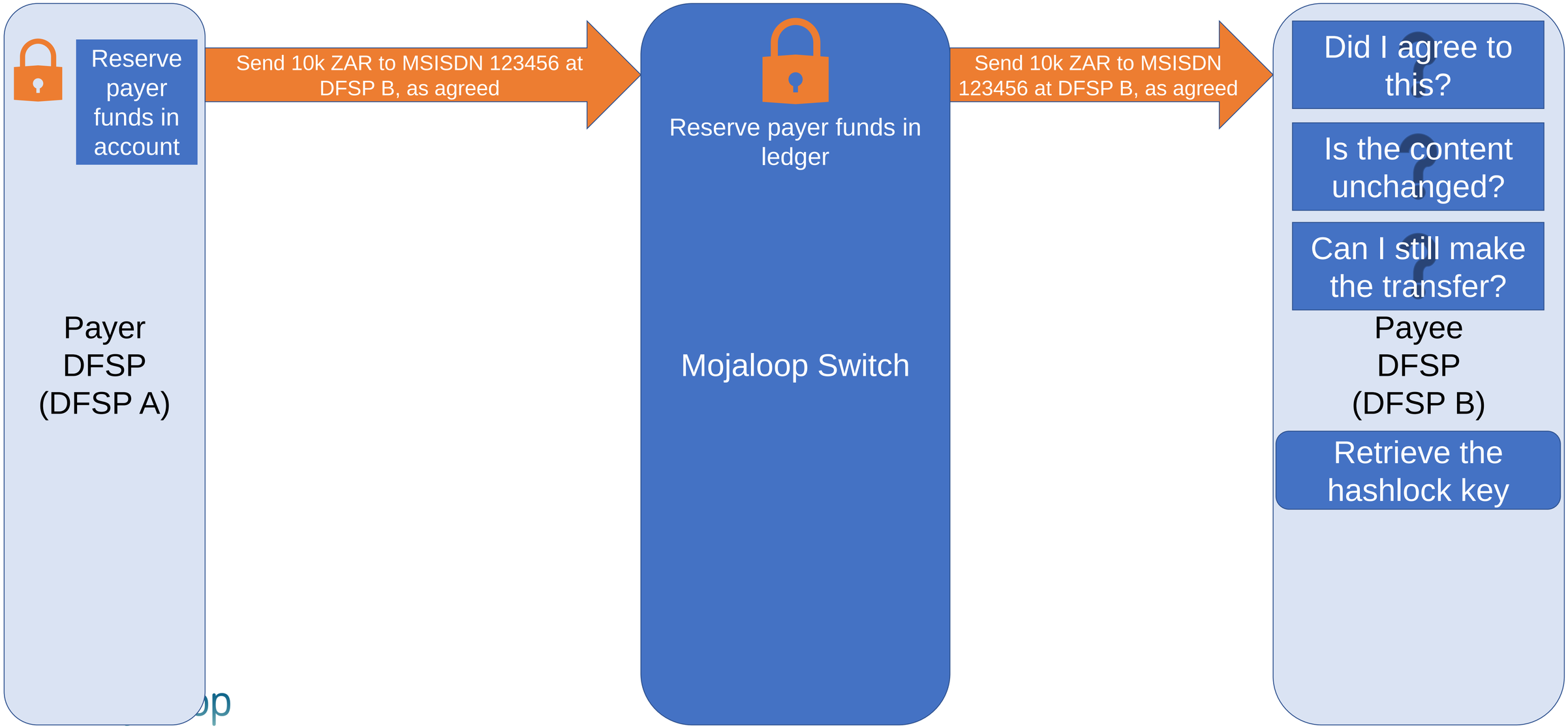
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

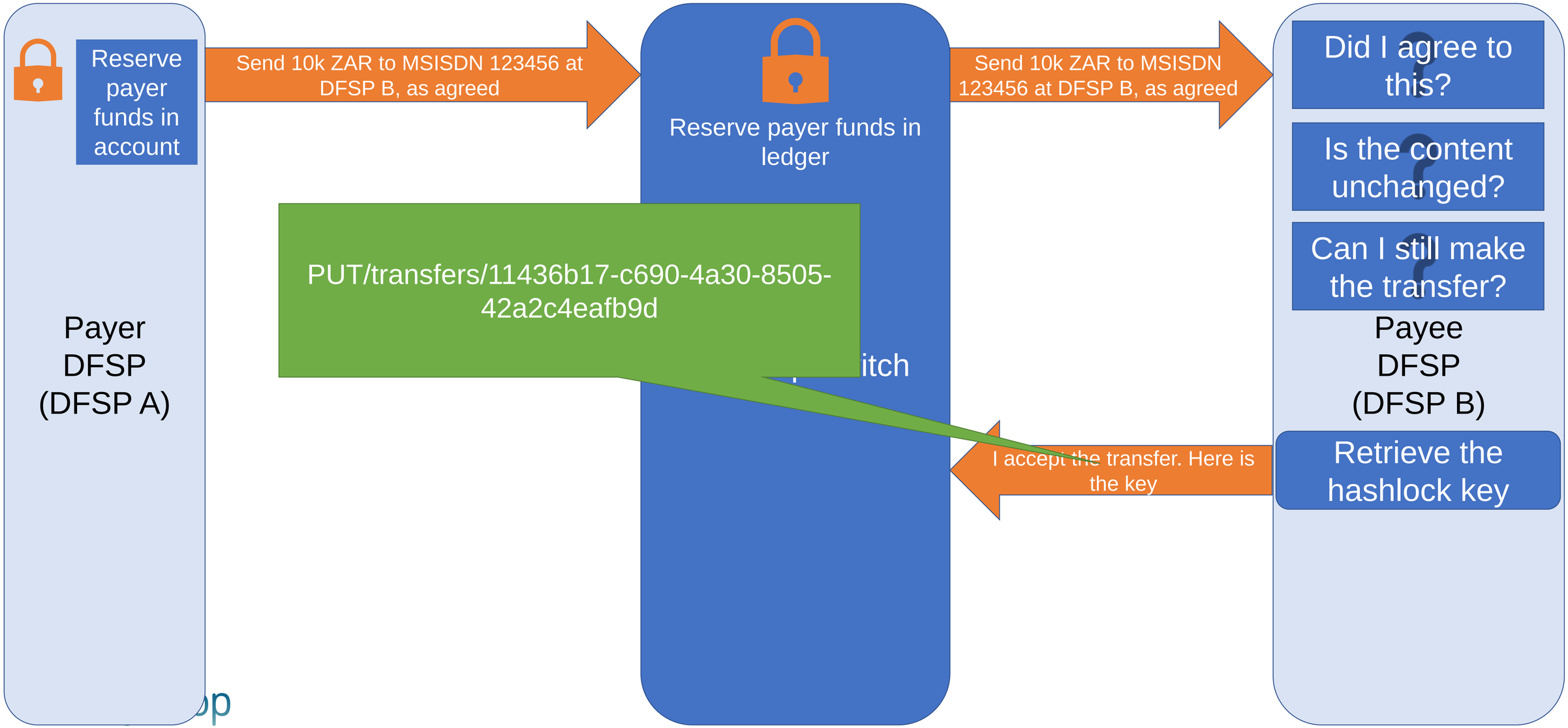
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)

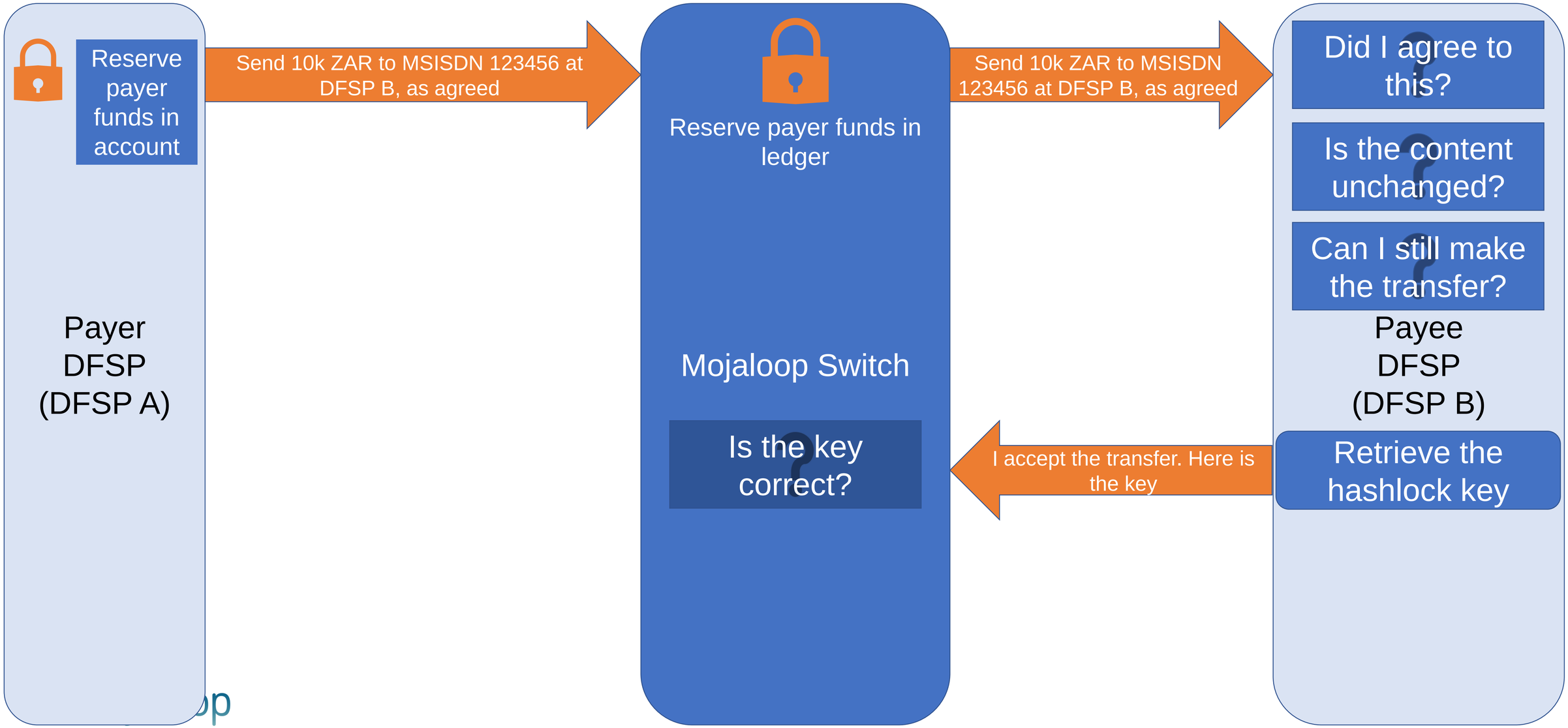
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Retrieve the hashlock key

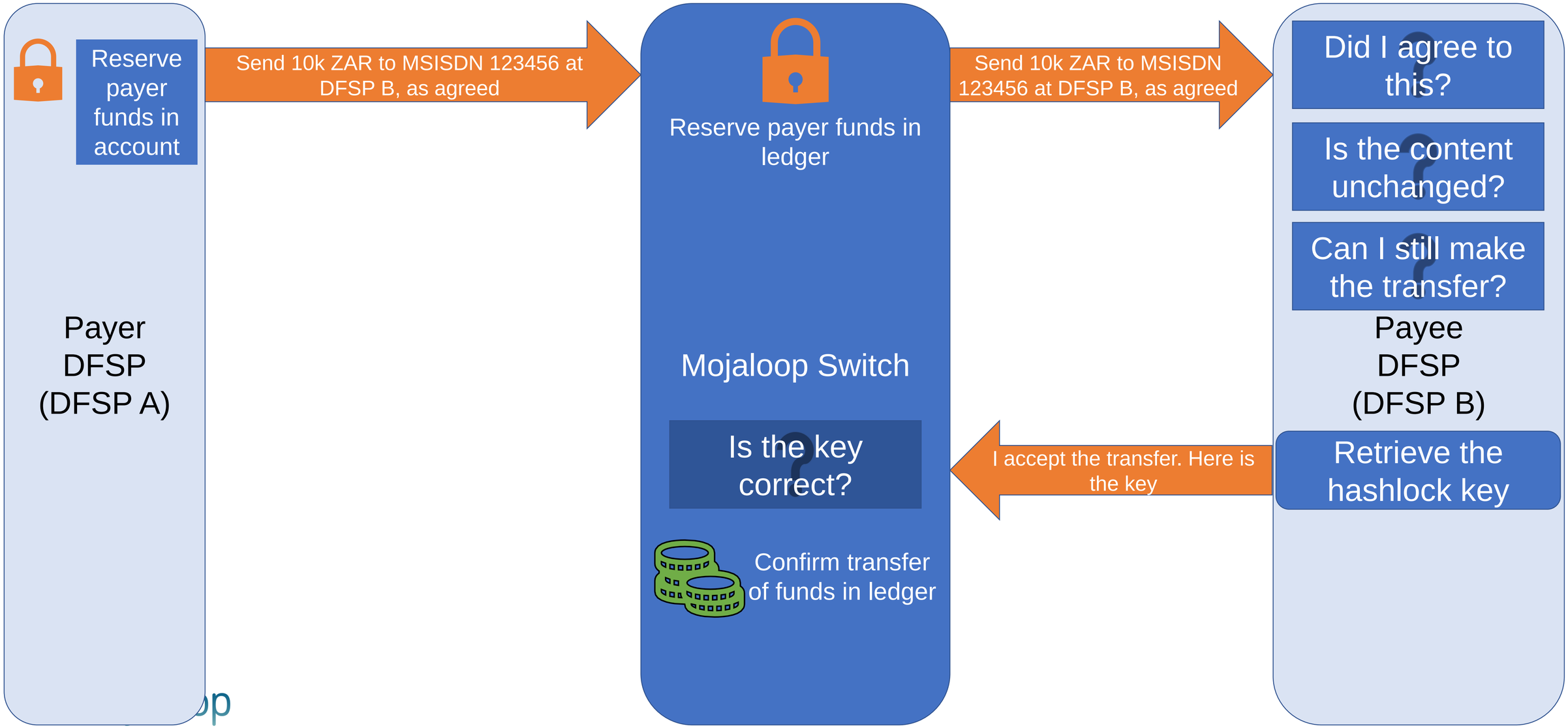
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
PUT/transfers/11436b17-c690-4a30-8505-42a2c4eafb9d
itch
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
I accept the transfer. Here is the key
Retrieve the hashlock key

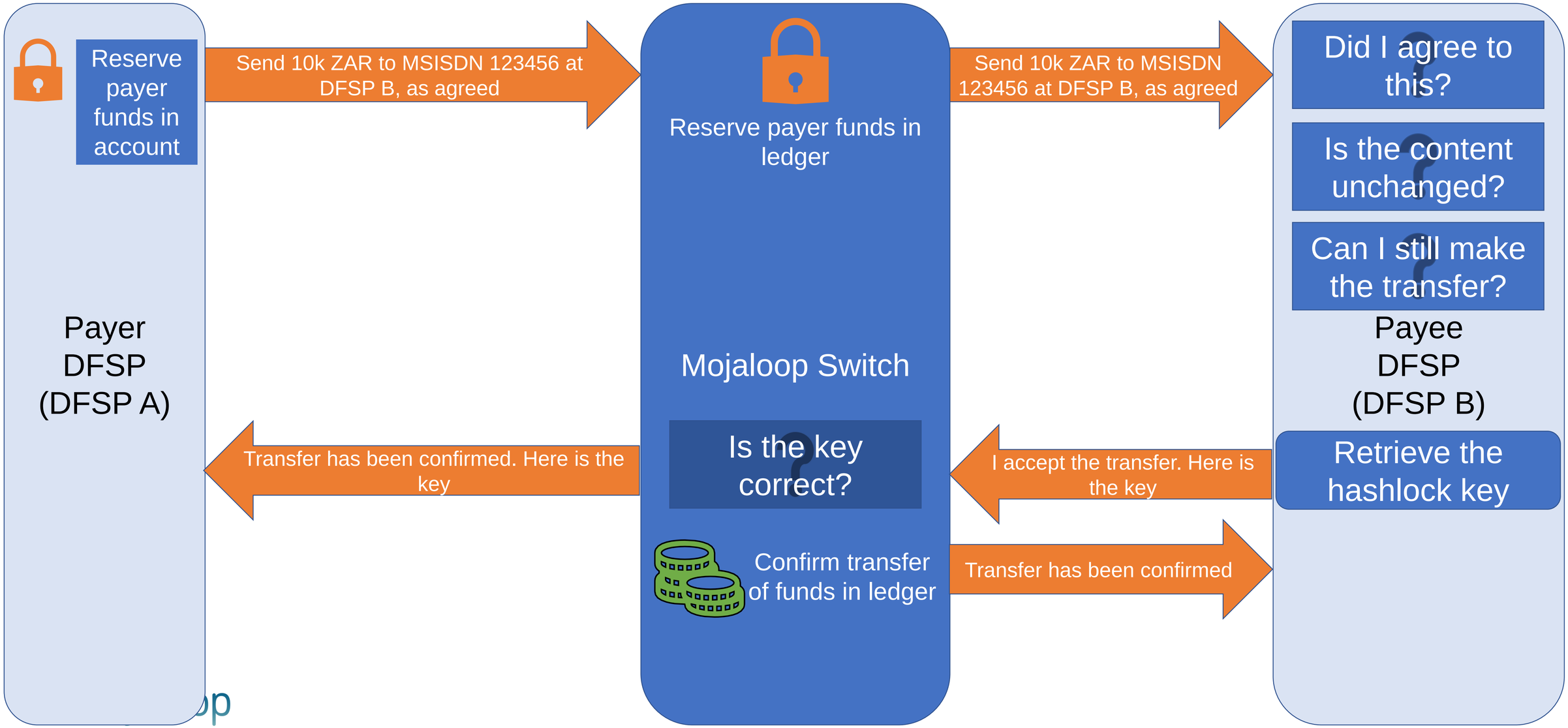
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
I accept the transfer. Here is the key
Retrieve the hashlock key

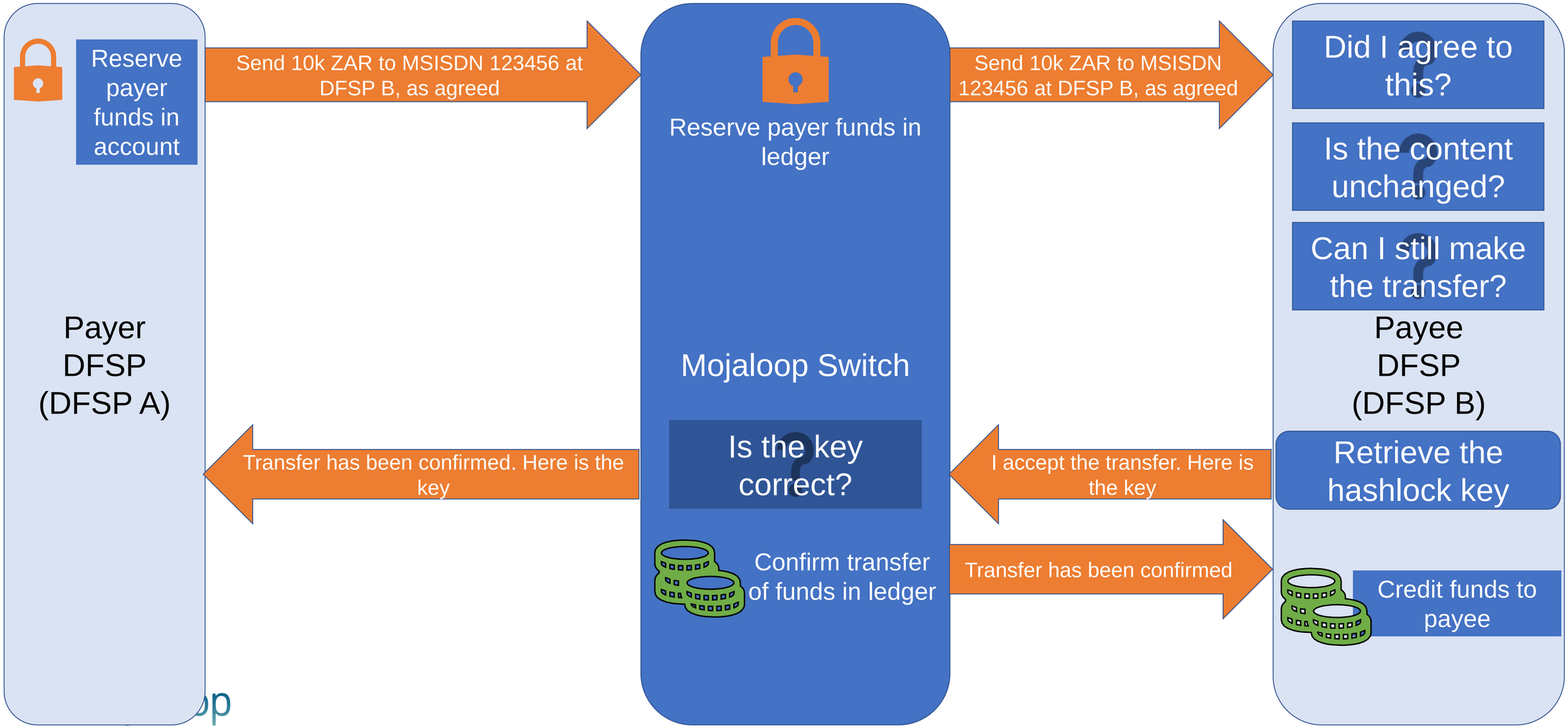
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
I accept the transfer. Here is the key
Retrieve the hashlock key
Confirm transfer of funds in ledger

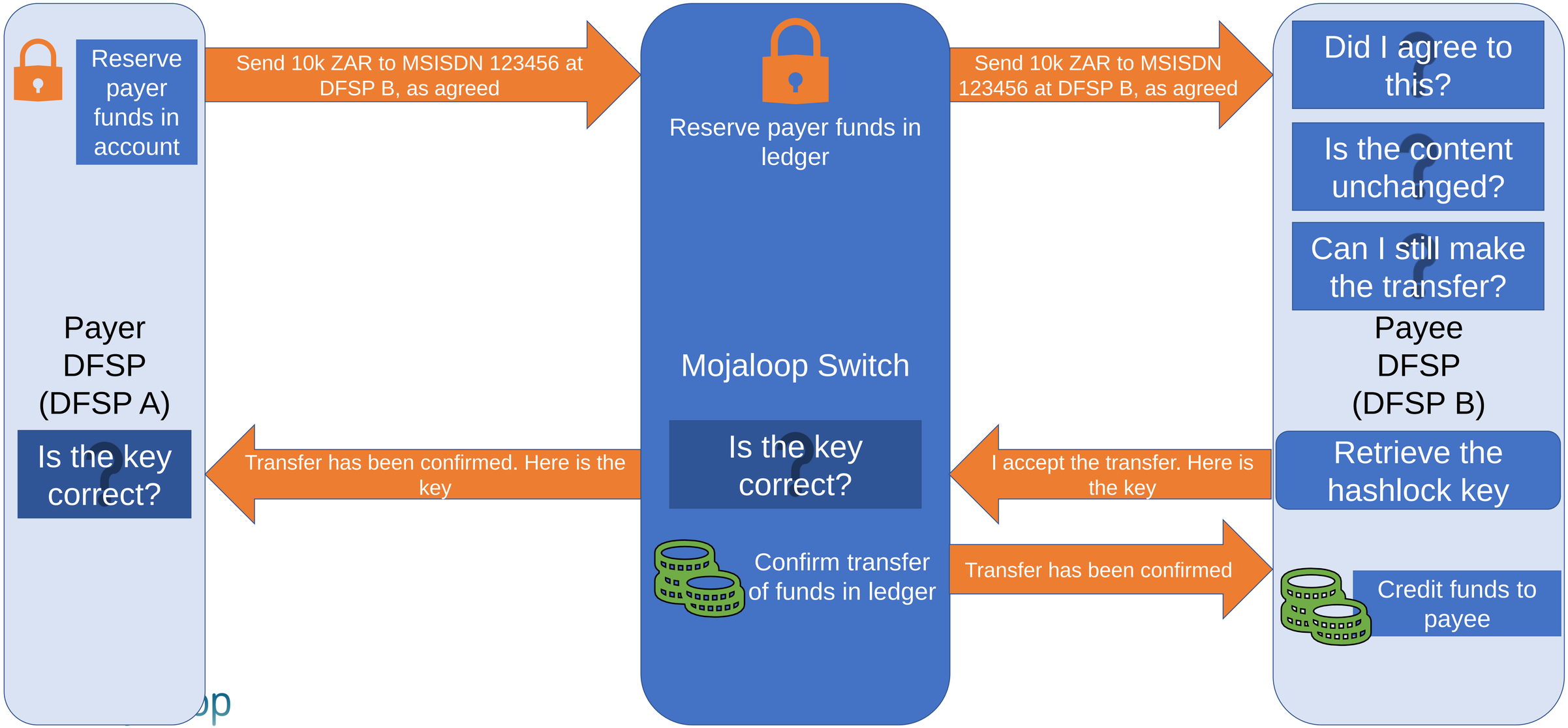
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
Transfer has been confirmed. Here is the key
I accept the transfer. Here is the key
Retrieve the hashlock key
Confirm transfer of funds in ledger
Transfer has been confirmed

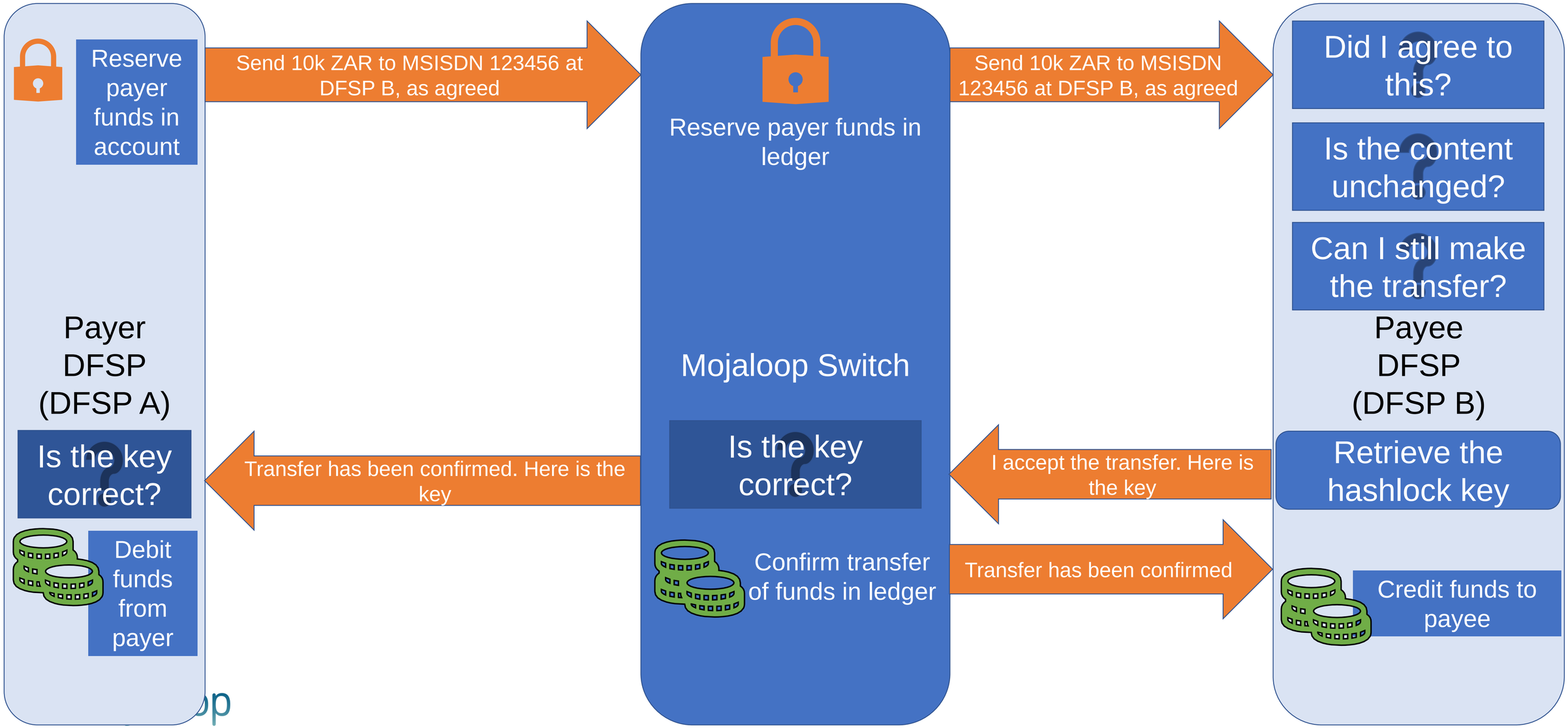
Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
Transfer has been confirmed. Here is the key
I accept the transfer. Here is the key
Retrieve the hashlock key
Confirm transfer of funds in ledger
Transfer has been confirmed
Credit funds to payee

Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
Transfer has been confirmed. Here is the key
Is the key correct?
I accept the transfer. Here is the key
Retrieve the hashlock key
Confirm transfer of funds in ledger
Transfer has been confirmed
Credit funds to payee

Transfer


Reserve payer funds in account
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Reserve payer funds in ledger
Send 10k ZAR to MSISDN 123456 at DFSP B, as agreed
Did I agree to this?
Is the content unchanged?
Can I still make the transfer?
Payer DFSP (DFSP A)
Mojaloop Switch
Payee DFSP (DFSP B)
Is the key correct?
Transfer has been confirmed. Here is the key
Is the key correct?
I accept the transfer. Here is the key
Retrieve the hashlock key
Debit funds from payer
Confirm transfer of funds in ledger
Transfer has been confirmed
Credit funds to payee

The merchant request to pay

Discovery

Payer DFSP (DFSP A)

Mojaloop Switch

Payee DFSP (DFSP B)

Discovery

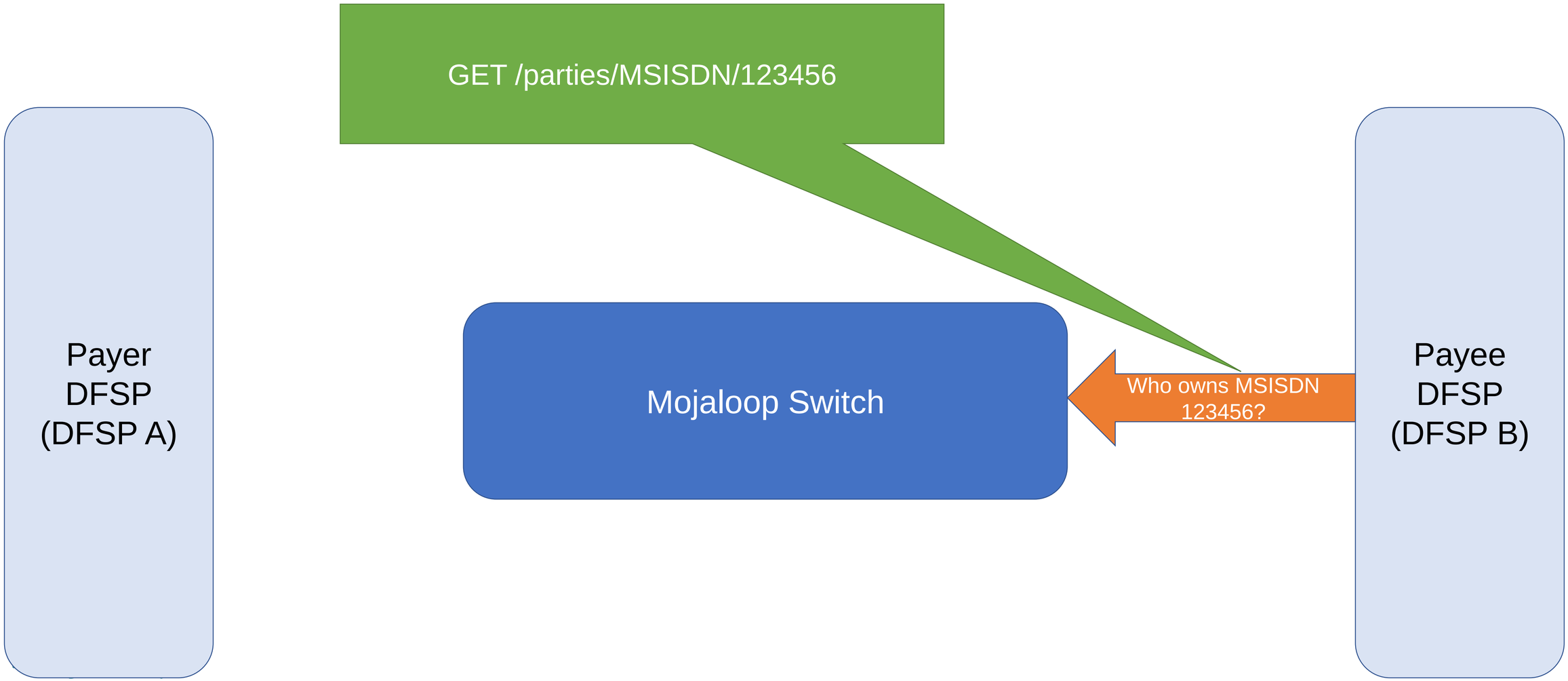
Please charge my phone, it’s 123456

Payer DFSP (DFSP A)

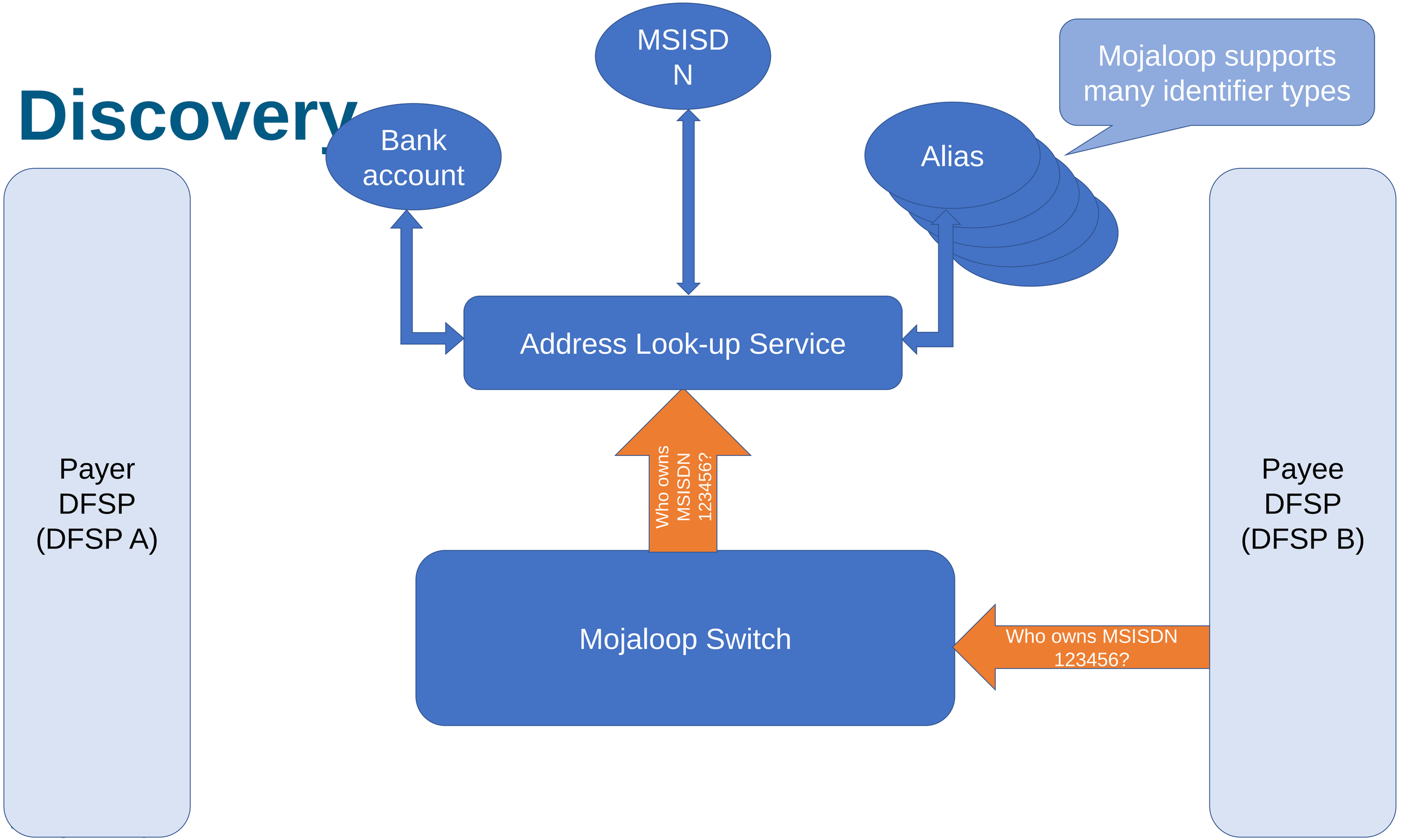
Mojaloop Switch

Payee DFSP (DFSP B)

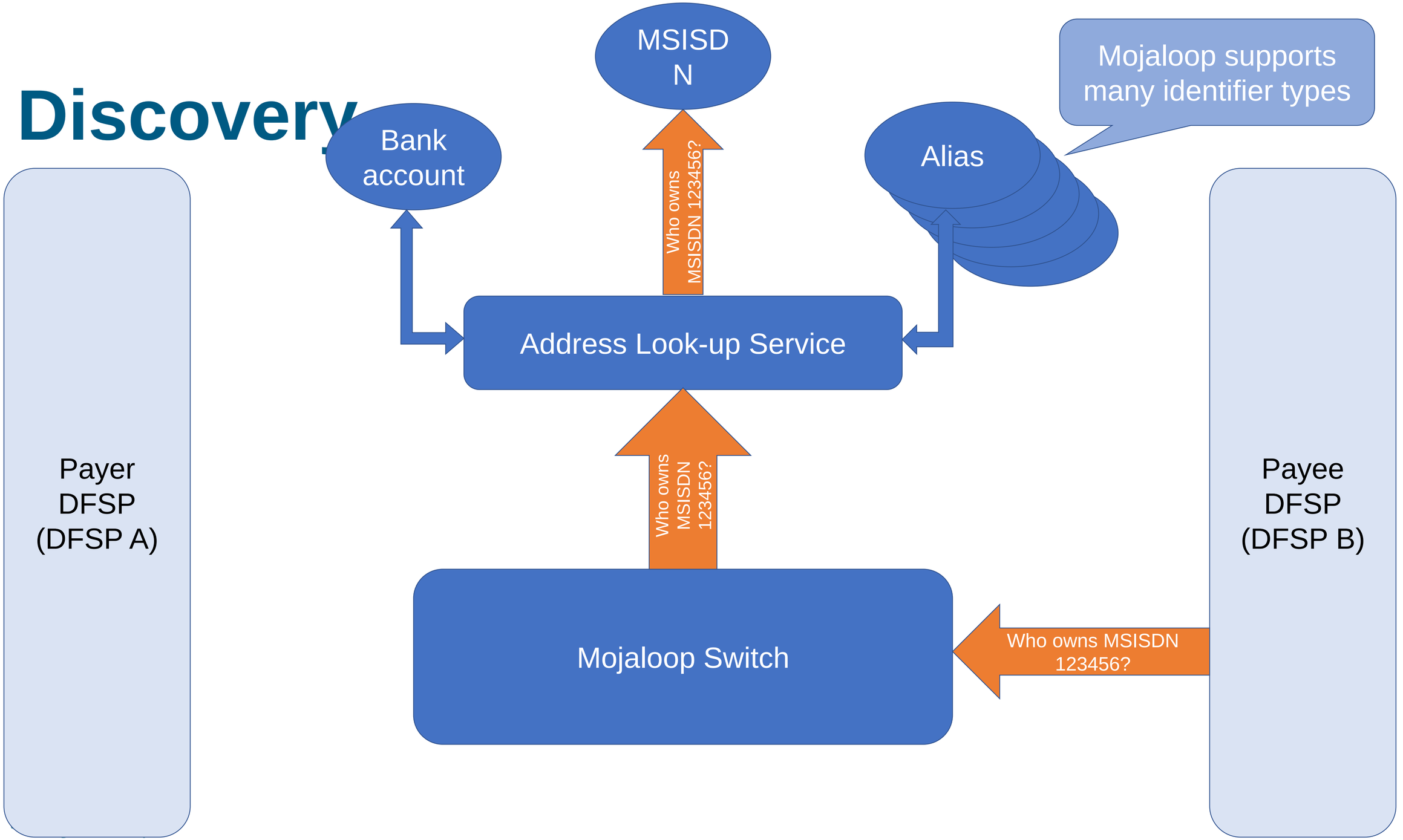
Discovery


GET /parties/MSISDN/123456
Payer
DFSP
(DFSP A)
Mojaloop Switch
Who owns MSISDN
123456?
Payee
DFSP
(DFSP B)

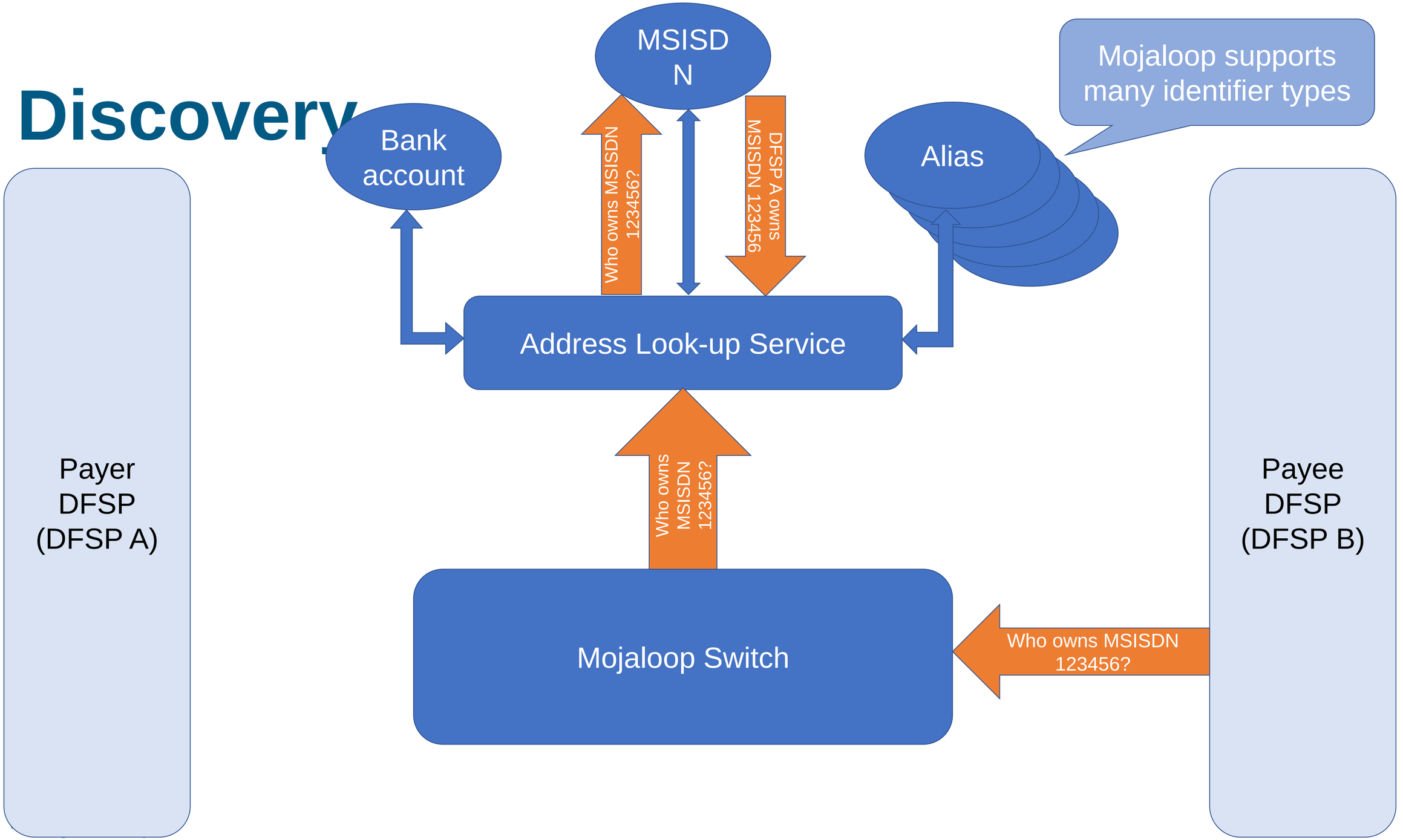
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Address Look-up Service
Payer DFSP (DFSP A)
Who owns MSISDN 123456?
Mojaloop Switch
Who owns MSISDN 123456?
Payee DFSP (DFSP B)

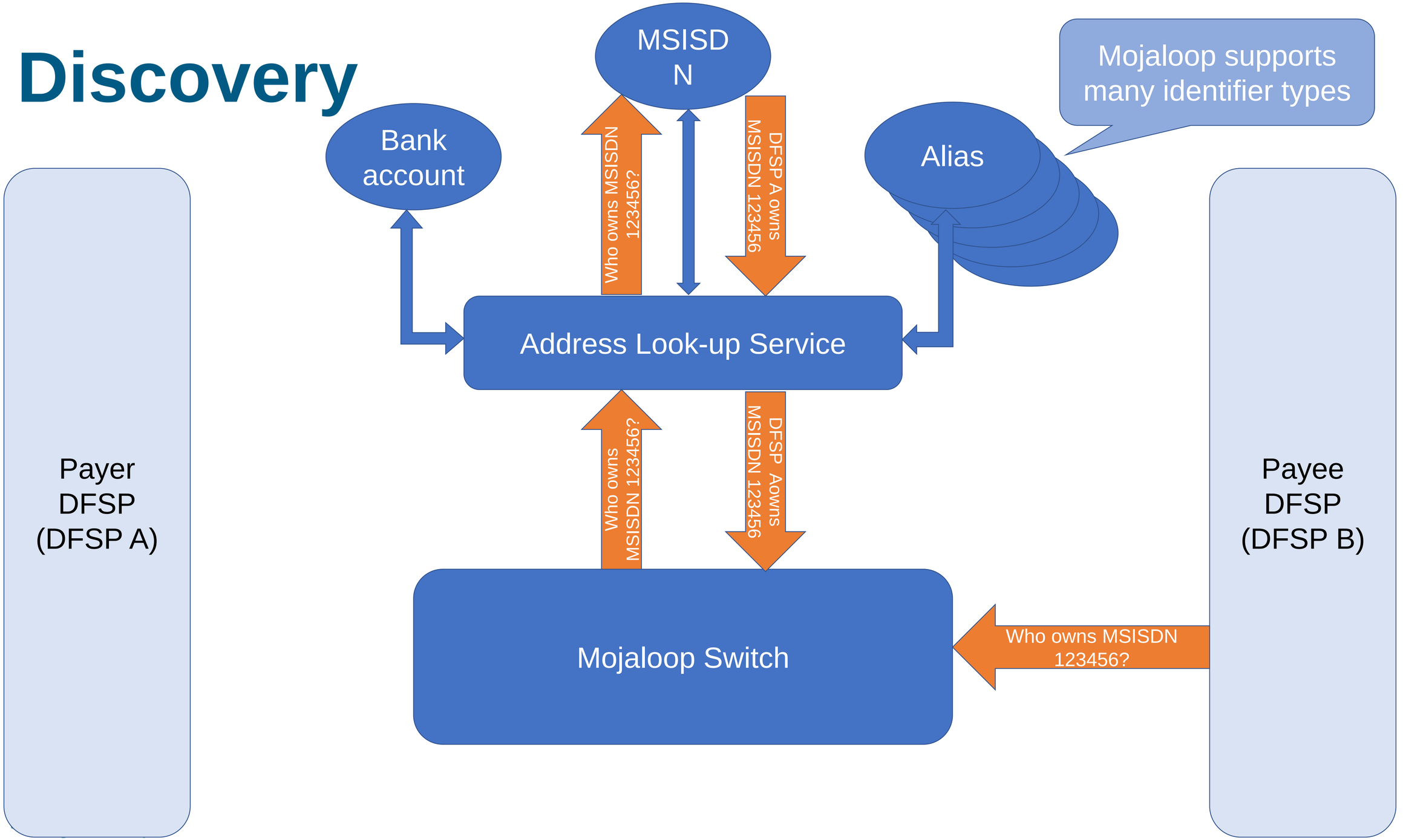
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
Address Look-up Service
Who owns MSISDN 123456?
Payer DFSP (DFSP A)
Mojaloop Switch
Who owns MSISDN 123456?
Payee DFSP (DFSP B)

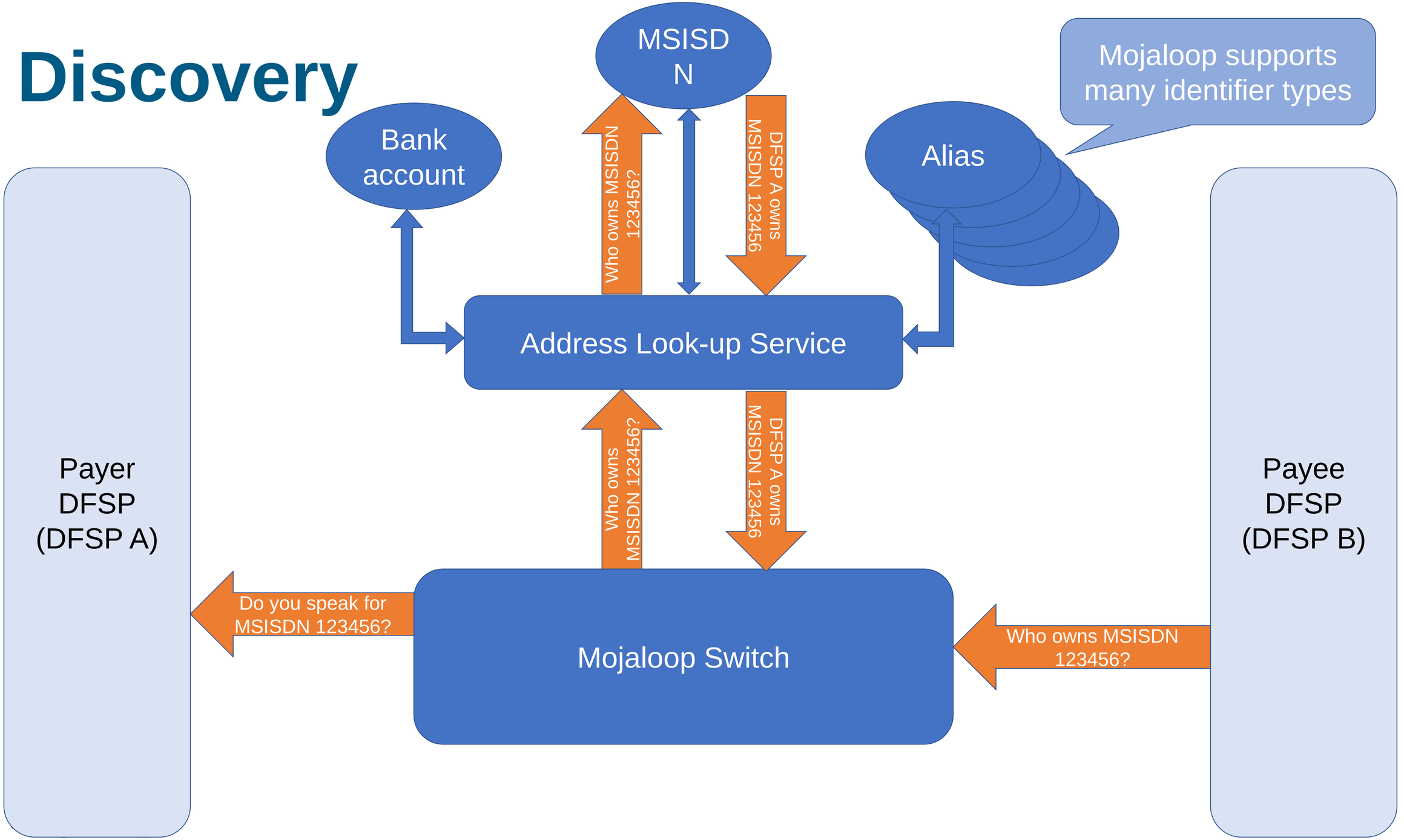
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
Payer DFSP (DFSP A)
Mojaloop Switch
Who owns MSISDN 123456?
Payee DFSP (DFSP B)

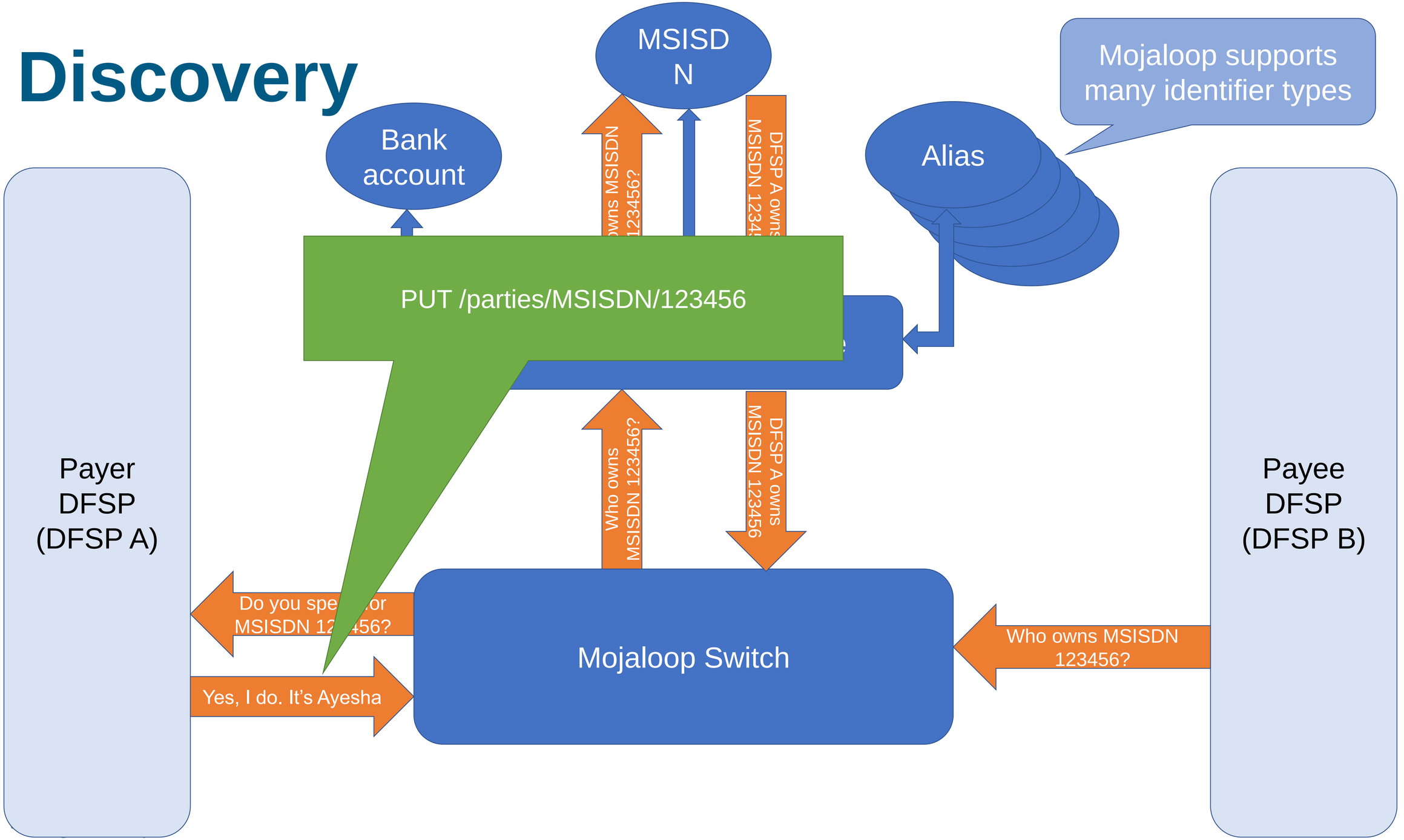
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
DFSP Aowns MSISDN 123456
Payer DFSP (DFSP A)
Mojaloop Switch
Who owns MSISDN 123456?
Payee DFSP (DFSP B)

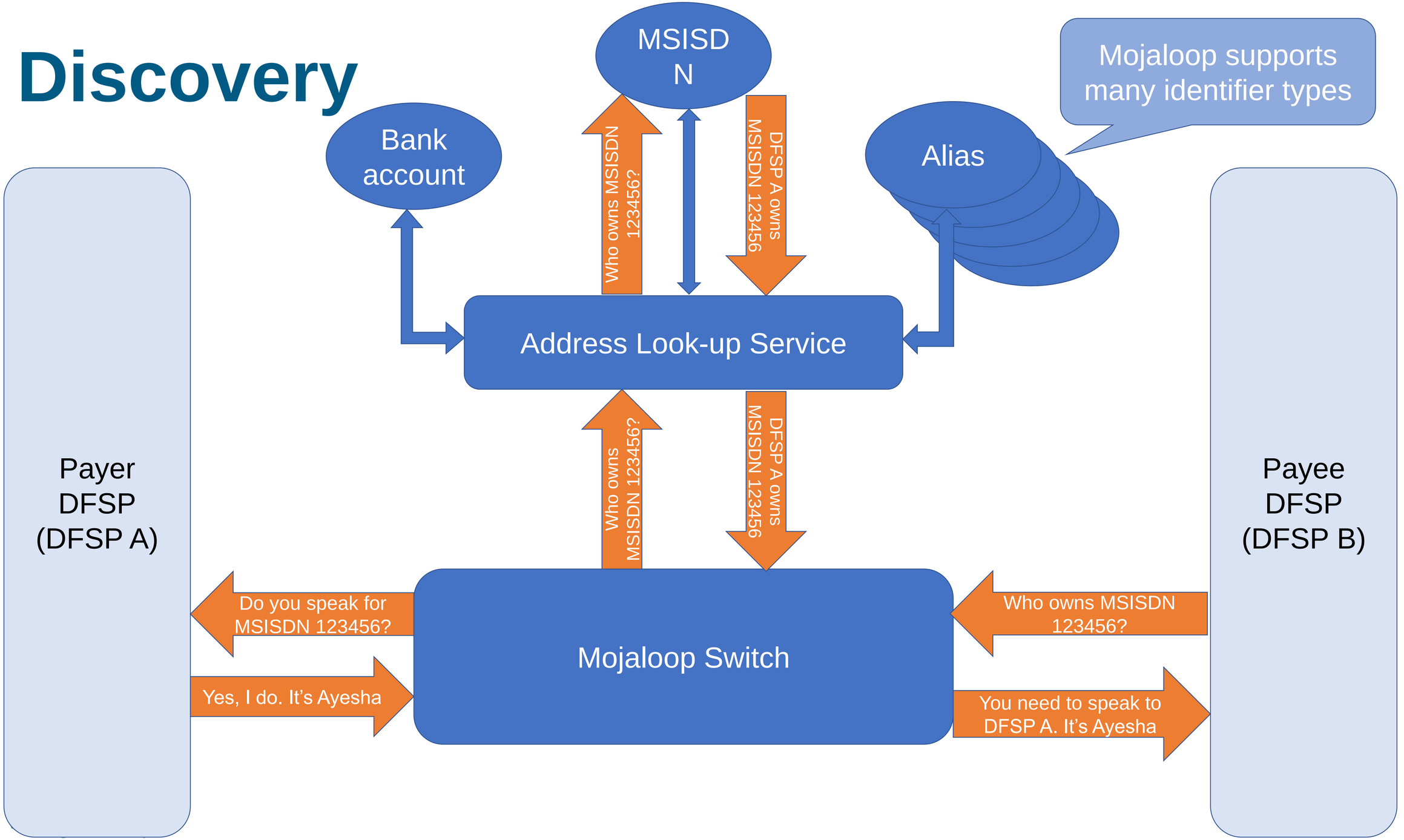
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Do you speak for MSISDN 123456?
Mojaloop Switch
Who owns MSISDN 123456?

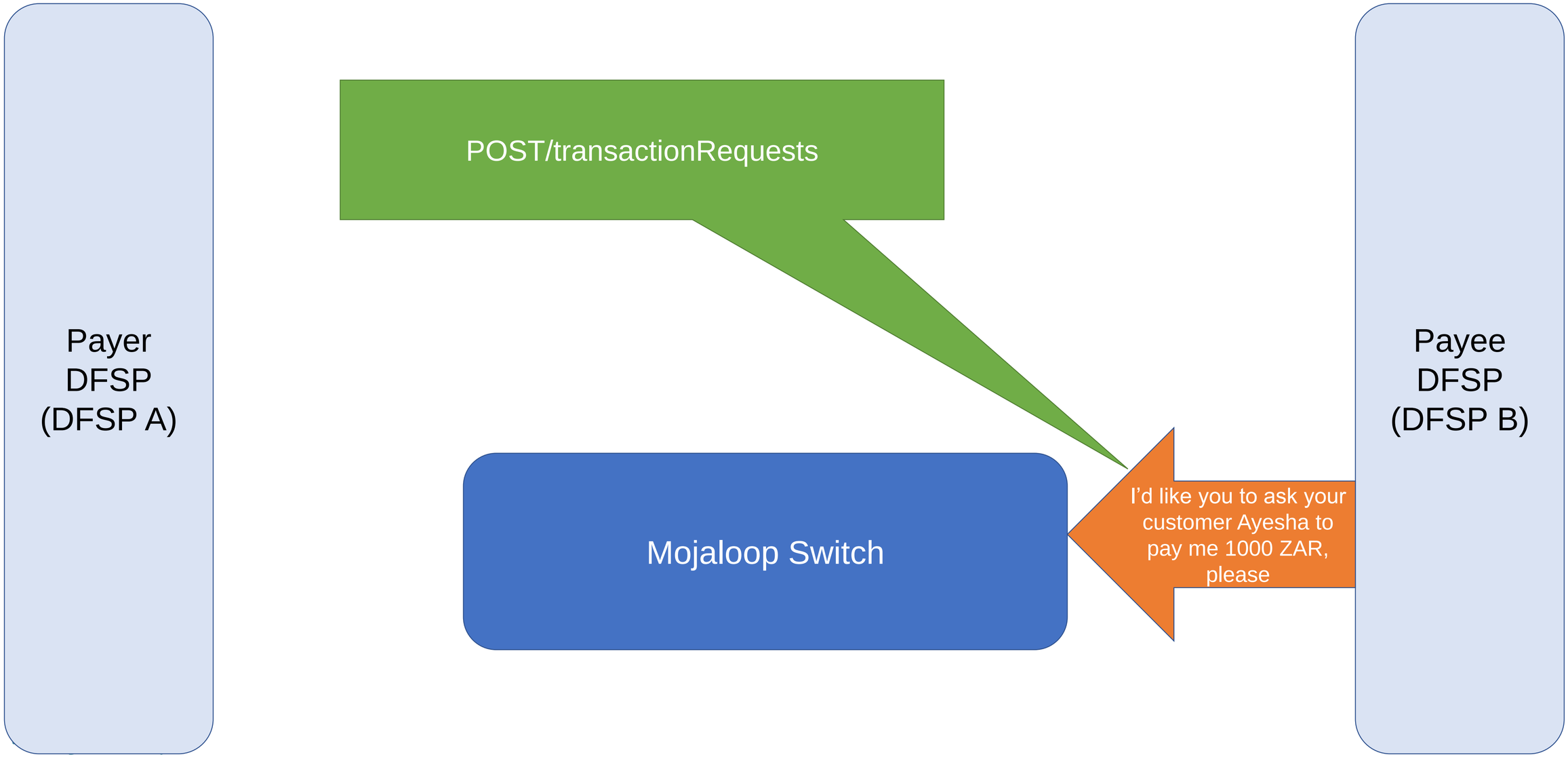
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
PUT /parties/MSISDN/123456
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Mojaloop Switch
Do you spe or MSISDN 12 456?
Yes, I do. It's Ayesha
Who owns MSISDN 123456?

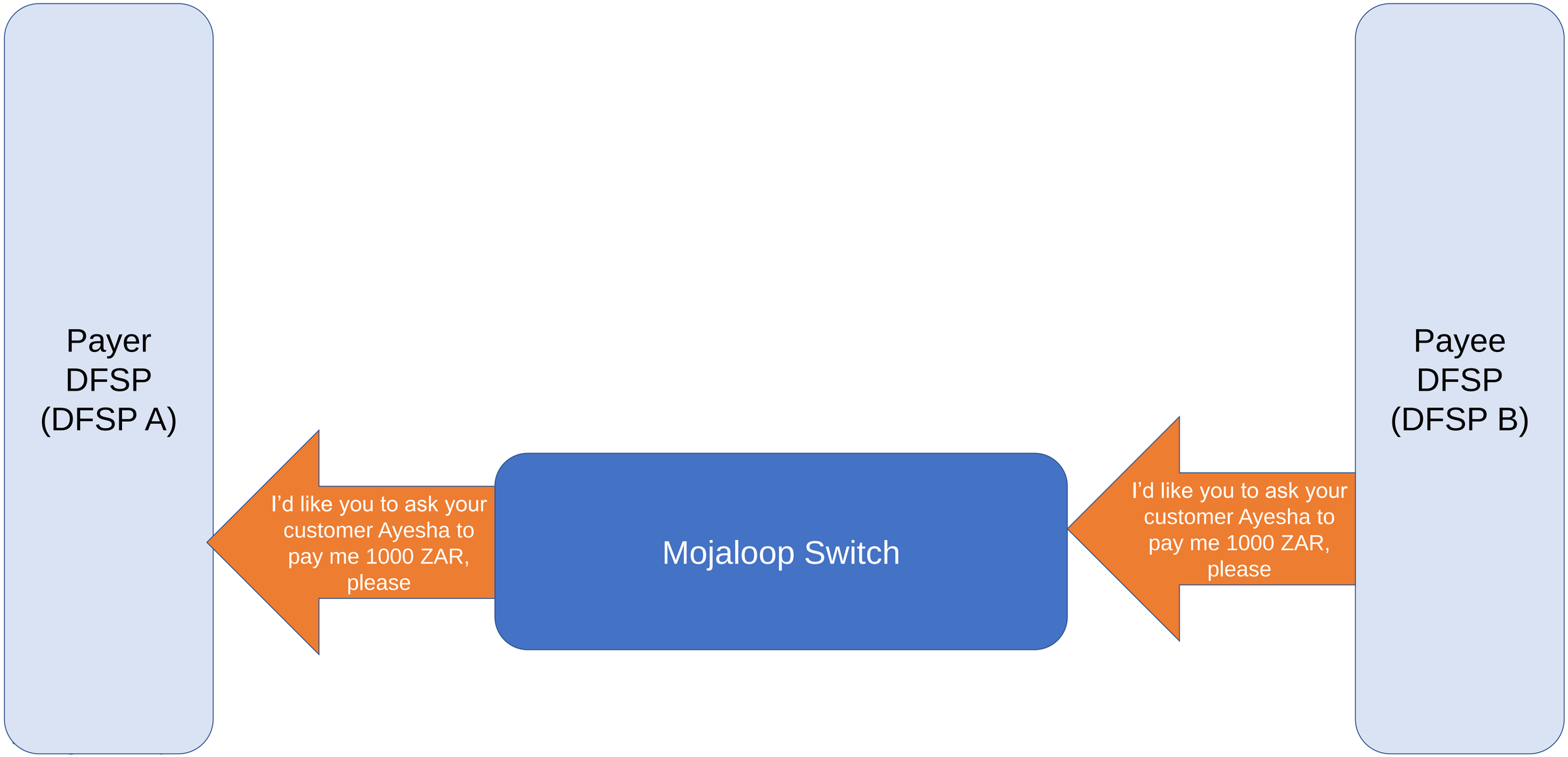
Discovery


MSISDN
Bank account
Alias
Mojaloop supports many identifier types
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Address Look-up Service
Who owns MSISDN 123456?
DFSP A owns MSISDN 123456
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Do you speak for MSISDN 123456?
Who owns MSISDN 123456?
Mojaloop Switch
Yes, I do. It's Ayesha
You need to speak to DFSP A. It's Ayesha

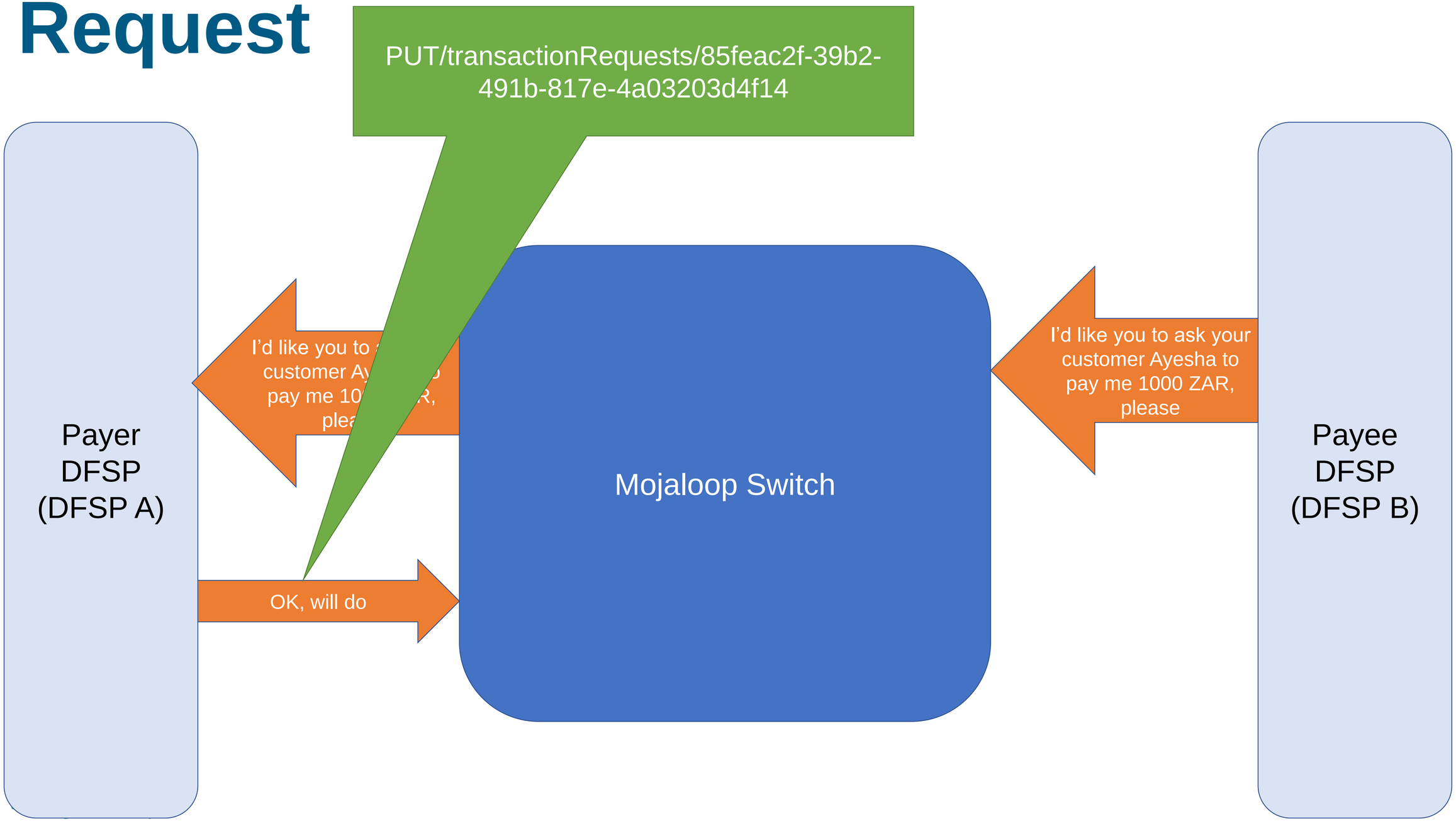
Request


Payer
DFSP
(DFSP A)
POST/transactionRequests
Mojaloop Switch
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
Payee
DFSP
(DFSP B)

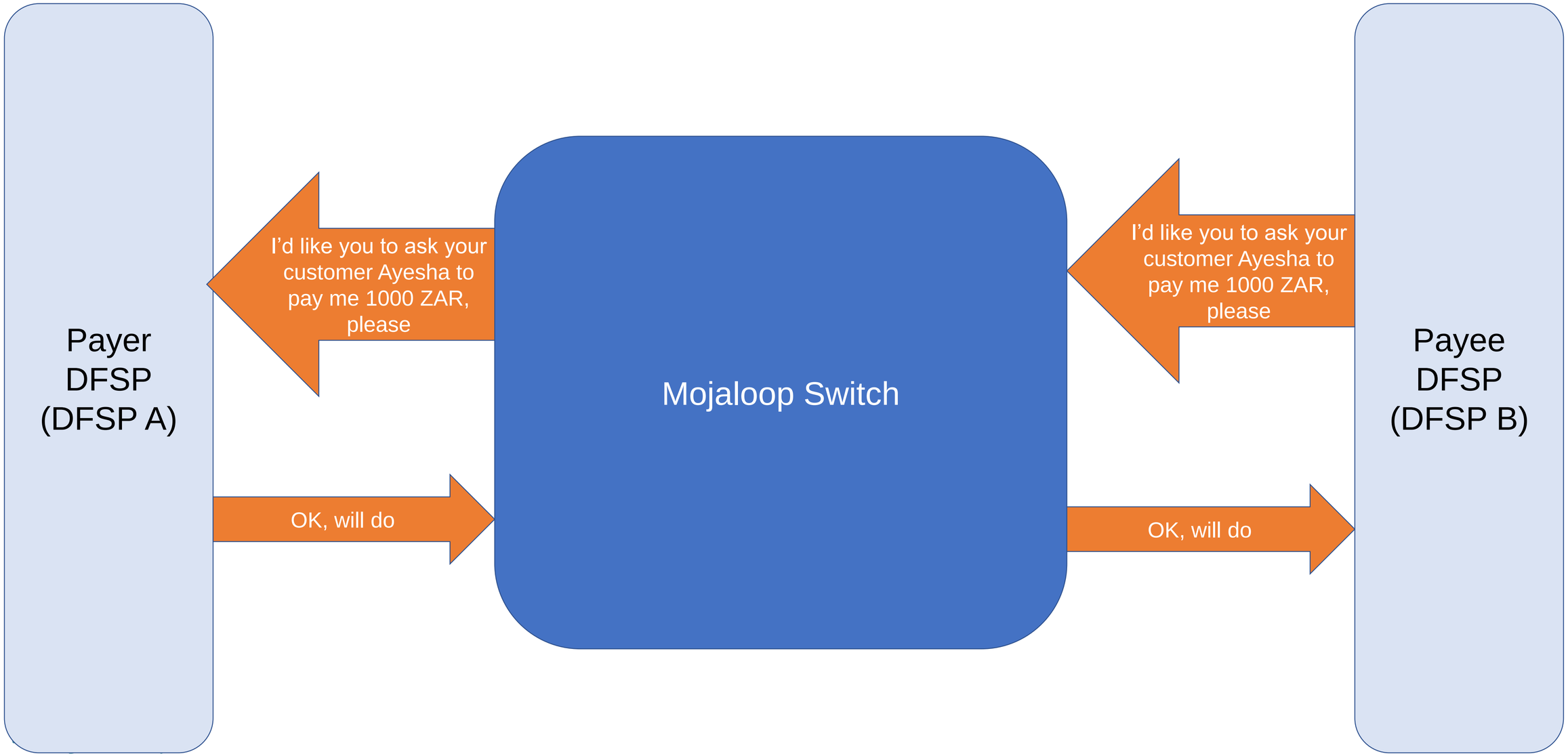
Request


Payer
DFSP
(DFSP A)
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
Mojaloop Switch
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
Payee
DFSP
(DFSP B)

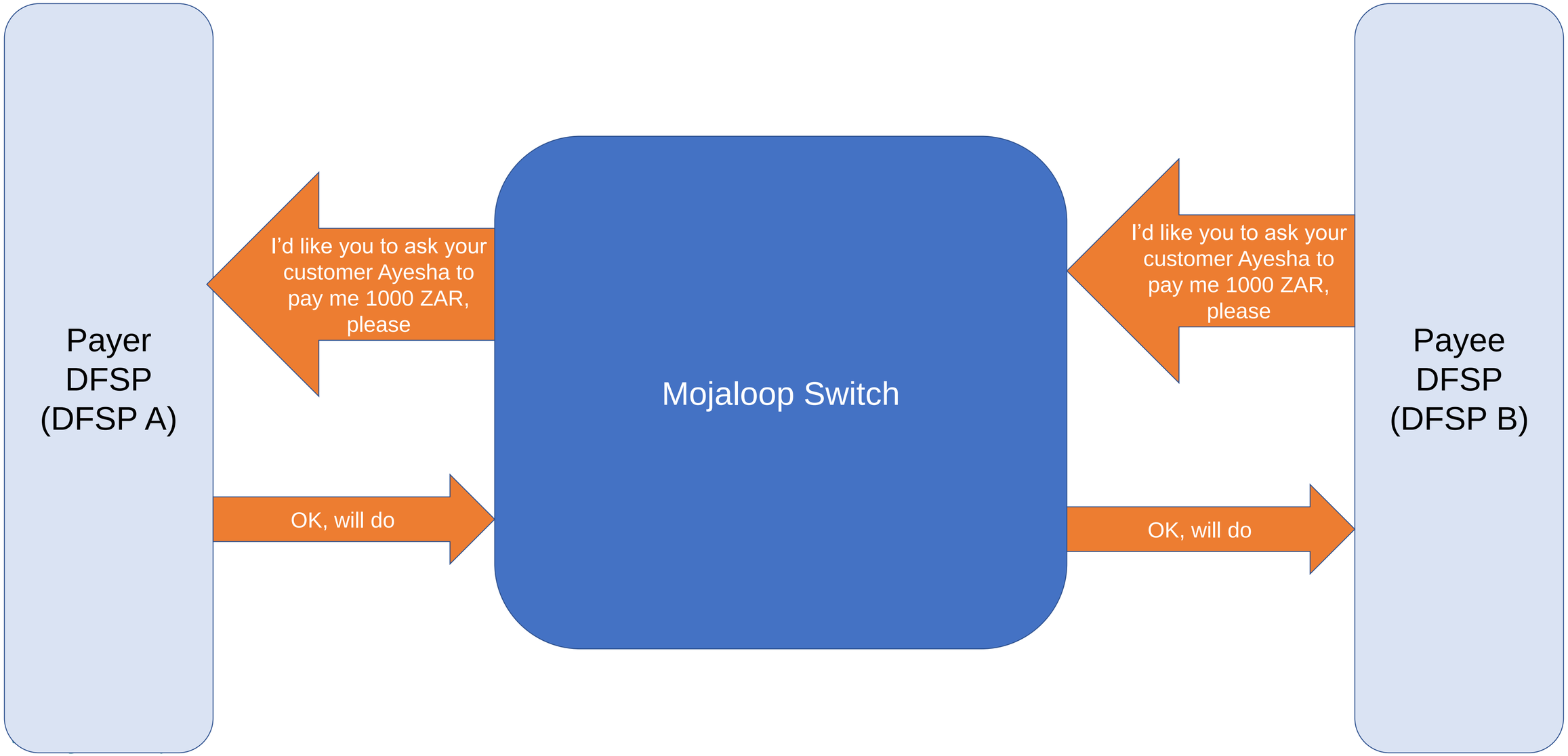
Request


PUT/transactionRequests/85feac2f-39b2-491b-817e-4a03203d4f14
Payer DFSP (DFSP A)
I'd like you to
customer Ay
pay me 10
R,
plea
OK, will do
Mojaloop Switch
I'd like you to ask your customer Ayesha to pay me 1000 ZAR, please
Payee DFSP (DFSP B)

Request


Payer
DFSP
(DFSP A)
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
OK, will do
Mojaloop Switch
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
OK, will do
Payee
DFSP
(DFSP B)

And next…


Payer
DFSP
(DFSP A)
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
Mojaloop Switch
I’d like you to ask your customer Ayesha to pay me 1000 ZAR, please
Payee
DFSP
(DFSP B)
OK, will do
OK, will do

Simples…

mojaloop