mojaloop

PISP Progress Update

PI 10 - April 2010

JJ Geewax, Lewis Daly

Goal

Overall: Enable 3rd party payment initiation within the Mojaloop Ecosystem.

This Presentation:

- Update the community on our progress
- Share insights into design and gather feedback
    - *Do you see security issues? Is there a use case you're thinking about that won't work? Please yell out.*

What this is not:

- A design session with 100+ people

Overview

1. **Background**
   a. What is a PISP?
   b. Links to last slide deck
   c. Transfers

2. **Account Linking Design**
   a. Initial Login and Consent
   b. Registering a FIDO Key

3. **API Changes**

4. **Next Steps**

Background

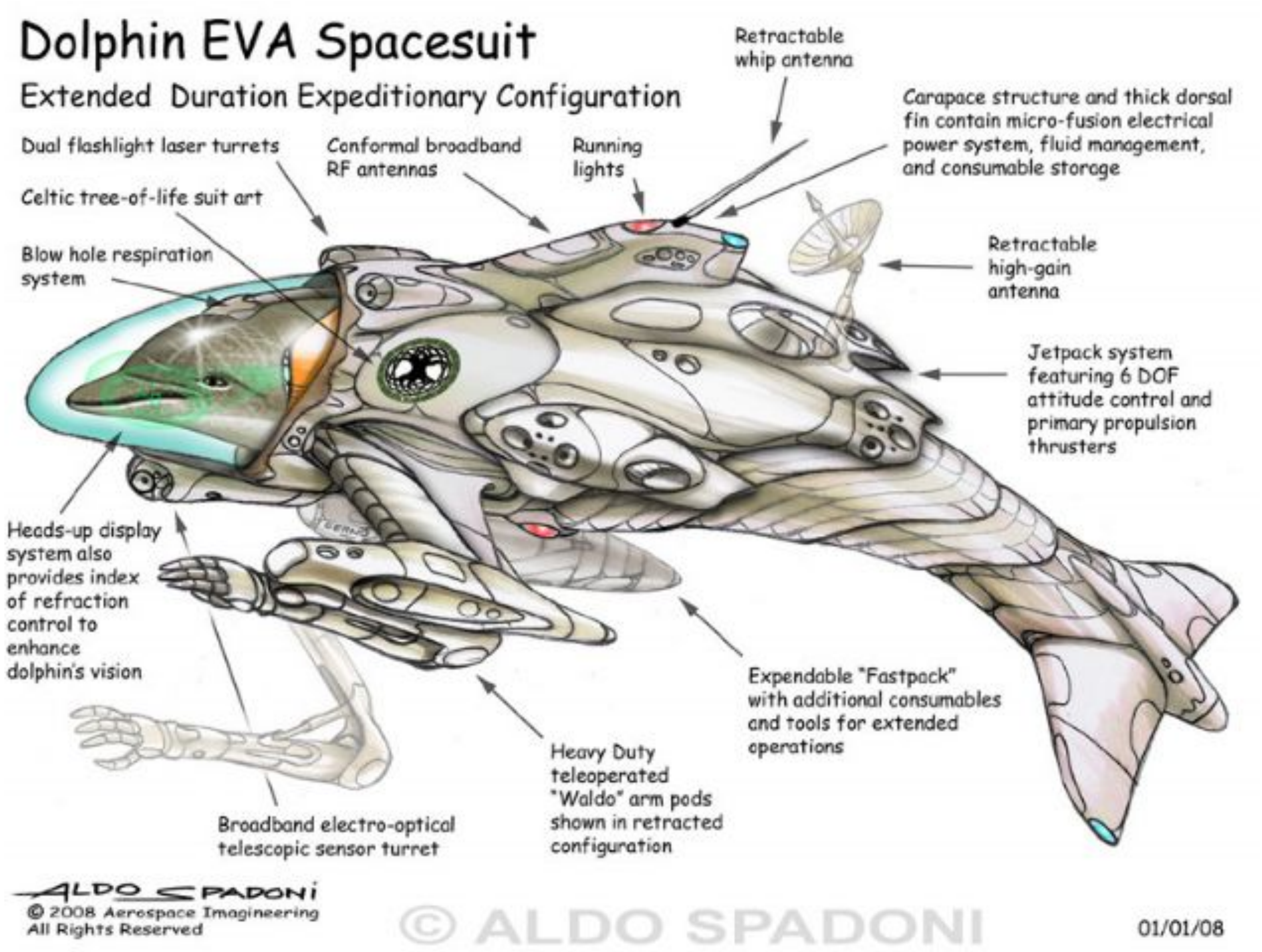
mojaloop

What is **PISP**?

What is **PISP**?

Porpoise Interstellar Space Programme?

PISP?


Dolphin EVA Spacesuit
Extended Duration Expeditionary Configuration
Dual flashlight laser turrets
Conformal broadband RF antennas
Running lights
Retractable whip antenna
Carapace structure and thick dorsal fin contain micro-fusion electrical power system, fluid management, and consumable storage
Celtic tree-of-life suit art
Blow hole respiration system
Retractable high-gain antenna
Jetpack system featuring 6 DOF attitude control and primary propulsion thrusters
Heads-up display system also provides index of refraction control to enhance dolphin's vision
Expendable "Fastpack" with additional consumables and tools for extended operations
Heavy Duty teleoperated "Waldo" arm pods shown in retracted configuration
Broadband electro-optical telescopic sensor turret
ALDO SPADONI
© 2008 Aerospace Imagineering
All Rights Reserved
© ALDO SPADONI
01/01/08

Second Anniversary Issue
Silverberg on Tomorrow's Cities
FUTURE LIFE
MARCH, 1980
#17
Filming the Future:
'The Black Hole'
'Saturn 3'
'Star Trek'
Your Workday in the 21st Century
Robot Workers Invade Industry
Computers in ESP Research
Real Starships
Inside: The Art of Rick Sternbach

source: [Say; Hello Spaceman]

Sadly Not.

Payment Initiation Service Provider

Background

According to PSD2:

PISP - Payment Initiation Service Provider

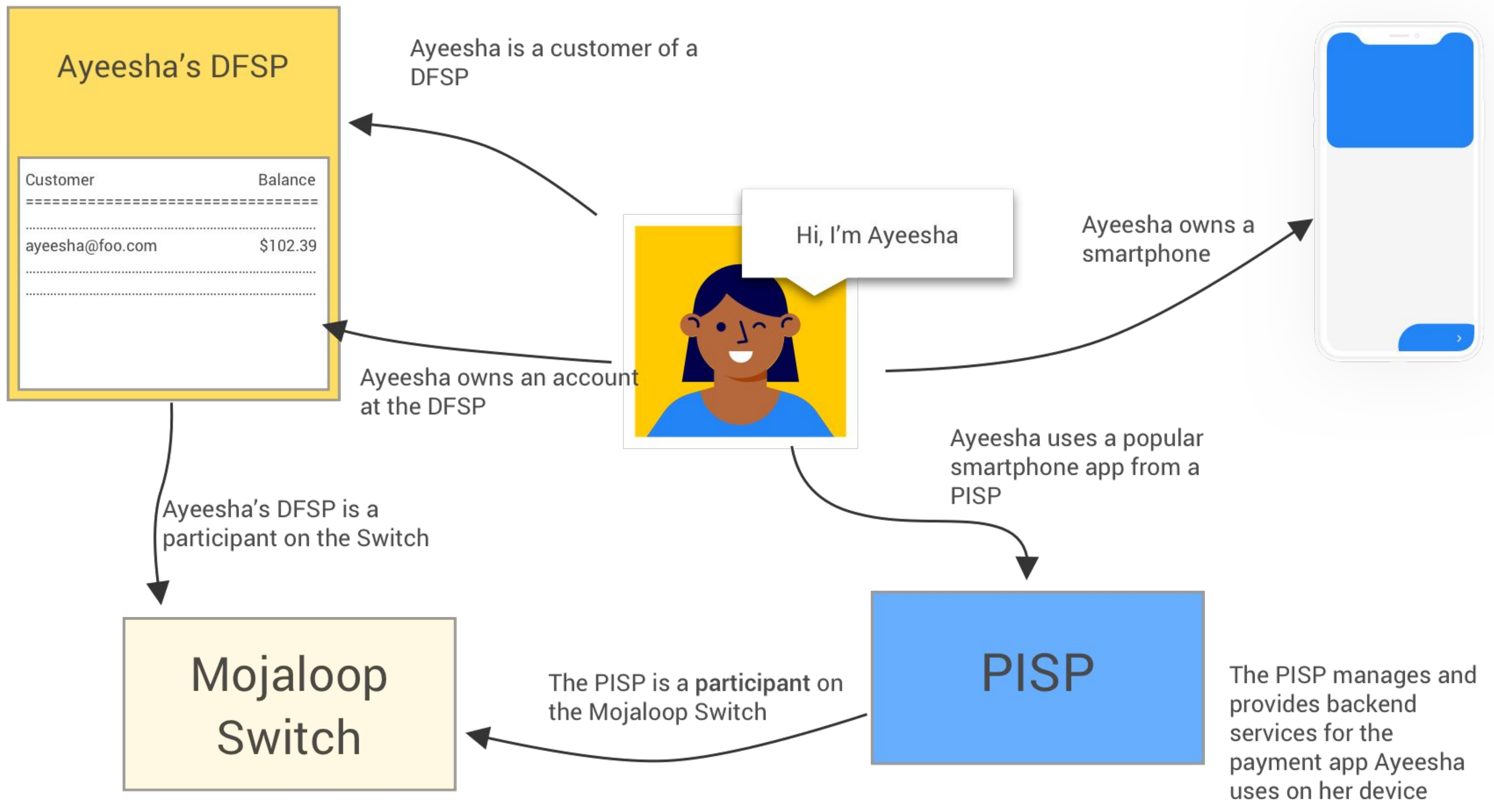
PISPs initiate payments from a user’s account (on behalf of the user) to a payee account.

In Mojaloop:

A PISP is a new **participant** role, which:

- Has no liquidity (or settlement) requirements
- Initiates transactions on behalf of users at DFSPs with **RequestToPay**

Background


Ayeesha's DFSP
Customer
Balance
ayeesha@foo.com
$102.39
Ayeesha is a customer of a DFSP
Hi, I'm Ayeesha
Ayeesha owns a smartphone
Ayeesha owns an account at the DFSP
Ayeesha uses a popular smartphone app from a PISP
Ayeesha's DFSP is a participant on the Switch
Mojaloop Switch
The PISP is a **participant** on the Mojaloop Switch
PISP
The PISP manages and provides backend services for the payment app Ayeesha uses on her device

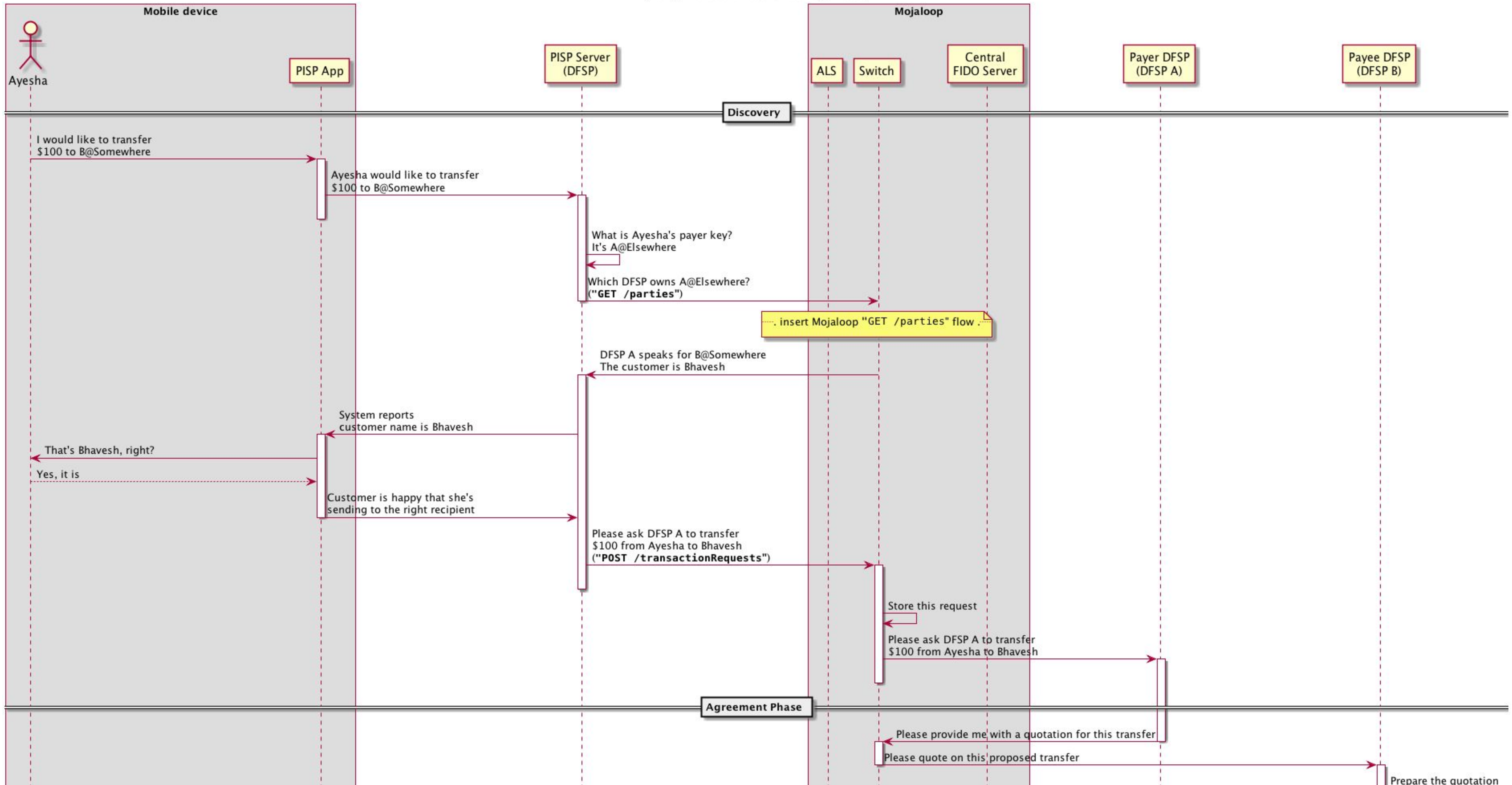
Original Source: [Mojaloop: 3rd Party Payment Initiation Proposal for Credit Transactions]

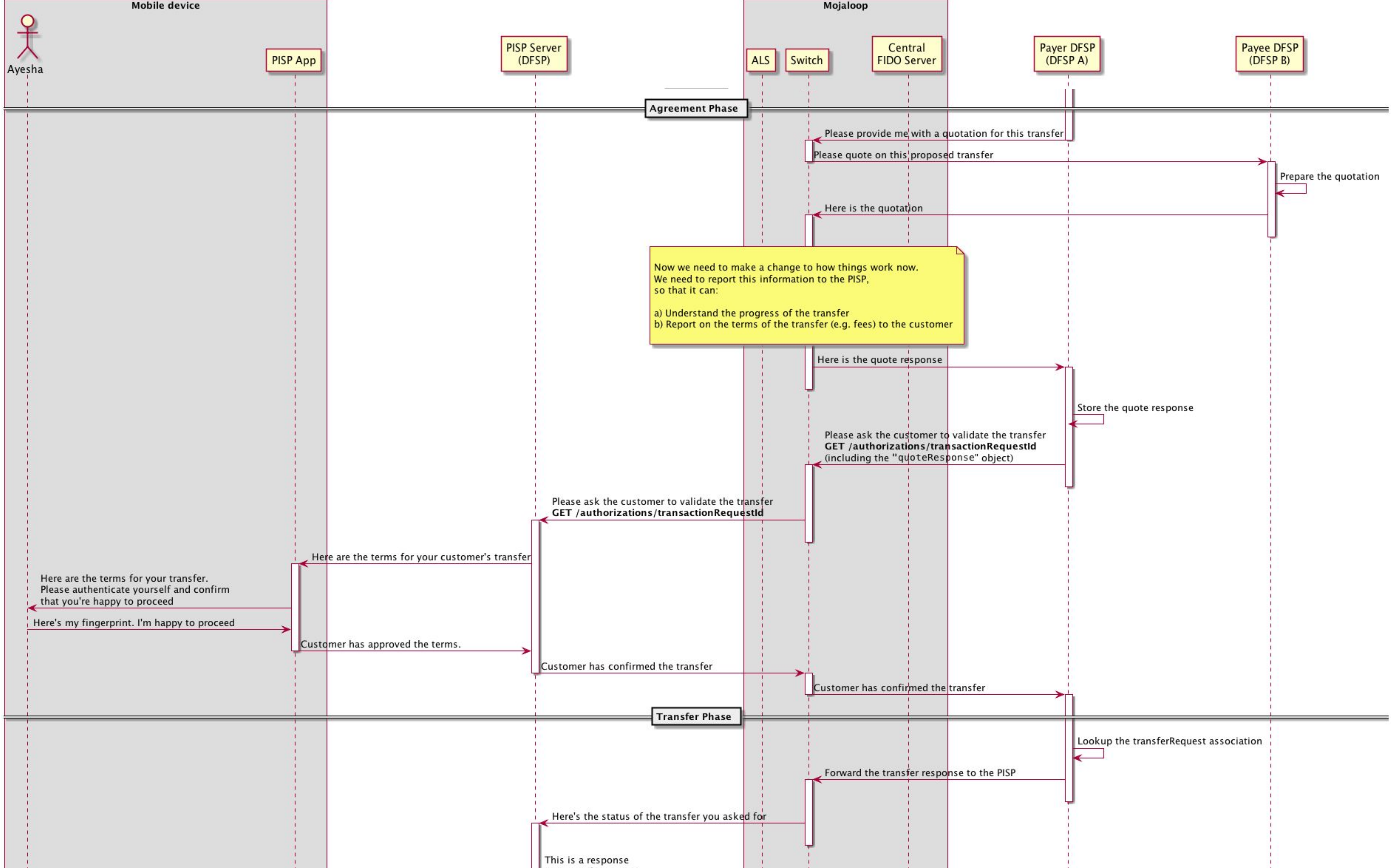
Transfers

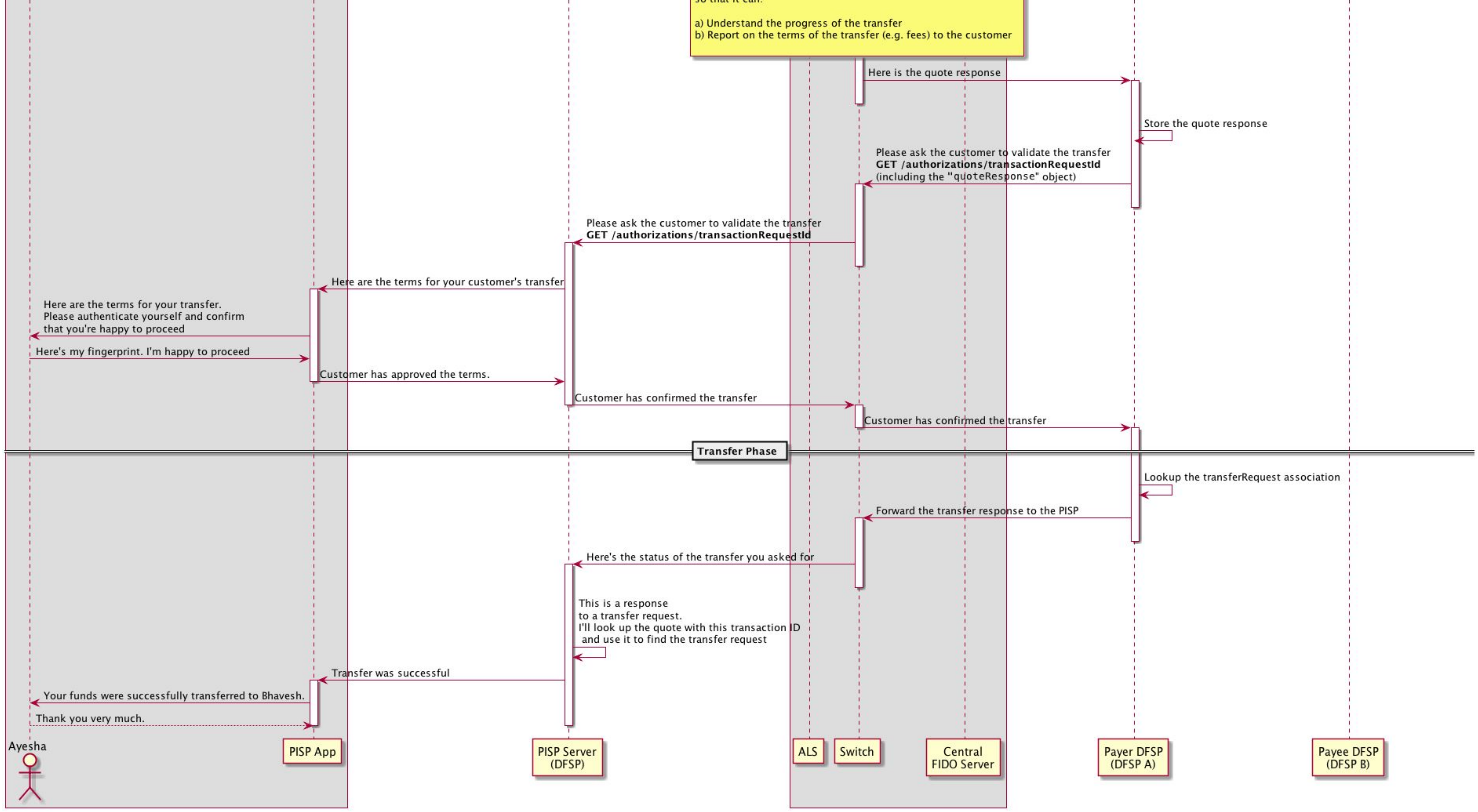
Background - Transfer

- How does a PISP initiate a transfer?
  - Calls `POST /transferRequests` to kick off the whole flow
  - Most of it runs like a normal Request To Pay, except there are a few places where the PISP needs callbacks from the switch

PISP transfer model
(using Merchant Request to Pay Model)


Mobile device
Mojaloop
Ayesha
PISP App
PISP Server (DFSP)
ALS
Switch
Central FIDO Server
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Discovery
I would like to transfer $100 to B@Somewhere
Ayesha would like to transfer $100 to B@Somewhere
What is Ayesha's payer key? It's A@Elsewhere
Which DFSP owns A@Elsewhere? ("GET /parties")
. insert Mojaloop "GET /parties" flow .
DFSP A speaks for B@Somewhere The customer is Bhavesh
System reports customer name is Bhavesh
That's Bhavesh, right?
Yes, it is
Customer is happy that she's sending to the right recipient
Please ask DFSP A to transfer $100 from Ayesha to Bhavesh ("POST /transactionRequests")
Store this request
Please ask DFSP A to transfer $100 from Ayesha to Bhavesh
Agreement Phase
Please provide me with a quotation for this transfer
Please quote on this proposed transfer
Prepare the quotation


Mobile device
Mojaloop
Ayesha
PISP App
PISP Server (DFSP)
ALS
Switch
Central FIDO Server
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)
Agreement Phase
Please provide me with a quotation for this transfer
Please quote on this proposed transfer
Prepare the quotation
Here is the quotation
Now we need to make a change to how things work now.
We need to report this information to the PISP,
so that it can:
a) Understand the progress of the transfer
b) Report on the terms of the transfer (e.g. fees) to the customer
Here is the quote response
Store the quote response
Please ask the customer to validate the transfer
GET /authorizations/transactionRequestId
(including the "quoteResponse" object)
Please ask the customer to validate the transfer
GET /authorizations/transactionRequestId
Here are the terms for your customer's transfer
Here are the terms for your transfer.
Please authenticate yourself and confirm
that you're happy to proceed
Here's my fingerprint. I'm happy to proceed
Customer has approved the terms.
Customer has confirmed the transfer
Customer has confirmed the transfer
Transfer Phase
Lookup the transferRequest association
Forward the transfer response to the PISP
Here's the status of the transfer you asked for
This is a response


a) Understand the progress of the transfer
b) Report on the terms of the transfer (e.g. fees) to the customer
Here is the quote response
Store the quote response
Please ask the customer to validate the transfer
GET /authorizations/transactionRequestId
(including the "quoteResponse" object)
Please ask the customer to validate the transfer
GET /authorizations/transactionRequestId
Here are the terms for your customer's transfer
Here are the terms for your transfer.
Please authenticate yourself and confirm
that you're happy to proceed
Here's my fingerprint. I'm happy to proceed
Customer has approved the terms.
Customer has confirmed the transfer
Customer has confirmed the transfer
Transfer Phase
Lookup the transferRequest association
Forward the transfer response to the PISP
Here's the status of the transfer you asked for
This is a response
to a transfer request.
I'll look up the quote with this transaction ID
and use it to find the transfer request
Transfer was successful
Your funds were successfully transferred to Bhavesh.
Thank you very much.
Ayesha
PISP App
PISP Server (DFSP)
ALS
Switch
Central FIDO Server
Payer DFSP (DFSP A)
Payee DFSP (DFSP B)

mojaloop

Account linking

mojaloop

Linking - Terminology

Authentication ("auth-n"):

- Mutual agreement of identity between two parties.
- *"I am who I say I am."*
- Usually one party is taken for granted
  (by going to *mydfsp.com* I authenticate that I'm talking to my DFSP).
- The other party provides some pre-agreed proof:
  - Knowledge: *"something you know"*
    - e.g., a password, security questions
  - Possession: *"something you have"*
    - e.g., a physical or software security key, mobile device
  - Immutable attributes: *"something you are"*
    - e.g., fingerprint scan, face recognition, other biometrics

Linking - Terminology

Authorization ("auth-z"):

- Permission to perform a given action
    - e.g., initiate a payment, delete a folder, download a file
- "Check this token. It says I am allowed to do this thing."
- Should be explicitly granted for a given action
- OAuth is the most popular flow for granting auth-z
- Auth-n is required when **granting** auth-z but may not be required when **performing the authorized action** (bearer tokens)
    - Sort of like bearer bonds or digitally signed upload URLs for Amazon’s S3 (Simple Storage Service) or GCS (Google Cloud Storage)

Linking - Process

Phase 1: Get secure consent from user to use PISP

1. Users auth-n themselves with PISP (usually in PISP mobile application)
2. Users auth-n themselves with their DFSP (various options)
3. Users auth-z the PISP to "act on their behalf" (e.g., initiate payments)

Phase 2: Upgrade auth-n to use FIDO and share credential

4. Users create a new FIDO credential to use to authenticate with the PISP in future
5. PISP shares details of the new credential with the DFSP so that it can validate future authentications.

Linking - Process

Why upgrade auth-n to use FIDO?

Ultimate goal is a **safer** form of third-party auth-n using FIDO:

- If all participants recognize a user's FIDO credential (public key), they can trust auth-n of the user on other participants' systems if signed with that credential.
- FIDO authenticators keep the credential private keys securely on the device.
- Many new mobile devices have FIDO authenticators built-in and this offers a superior UX and security to other authentication methods.

Linking - FIDO

- Credentials are **private** (only the creator of a credential can use it)

- Therefore, the credential **must** be created by the PISP
  - It can be shared with others, but only the PISP can ask for signatures

- This means the DFSP **must** trust the PISP to handle enrollment.

- **Proposal**: Allow third-parties to create FIDO credentials **on behalf of** others
  - E.g., DFSP could register FIDO credentials that PISP would use for transactions.

Linking - Architecture

- Design allows the Mojaloop Switch to run services centrally to handle the steps that DFSPs can’t handle themselves such as:
  - AuthN User (e.g. host login page on public Web)
  - AuthZ Consent (e.g. host consent page on public Web)
  - FIDO Server (e.g. generate auth-n challenge, store credentials, etc)

- This simplifies the design initially, while allowing for DFSPs to bring their own services online in the future in a phased approach

- All backend interactions happen via Mojaloop API calls (minimize front-channel interactions via the Web)

Designs - Linking

Requirements

1. User Authenticates with their DFSP (AuthN)
2. DFSP trusts that the user saw what they are authorizing the PISP to do and agreed to it (Grant Consent)

E.g. OAuth2 solves this by redirecting the user via the Web

Proposal

1. The user authenticates directly with the DFSP (login to website, supply OTP)
2. User is presented with details of authorization request by the DFSP (shown on DFSP website, sent via SMS by DFSP)

Designs - Linking

OAuth2

- OAuth2 is the defacto standard on the Web for AuthZ.
- Mojaloop is not the Web. But, we can leverage the lessons learned developing OAuth and the extra security we have in Mojaloop

Plan

- Use OAuth2-based framework + Pushed Authorization Requests
  - This bundles up all the various parameters into a single chunk at the **start** of the process.
- Use Mojaloop network for secure comms between the PISP and DFSP
- AuthN of the user and collecting consent can be done via SMS OTP, the Web, push messages to DFSP app (DFSP decides)

Linking - FIDO escalation

Once the PISP has consent, they can trigger the FIDO registration process:

1. PISP Server asks a central FIDO server for a "challenge".

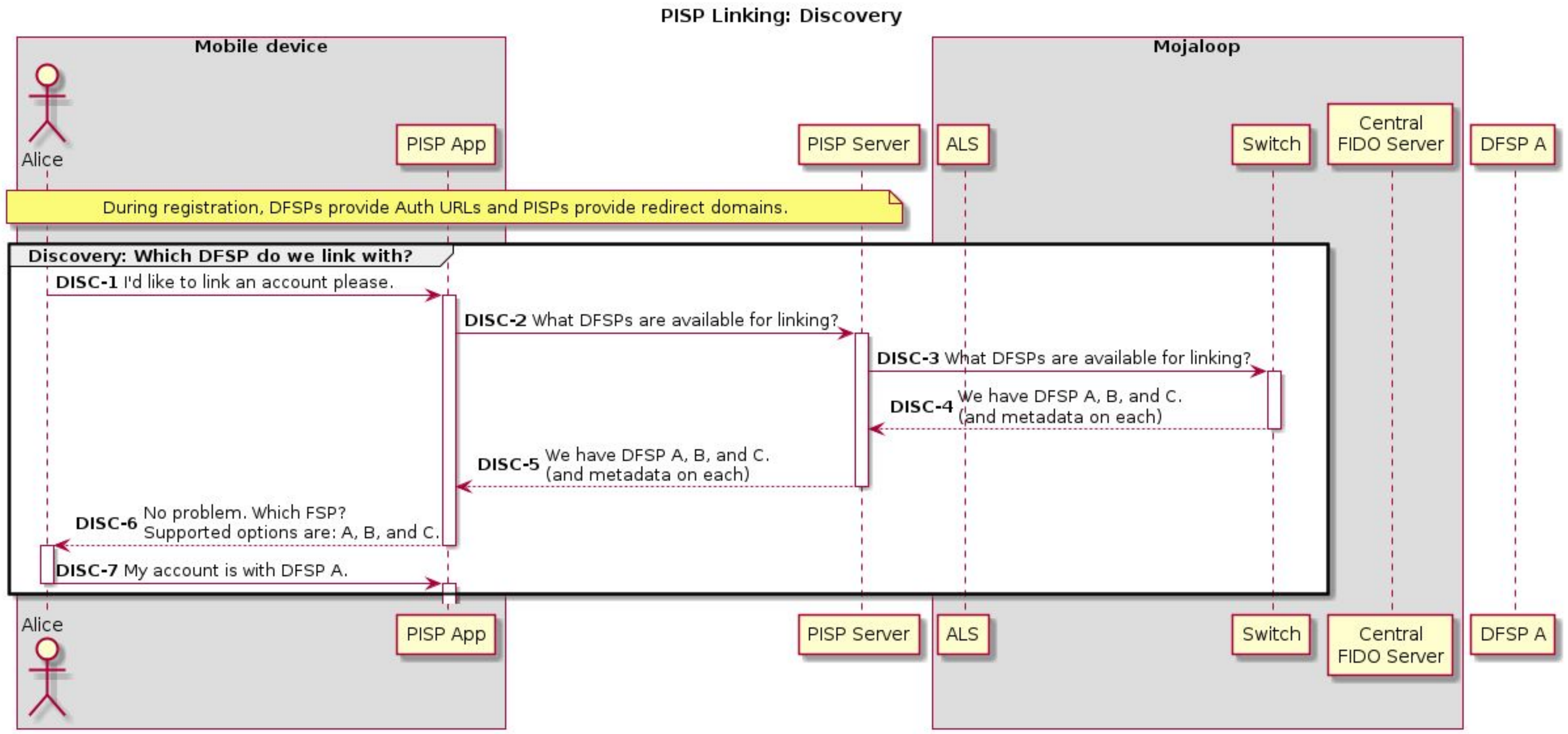
2. PISP App asks Alice's authenticator to:
   a. generate a FIDO credential,
      - (this credential can **only** be used by the application that registered the key)

   b. sign the challenge, and
   c. return the signed challenge and public FIDO credential

3. PISP forwards the FIDO credential to the DFSP, the DFSP records the credential against the user's account, and the FIDO key can be used in the future to authenticate the user

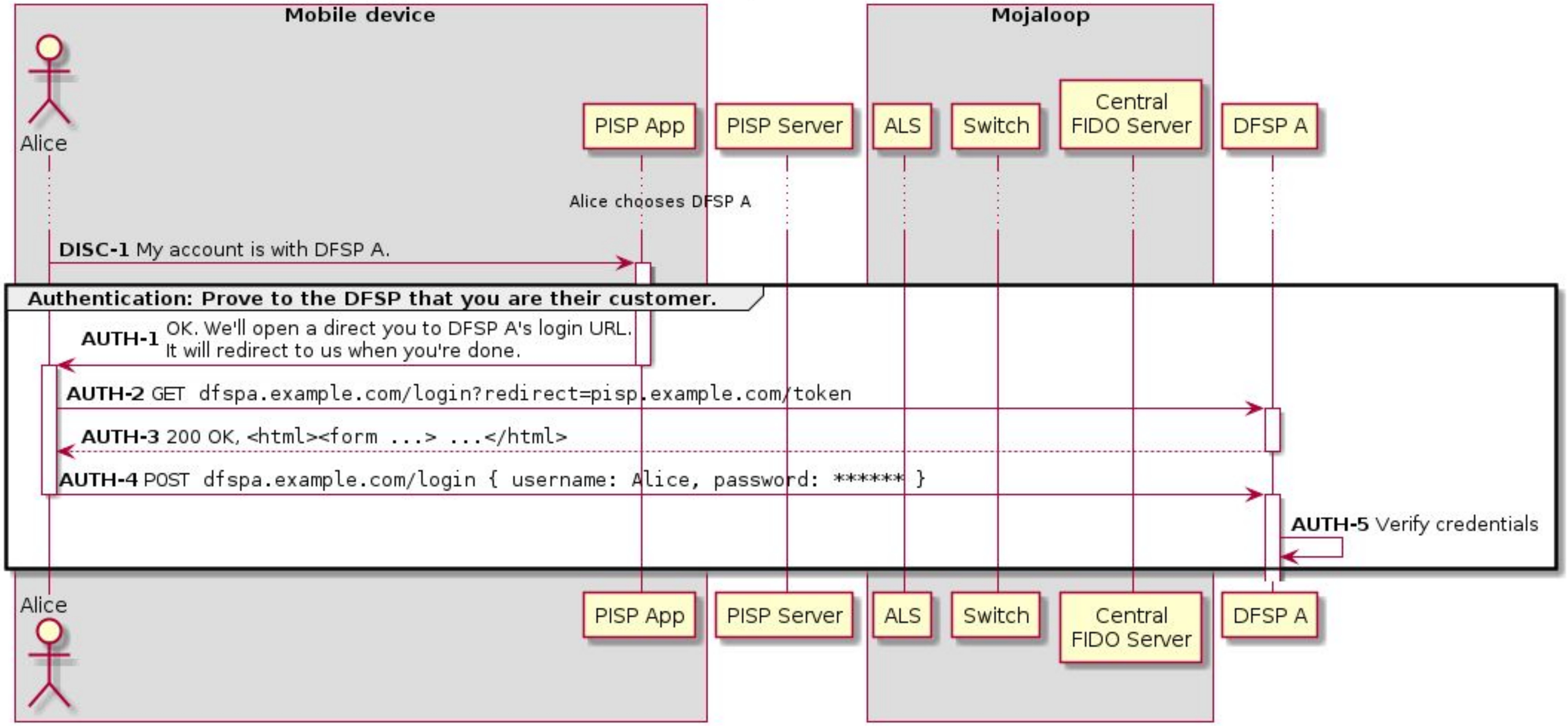
High Level Flows

For more detailed flows, go to
github.com/jgeewax/mojaloop-pisp


PISP Linking: Discovery
Mobile device
Mojaloop
Alice
PISP App
PISP Server
ALS
Switch
Central FIDO Server
DFSP A
During registration, DFSPs provide Auth URLs and PISPs provide redirect domains.
Discovery: Which DFSP do we link with?
DISC-1 I'd like to link an account please.
DISC-2 What DFSPs are available for linking?
DISC-3 What DFSPs are available for linking?
DISC-4 We have DFSP A, B, and C. (and metadata on each)
DISC-5 We have DFSP A, B, and C. (and metadata on each)
DISC-6 No problem. Which FSP? Supported options are: A, B, and C.
DISC-7 My account is with DFSP A.
Alice
PISP App
PISP Server
ALS
Switch
Central FIDO Server
DFSP A

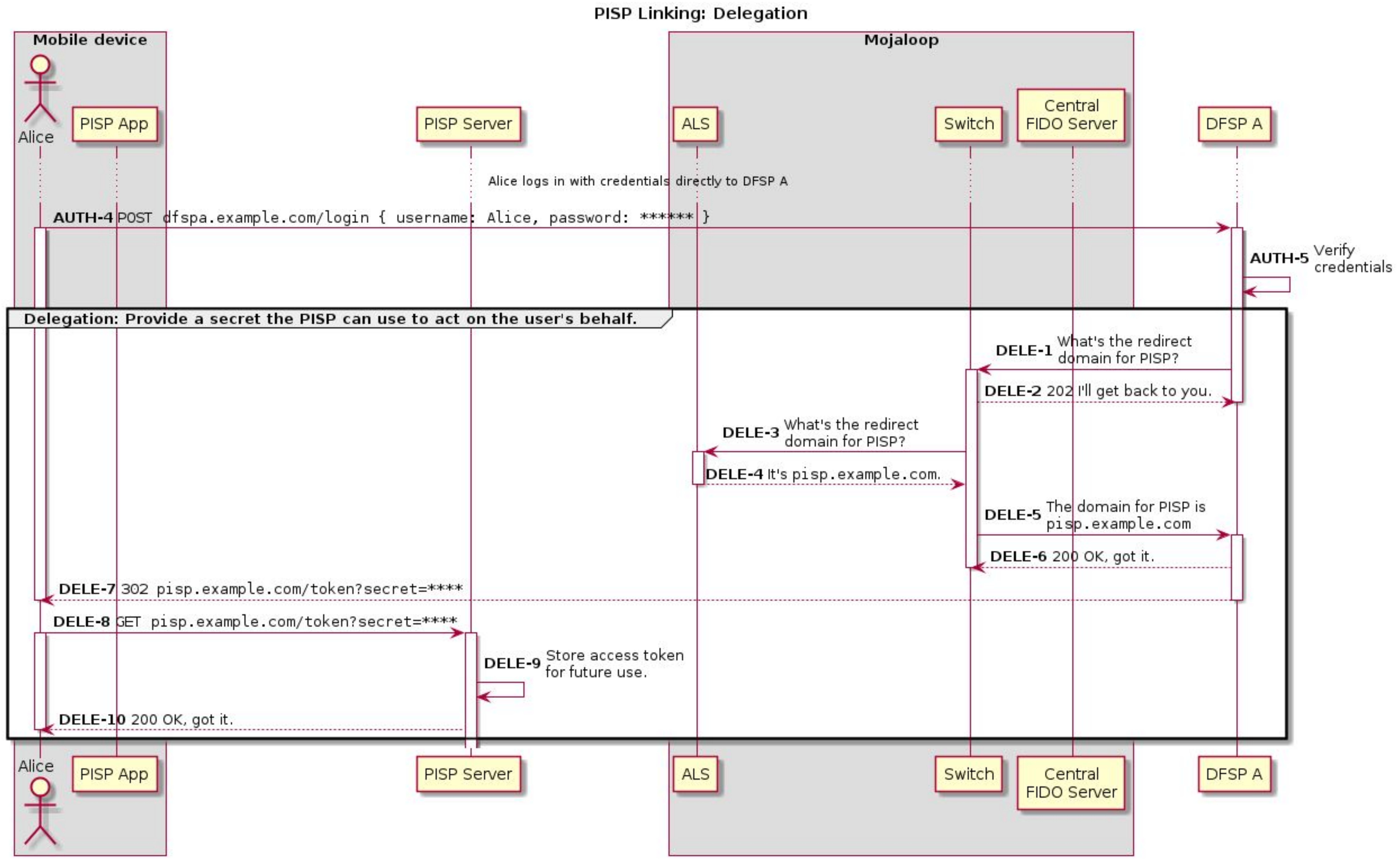
mojaloop

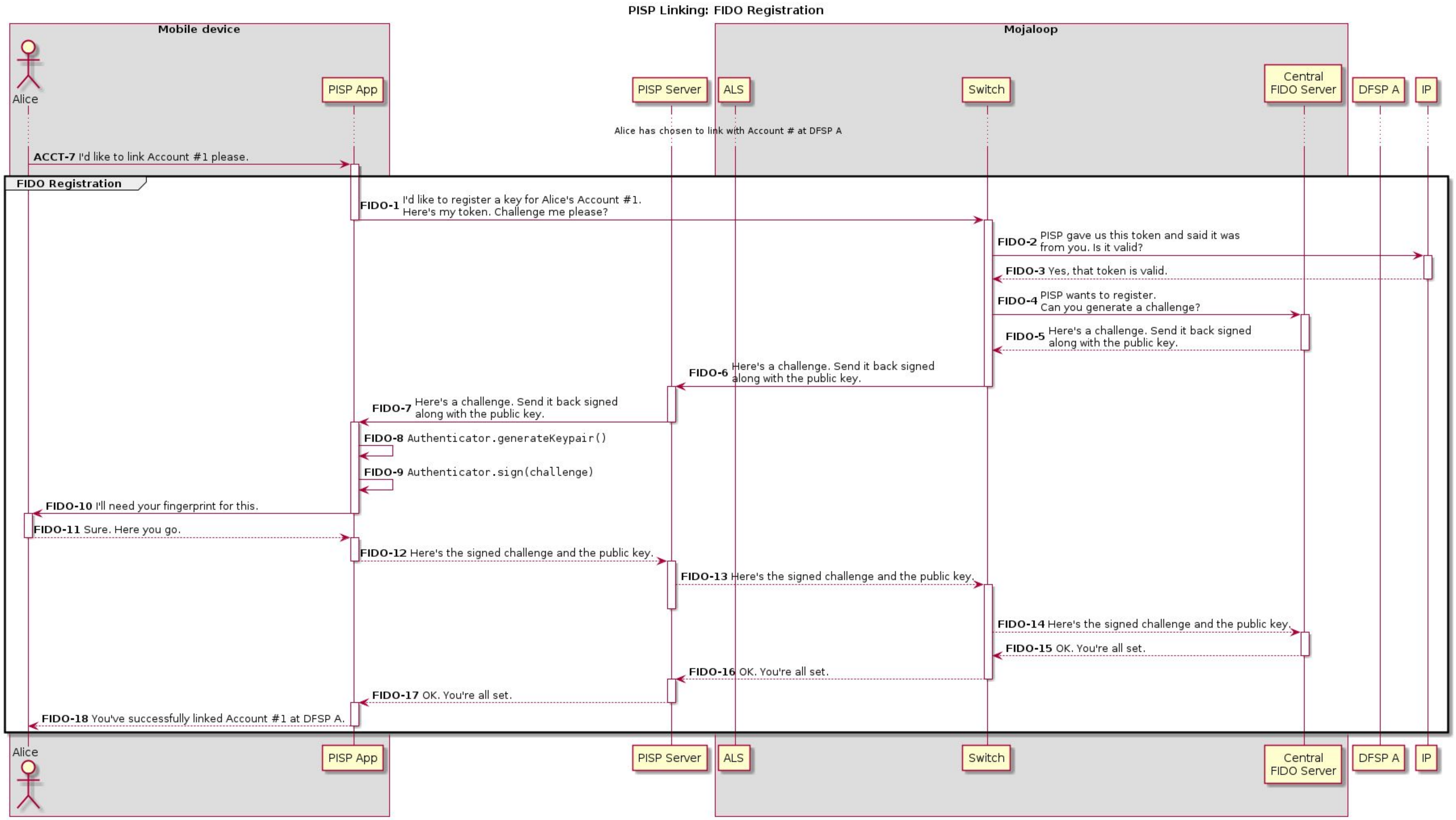
PISP Linking: Authentication



Mobile device
Mojaloop
Alice
PISP App
PISP Server
ALS
Switch
Central FIDO Server
DFSP A
Alice chooses DFSP A
DISC-1 My account is with DFSP A.
Authentication: Prove to the DFSP that you are their customer.
AUTH-1 OK. We'll open a direct you to DFSP A's login URL. It will redirect to us when you're done.
AUTH-2 GET dfspa.example.com/login?redirect=pisp.example.com/token
AUTH-3 200 OK, <html><form ...> ...</html>
AUTH-4 POST dfspa.example.com/login { username: Alice, password: ****** }
AUTH-5 Verify credentials

mojaloop


PISP Linking: Delegation
Mobile device
Mojaloop
Alice
PISP App
PISP Server
ALS
Switch
Central FIDO Server
DFSP A
Alice logs in with credentials directly to DFSP A
AUTH-4 POST dfspa.example.com/login { username: Alice, password: ****** }
AUTH-5 Verify credentials
Delegation: Provide a secret the PISP can use to act on the user's behalf.
DELE-1 What's the redirect domain for PISP?
DELE-2 202 I'll get back to you.
DELE-3 What's the redirect domain for PISP?
DELE-4 It's pisp.example.com.
DELE-5 The domain for PISP is pisp.example.com
DELE-6 200 OK, got it.
DELE-7 302 pisp.example.com/token?secret=****
DELE-8 GET pisp.example.com/token?secret=****
DELE-9 Store access token for future use.
DELE-10 200 OK, got it.
Alice
PISP App
PISP Server
ALS
Switch
Central FIDO Server
DFSP A



Alice has chosen to link with Account # at DFSP A

ACCT-7 I'd like to link Account #1 please.

FIDO-1 I'd like to register a key for Alice's Account #1. Here's my token. Challenge me please?

FIDO-2 PISP gave us this token and said it was from you. Is it valid?

FIDO-3 Yes, that token is valid.

FIDO-4 PISP wants to register. Can you generate a challenge?

FIDO-5 Here's a challenge. Send it back signed along with the public key.

FIDO-6 Here's a challenge. Send it back signed along with the public key.

FIDO-7 Here's a challenge. Send it back signed along with the public key.

FIDO-8 `Authenticator.generateKeypair()`

FIDO-9 `Authenticator.sign(challenge)`

FIDO-10 I'll need your fingerprint for this.

FIDO-11 Sure. Here you go.

FIDO-12 Here's the signed challenge and the public key.

FIDO-13 Here's the signed challenge and the public key.

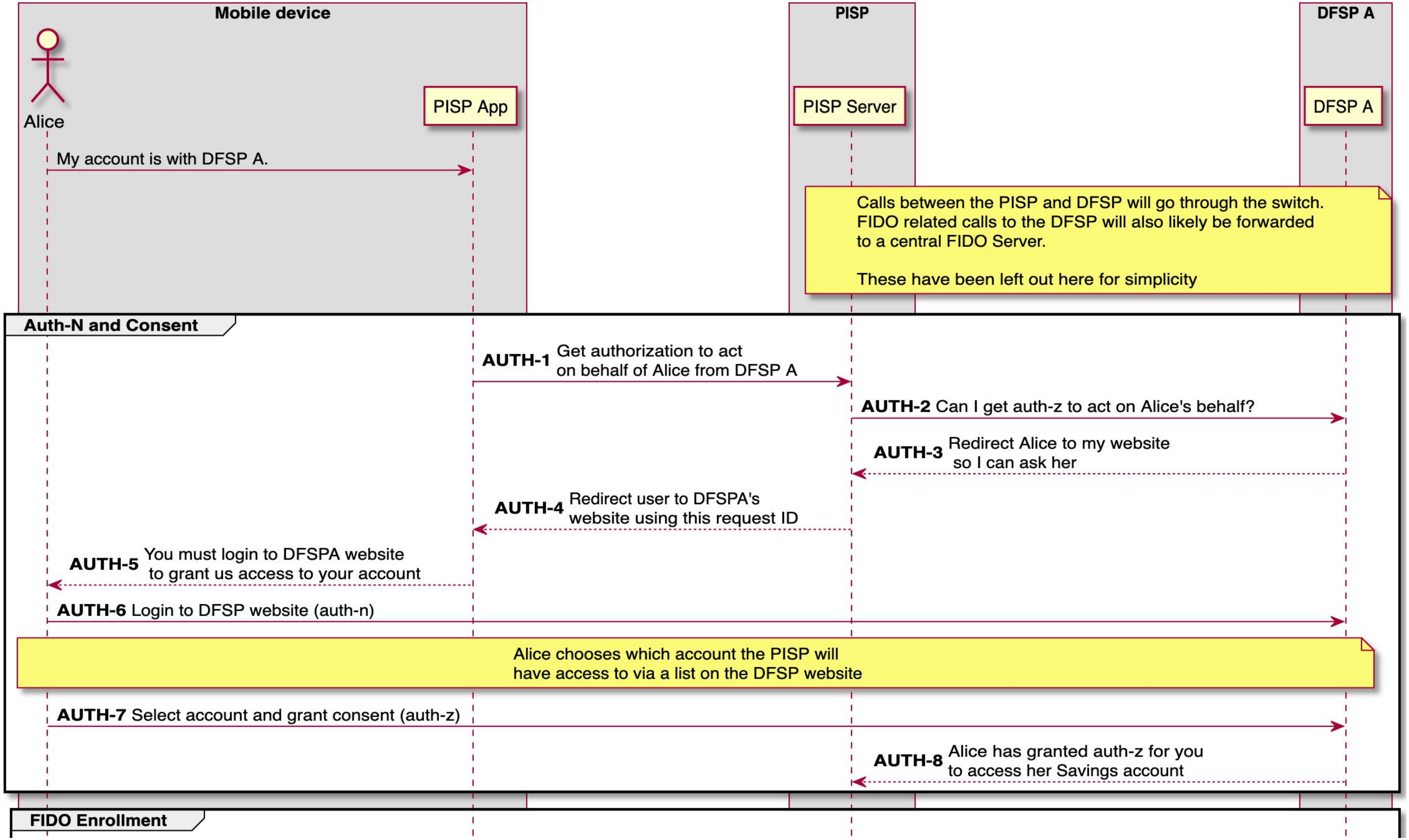
FIDO-14 Here's the signed challenge and the public key.

FIDO-15 OK. You're all set.

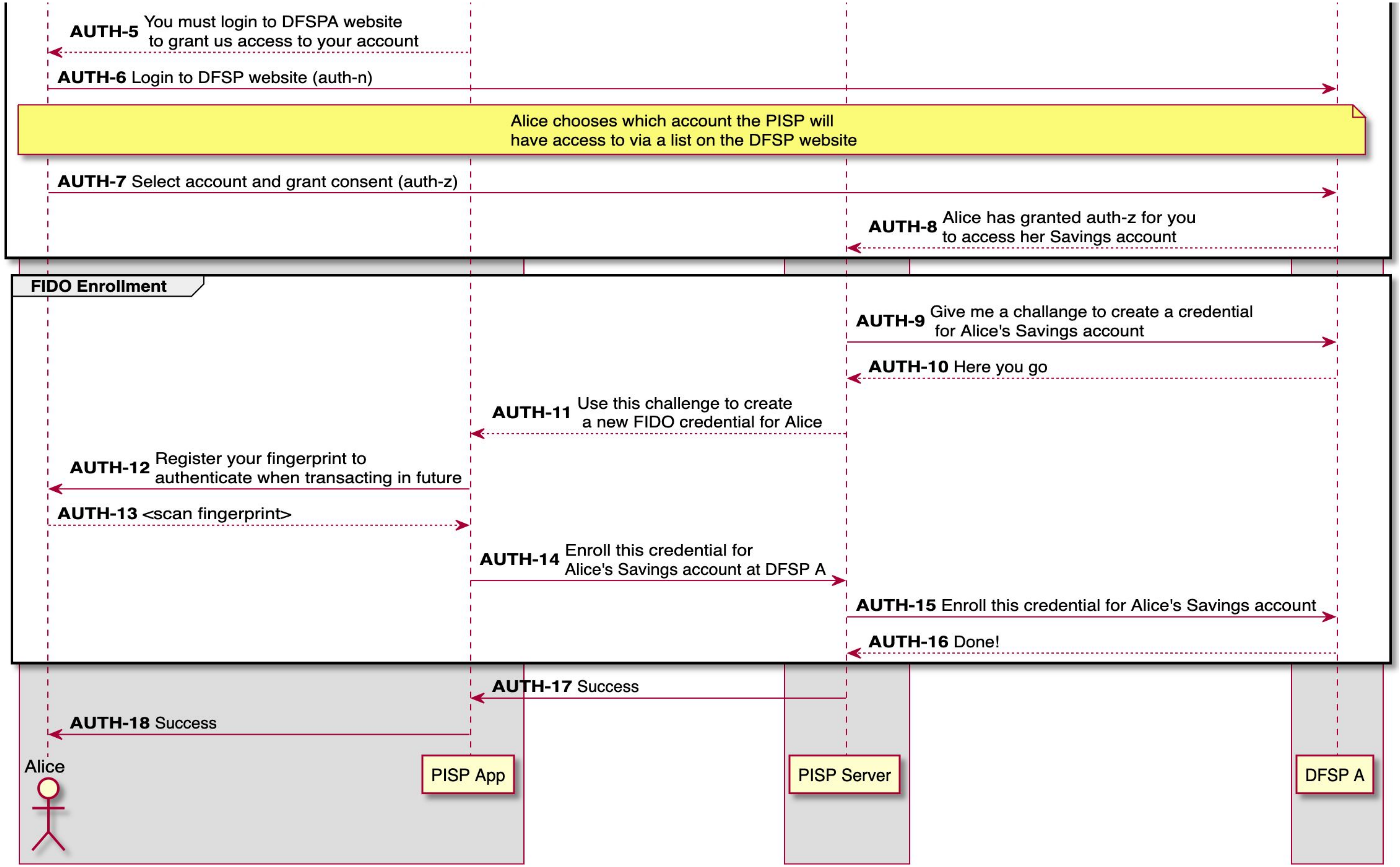
FIDO-16 OK. You're all set.

FIDO-17 OK. You're all set.

FIDO-18 You've successfully linked Account #1 at DFSP A.


Mobile device
Alice
PISP App
PISP
PISP Server
DFSP A
DFSP A
My account is with DFSP A.
Calls between the PISP and DFSP will go through the switch. FIDO related calls to the DFSP will also likely be forwarded to a central FIDO Server.
These have been left out here for simplicity
Auth-N and Consent
AUTH-1 Get authorization to act on behalf of Alice from DFSP A
AUTH-2 Can I get auth-z to act on Alice's behalf?
AUTH-3 Redirect Alice to my website so I can ask her
AUTH-4 Redirect user to DFSPA's website using this request ID
AUTH-5 You must login to DFSPA website to grant us access to your account
AUTH-6 Login to DFSP website (auth-n)
Alice chooses which account the PISP will have access to via a list on the DFSP website
AUTH-7 Select account and grant consent (auth-z)
AUTH-8 Alice has granted auth-z for you to access her Savings account
FIDO Enrollment

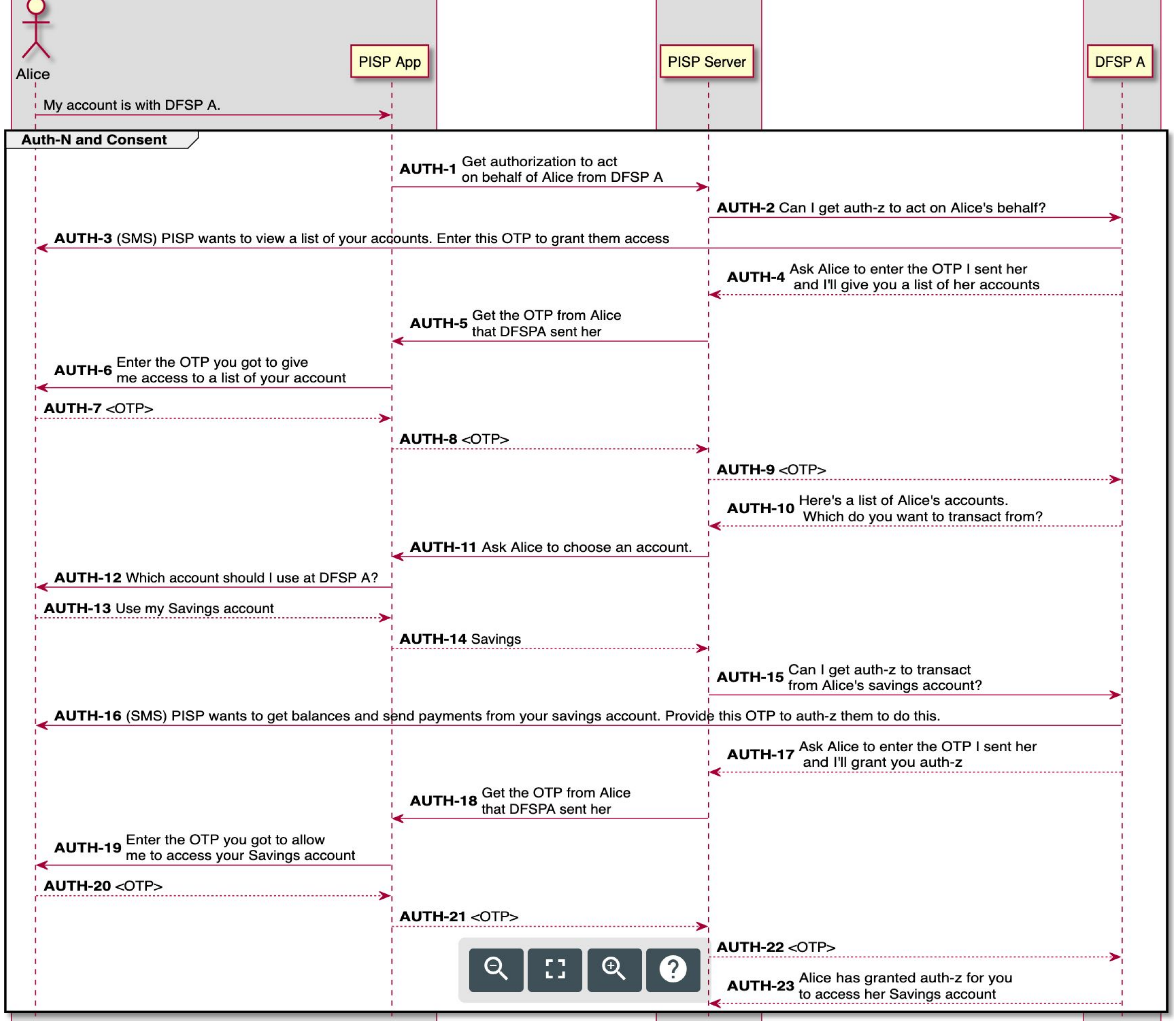
mojaloop


AUTH-5 You must login to DFSPA website to grant us access to your account
AUTH-6 Login to DFSP website (auth-n)
Alice chooses which account the PISP will have access to via a list on the DFSP website
AUTH-7 Select account and grant consent (auth-z)
AUTH-8 Alice has granted auth-z for you to access her Savings account
FIDO Enrollment
AUTH-9 Give me a challange to create a credential for Alice's Savings account
AUTH-10 Here you go
AUTH-11 Use this challenge to create a new FIDO credential for Alice
AUTH-12 Register your fingerprint to authenticate when transacting in future
AUTH-13 <scan fingerprint>
AUTH-14 Enroll this credential for Alice's Savings account at DFSP A
AUTH-15 Enroll this credential for Alice's Savings account
AUTH-16 Done!
AUTH-17 Success
AUTH-18 Success
Alice
PISP App
PISP Server
DFSP A

mojaloop

Variation:

Auth-N and Consent via SMS OTP



My account is with DFSP A.

AUTH-1 Get authorization to act on behalf of Alice from DFSP A

AUTH-2 Can I get auth-z to act on Alice's behalf?

AUTH-3 (SMS) PISP wants to view a list of your accounts. Enter this OTP to grant them access

AUTH-4 Ask Alice to enter the OTP I sent her and I'll give you a list of her accounts

AUTH-5 Get the OTP from Alice that DFSPA sent her

AUTH-6 Enter the OTP you got to give me access to a list of your account

AUTH-7 <OTP>

AUTH-8 <OTP>

AUTH-9 <OTP>

AUTH-10 Here's a list of Alice's accounts. Which do you want to transact from?

AUTH-11 Ask Alice to choose an account.

AUTH-12 Which account should I use at DFSP A?

AUTH-13 Use my Savings account

AUTH-14 Savings

AUTH-15 Can I get auth-z to transact from Alice's savings account?

AUTH-16 (SMS) PISP wants to get balances and send payments from your savings account. Provide this OTP to auth-z them to do this.

AUTH-17 Ask Alice to enter the OTP I sent her and I'll grant you auth-z

AUTH-18 Get the OTP from Alice that DFSPA sent her

AUTH-19 Enter the OTP you got to allow me to access your Savings account

AUTH-20 <OTP>

AUTH-21 <OTP>

AUTH-22 <OTP>

AUTH-23 Alice has granted auth-z for you to access her Savings account

mojaloop

API Changes (tentative)

mojaloop

API Changes (tentative)

New Resources

- `/authorizationRequests` - starts the Pushed Authorization Request OAuth2 flow
- `POST /authorizations/{id}` - register a new FIDO Key

Modified Resources

- `PUT /authorizations/{id}` - Now will return the Quote response object along with authorization request *(shout out to team Coil)*
- `/transactionRequests` - Allow for an *initiator*, who is not the sending or receiving DFSP

Keep an eye out on the #pisp channel for a more thorough Spec/PR

Next Steps

mojaloop

Next Steps

- Keep an eye on the `#pisp` Slack channel

- Get in touch with us if you want to contribute ideas/use cases/outrage
  - especially if your use case doesn't work with what we've presented

- Find links to work-in-progress docs
  - mojaloop-pisp

- In active development, once design is finalized we'll be dividing the work among the community
  - Google is writing code to make this happen
  - Coil planning to contribute OAuth components
  - ModusBox + Crosslake involved in Design and Writing code