



FIDO & FEDERATION (& A SMALL BIT OF IOT) — BETTER TOGETHER



Paul Madsen
Office of the CTO, Ping Identity

Made for each other

Mature federation protocol seeks youthful authentication standard for integrations AND MORE. I enjoy long redirects on the browser, but detest form fill. I'm tired of insecure password posers - and am looking for something real. If you think you are 'Something I (Should) Have', let's Connect!

FIDO-based authentication can both

- Complement federated authentication
- Compete with federated authentication

Federation

- A model of identity management where the different components of a given transaction are distributed across actors
 - One actor relies on the identity data that another actor provides
 - Manifests in issuance, storage, presentation, and validation of 'security tokens'
- Archetypical manifestation is Web SSO
- May cross policy boundaries, e.g. business partners, enterprise/SaaS, education institutions, social providers
- Federation standards define
 - semantics of token (authn, authz, attributes)
 - Token format (XML -> JSON)
 - Protocols for moving tokens over network (SOAP -> REST)

- Security Assertion Markup Language
- Grand-daddy of federation protocols
- Defines a powerful framework by which identity attributes can be asserted and delivered across network
- Current default SSO protocol for higher-ed, B2B, and SaaS.

OAuth 2.0

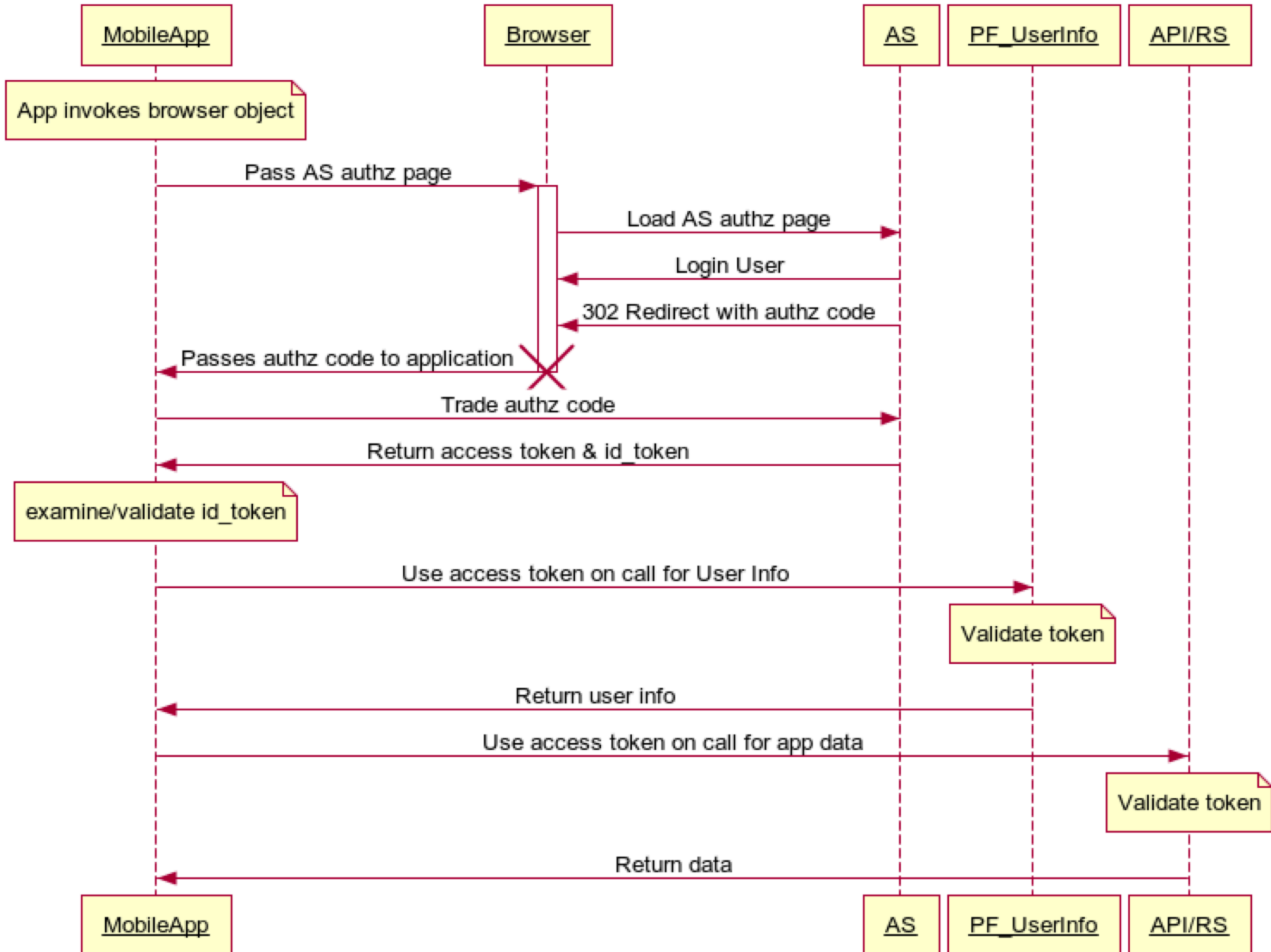
- OAuth 2.0 defines an authentication & authorization framework for API access
- Notably, can be leveraged by native mobile apps calling their corresponding APIs
- Built in support for user-consent step as part of token issuance process – thus relevance to consumer applications
- Emerged from consumer world, standardized under IETF in 2013 to reflect enterprise use cases

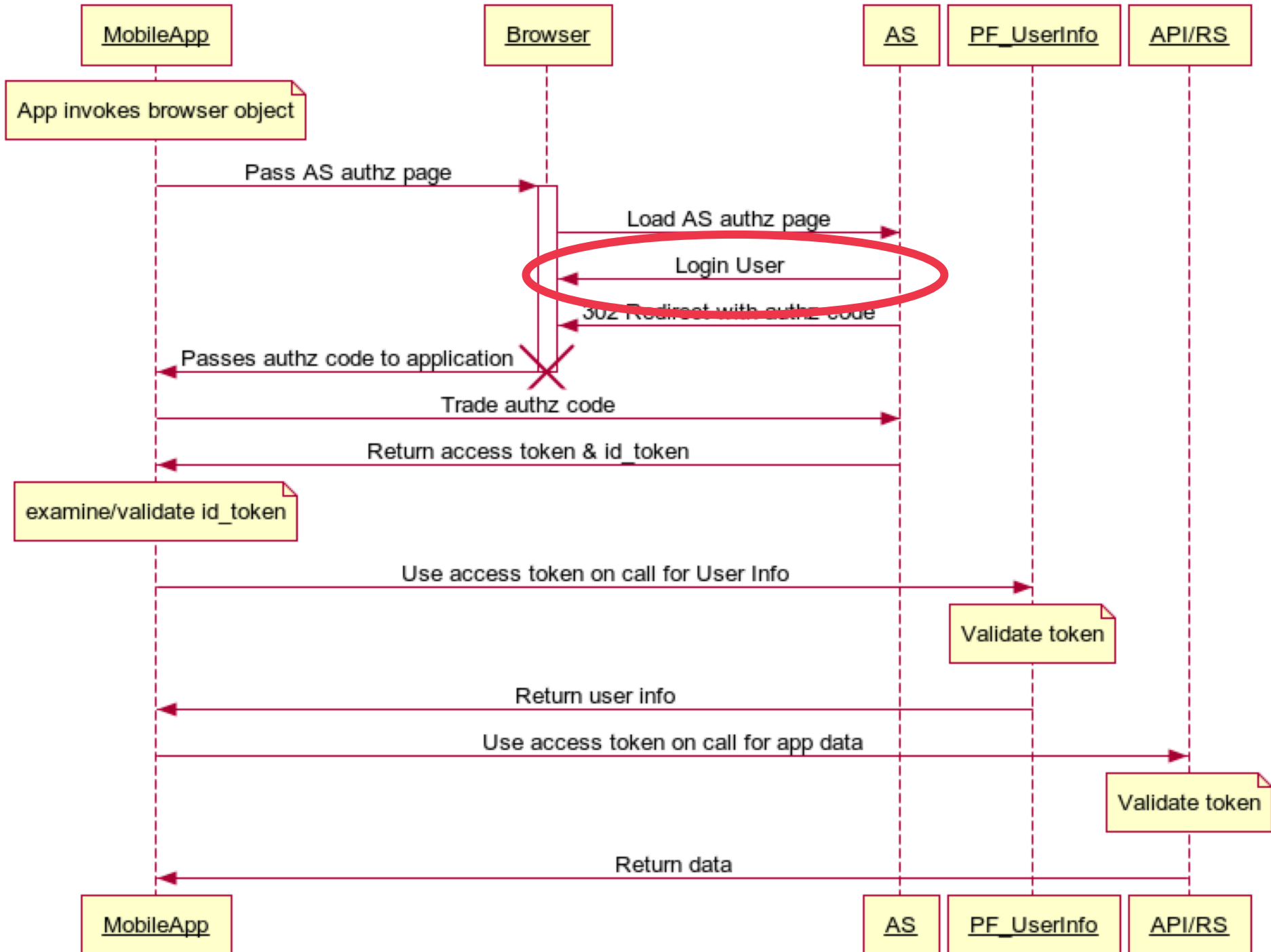
OpenID Connect 1.0

- OpenID Connect normalizes an identity layer on top of OAuth 2.0
- Newly standardized from OpenID Foundation
- Adds identity semantics to base OAuth flow to enable
 - a web SSO model (like SAML)
 - User attribute sharing
- Arguably matches functionality of SAML, though with a more modern architecture

Federation's
dirty little
secret







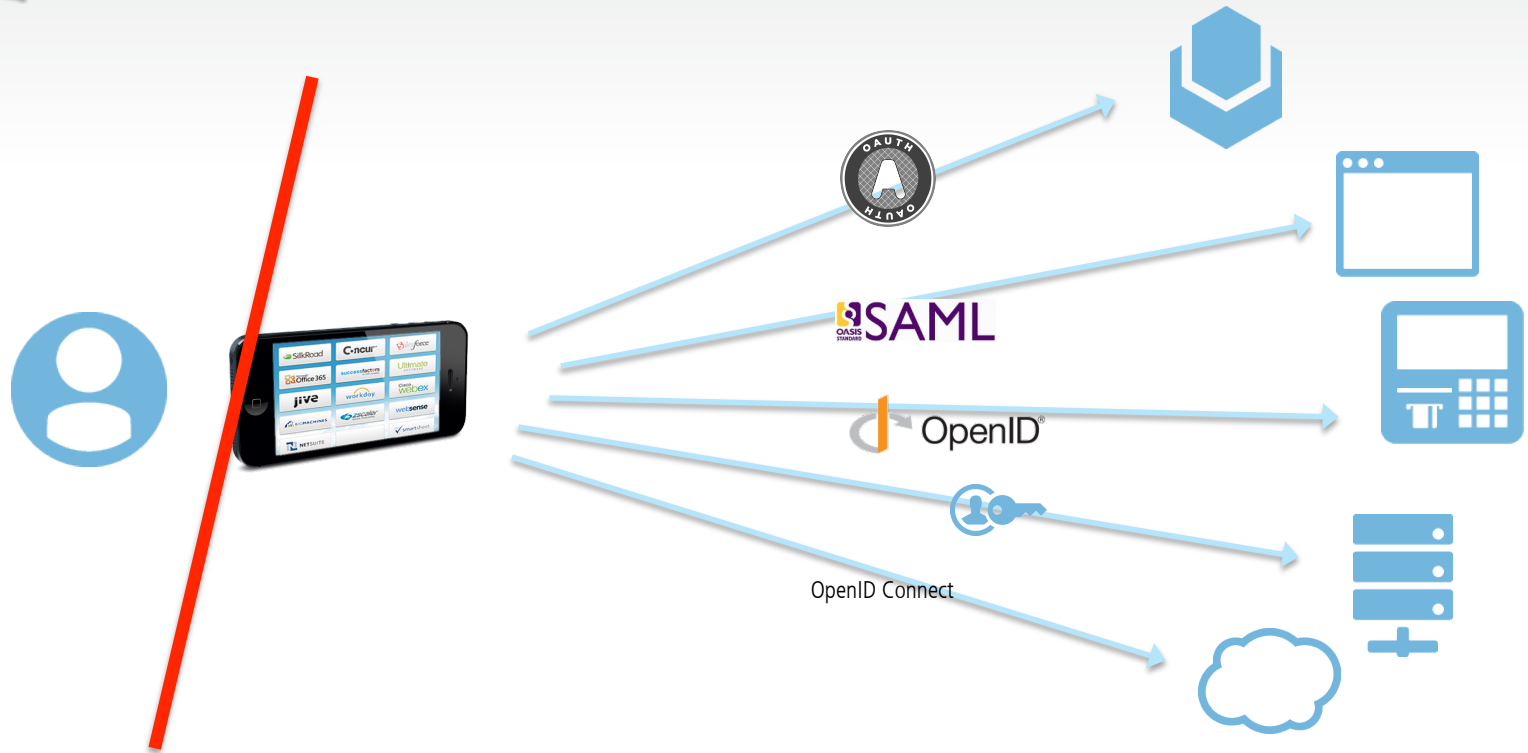
Brittleness in IdM?

- Brittle is breaking one component of an identity architecture when you change another.
- For instance, when you add a
 - business partner
 - Authentication factor
- Brittleness happens when architecture components are too tightly bound to each other
- Abstraction layers insulate components from each other – and so guard against brittleness



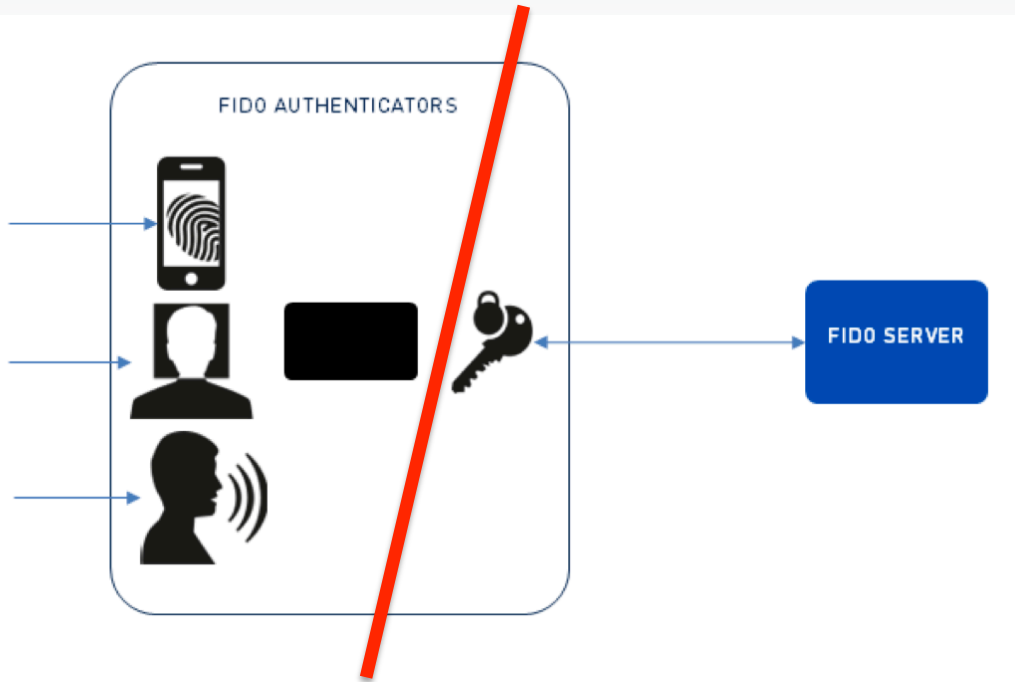
<https://www.flickr.com/photos/hzader/13040698575>

Federation & brittleness?



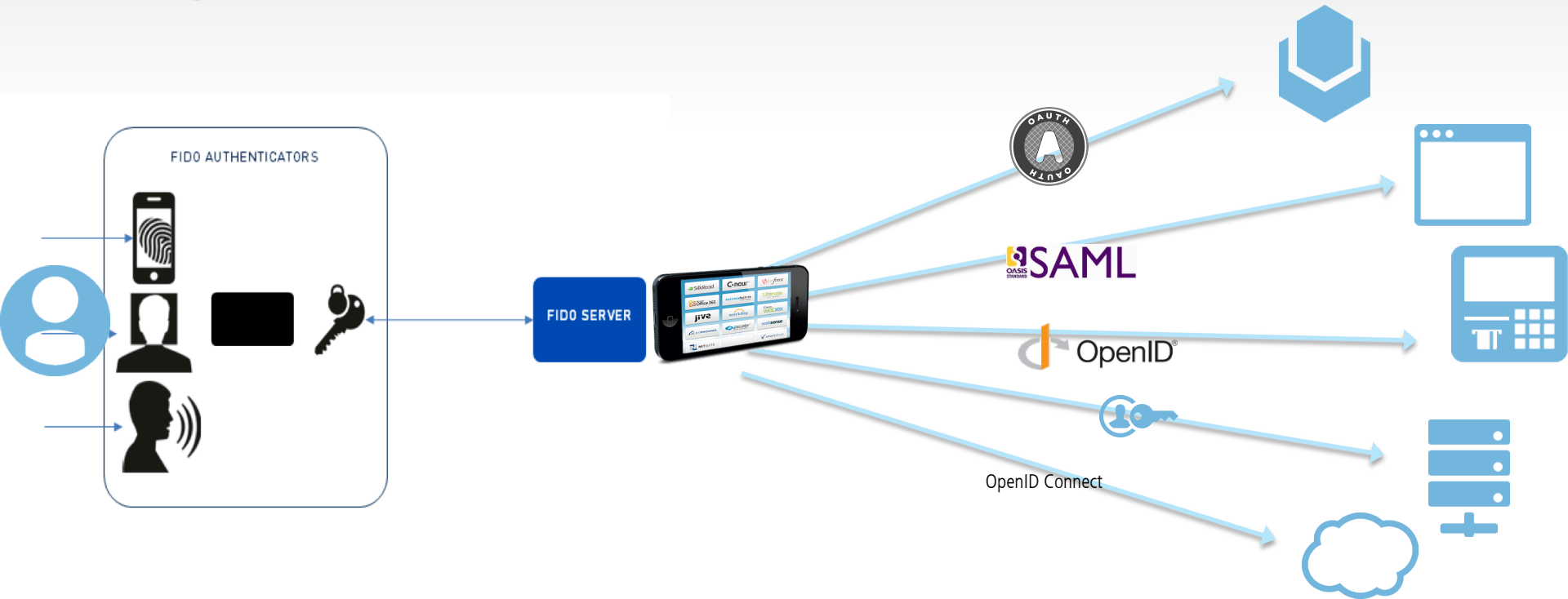
1. Separates the application from the specifics of the business partner
2. And so allow for the authenticating party to change (e.g. new customer, new partner, etc) without impacting the application – becomes a configuration & policy issue

FIDO & brittleness?



1. Separates the authentication server from the specific authentication model performed by the user to login to device
2. And so allow for authentication models to change (eg retinal scan, etc) without impacting the authentication server – becomes a configuration & policy issue

FIDO & Federation



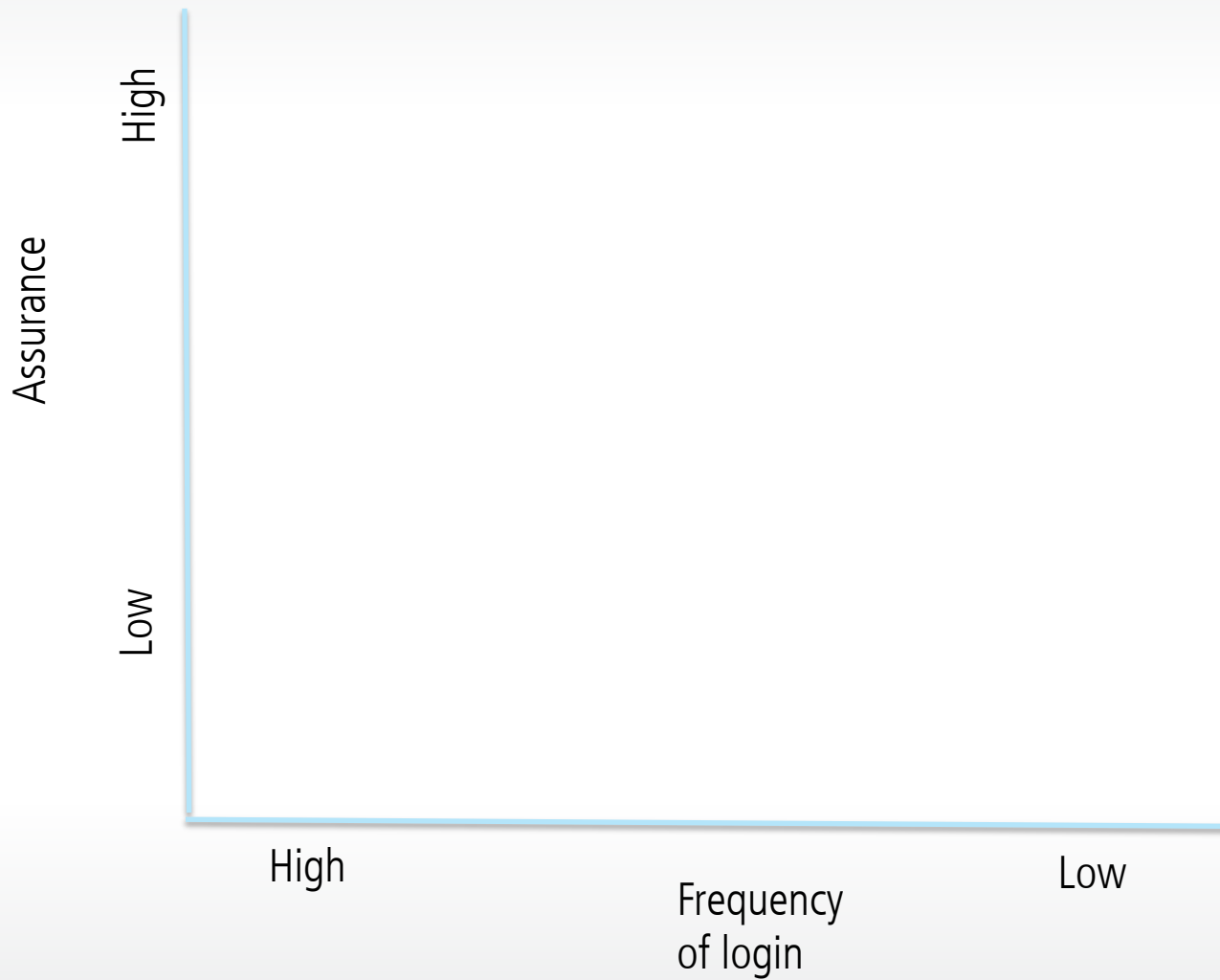
1. Completely abstract user authentication (both details & server) from the applications
2. Allowing the authentication method & provider to change without impacting the application

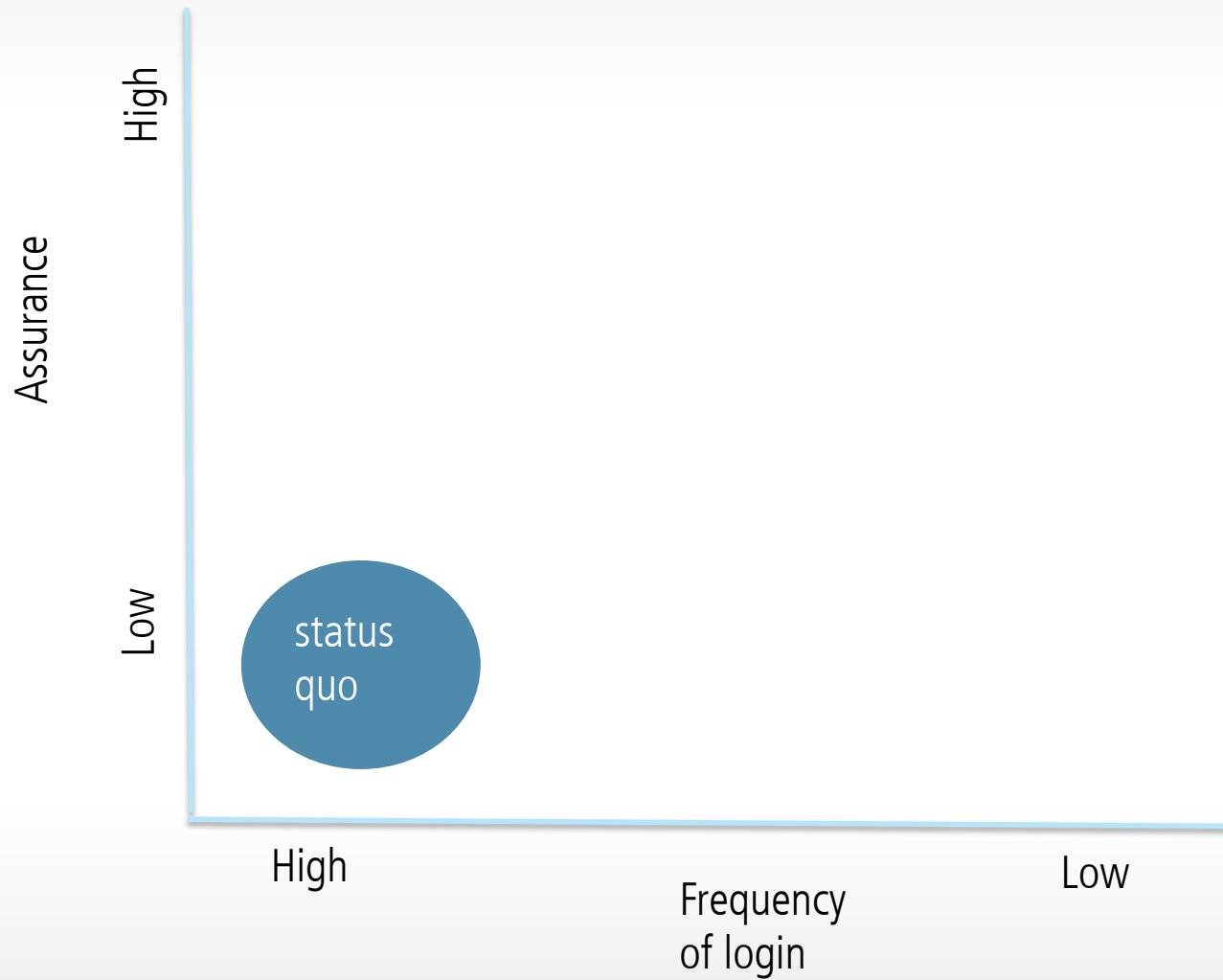
- FIDO

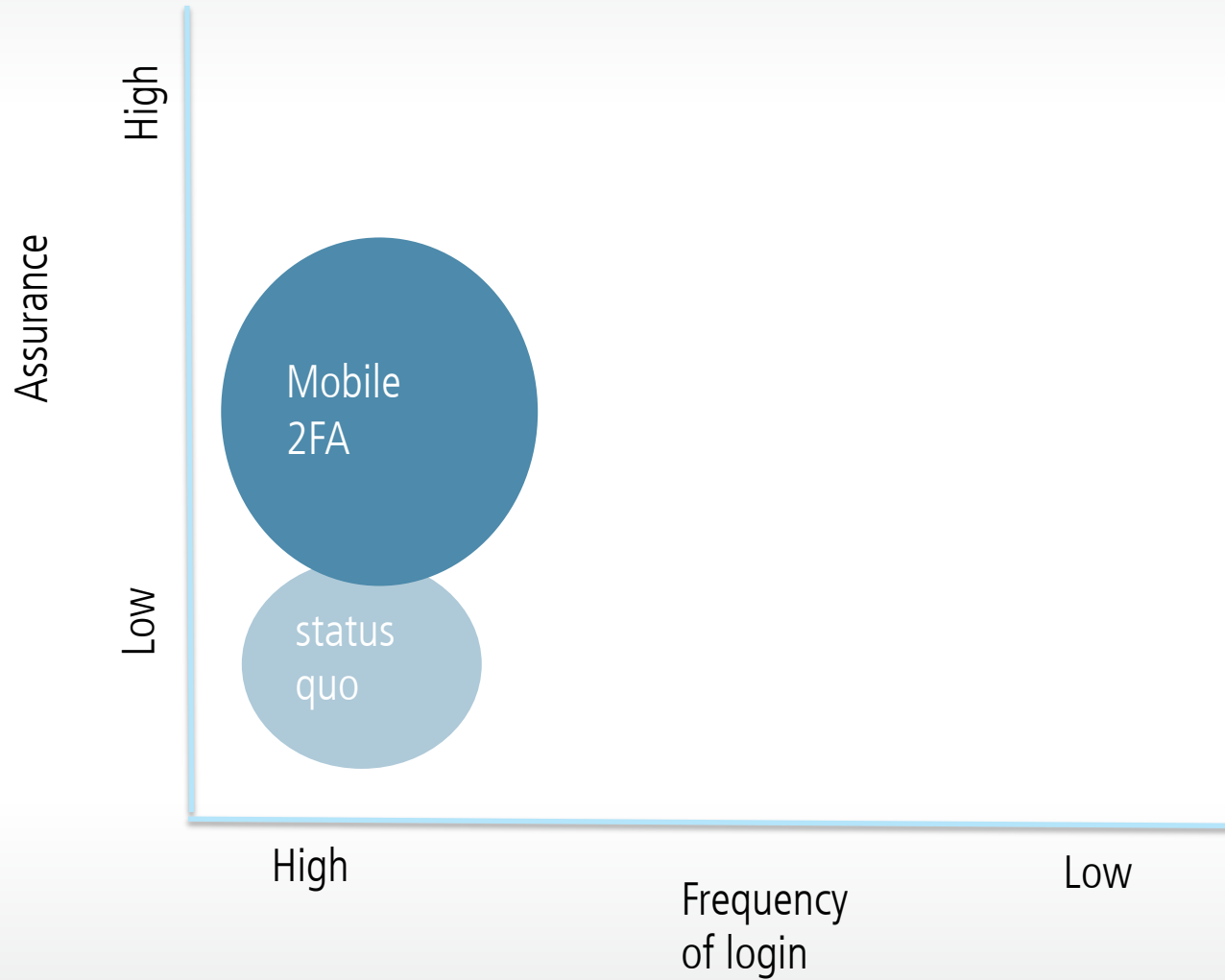
- Insulates authentication server from specific authenticators
- Focused solely on **primary** authentication
- Does not support attribute sharing
- Can communicate details of authentication from device to server

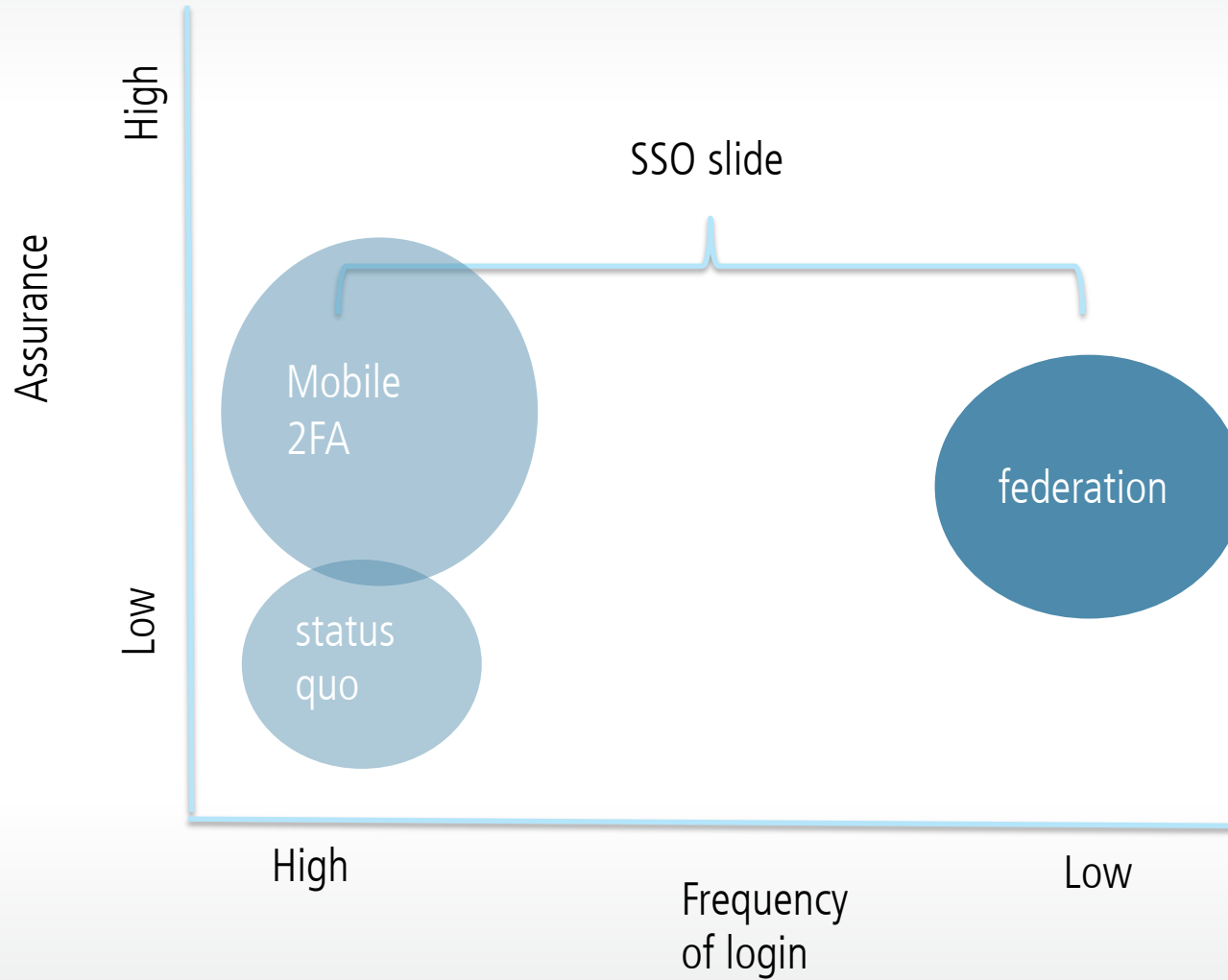
- Federation

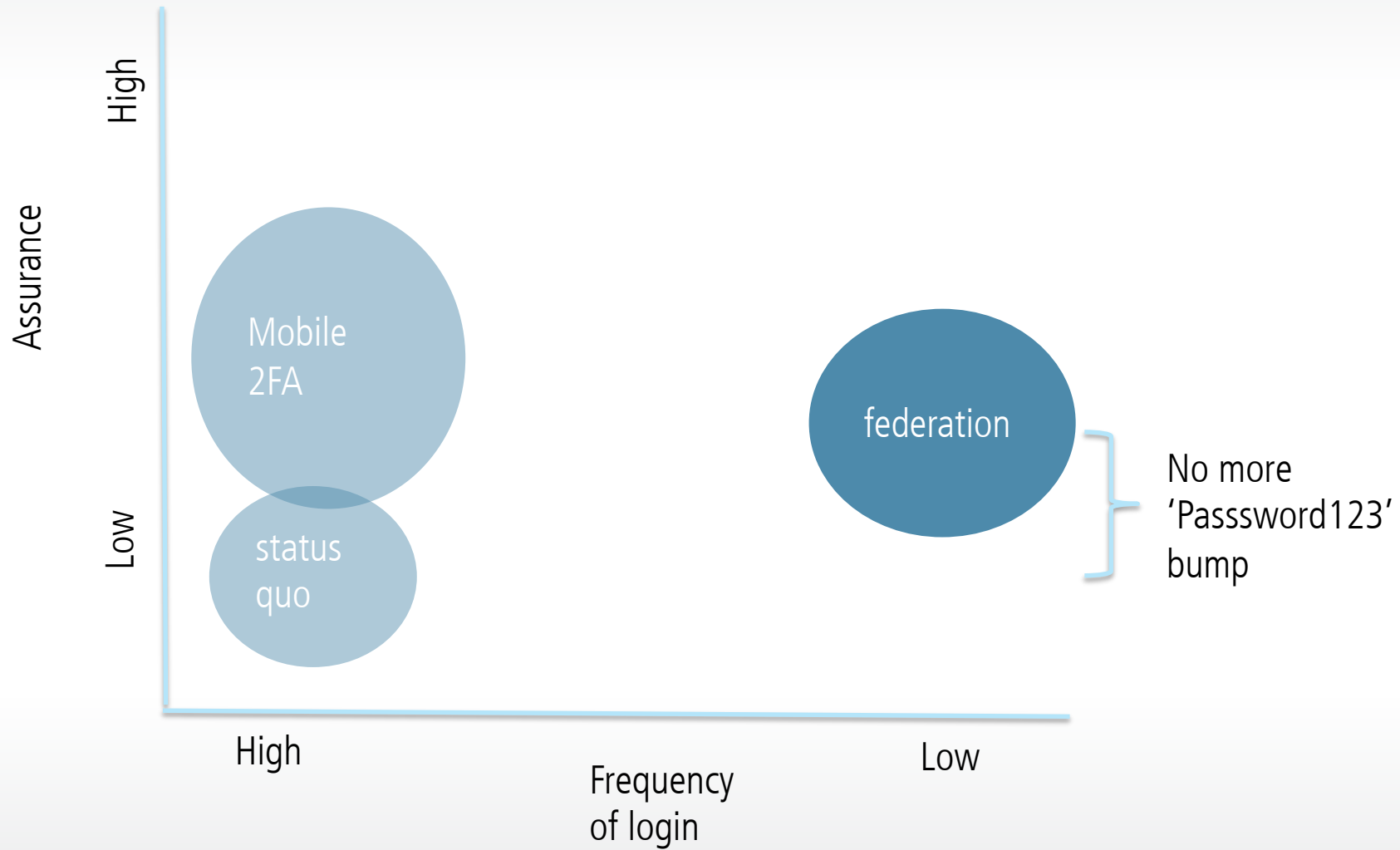
- Insulates application from specific identity providers
- Does not address primary authentication
- Does enable **secondary** authentication & attribute sharing
- Can communicate details of authentication from IdP to SP

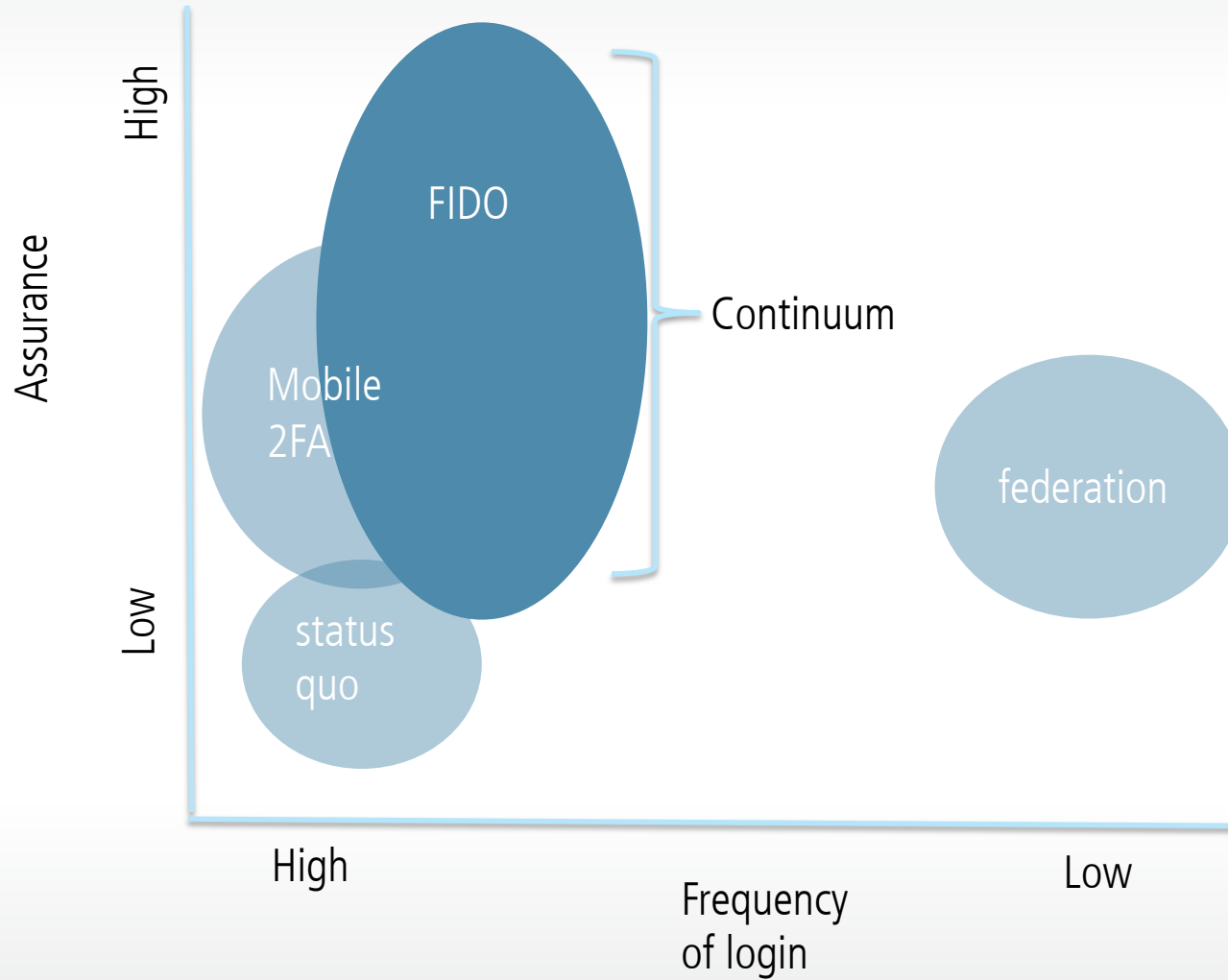


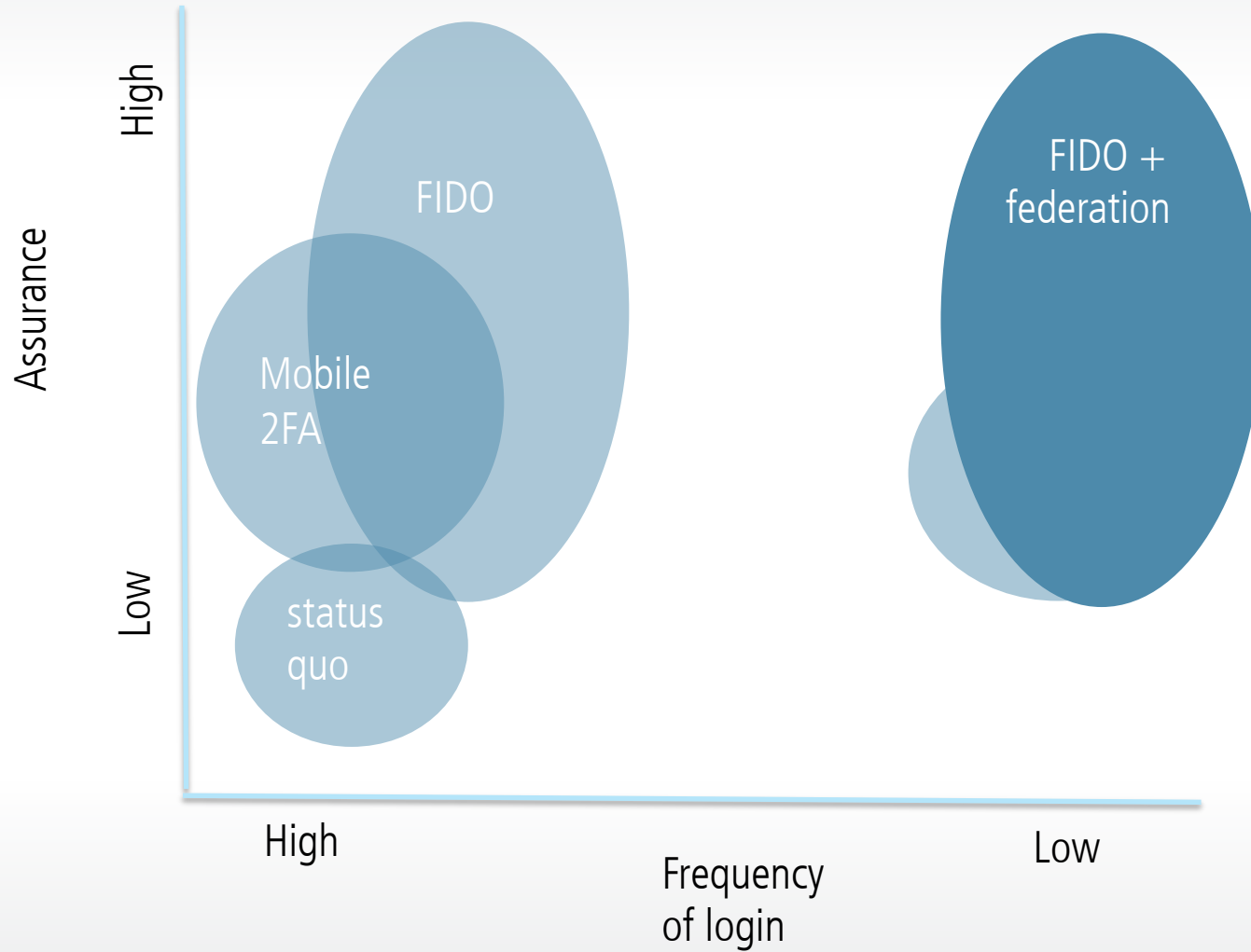












Making it real

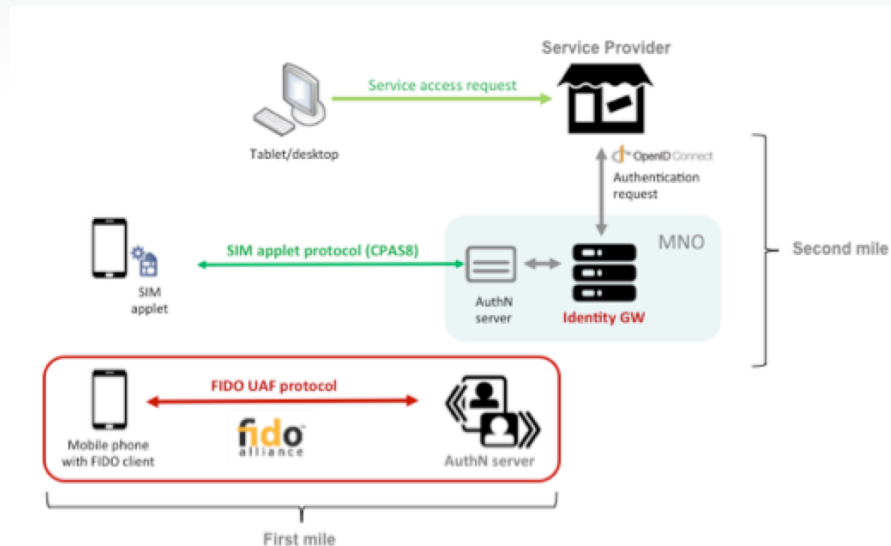
- FIDO drafting federations guideline doc define how to compose FIDO & Federation.
- How to express in a federation token that the authentication was FIDO-based?
 - SAML AuthenticationContext
 - OpenID Connect 'acr'
- How does a federation relying party request a FIDO-based authentication?

Mobile Connect

- Mobile Connect is GSMA effort designed to leverage phones for authentication & identity into applications
- Technically, manifests as a profile of OpenID Connect
 - operators act as ASs
 - Web sites act as Clients
- Like FIDO, leverages phone for user authentication
- Unlike FIDO, also defines subsequent federation piece
- Consequently complementary

Mobile Connect & FIDO

- GSMA & FIDO working on integration
 1. FIDO as an alternative to SIM-based login within Mobile Connect
 2. Using SIM card to enhance FIDO authentication





★ Minor updates to your Google sign-in experience



Categories: [Discuss with others](#) [Account Access and Safety](#) [Desktop - Other \(please specify\)](#) [Google Chrome](#)



Jordan E.  

11 May

Images are hidden - [Show images](#)

Hi everyone,

Today, you sign in to Google on a page that includes both the 'email' and 'password' fields on the same page. We'll be gradually splitting those two fields into separate pages in the coming days; the sign-in process won't change otherwise.

As we've said many times, we're working towards introducing new authentication solutions that complement traditional passwords. We've already separated the 'username' and 'password' fields onto separate pages on a successful launch in Android last year. This change to our web sign-in page is another step in that direction.

To help make sign-in easier and more personal, you may see a screen with your profile picture and full name when signing in to Google. We'll only show this information if you are signing in from a location or device you've signed in from before, like your home computer.

This new Google account sign-in flow will provide the following advantages:

- Preparation for future authentication solutions that complement passwords
- Reduced confusion among people who have multiple Google accounts
- A better experience for SAML SSO users, such as university students or corporate users that sign in with a different identity provider than Google

If you have any feedback about the new sign-in flow, please feel free to reply directly on this thread!

Thanks,

.Jordan

★ Minor updates to your Google sign-in experience



Categories: [Discuss with others](#) [Account Access and Safety](#) [Desktop - Other \(please specify\)](#) [Google Chrome](#)



Jordan E.  

11 May

Images are hidden - [Show images](#)

Hi everyone,

Today, you sign in to Google on a page that includes both the 'email' and 'password' fields on the same page. We'll be gradually splitting those two fields into separate pages in the coming days; the sign-in process won't change otherwise.

As we've said many times, we're working towards introducing new authentication solutions that complement traditional passwords. We've already separated the 'username' and 'password' fields onto separate pages on a successful launch in Android last year. This change to our web sign-in page is another step in that direction.

To help make sign-in easier and more personal, you may see a screen with your profile picture and full name when signing in to Google. We'll only show this information if you are signing in from a location or device you've signed in from before, like your home computer.

This new Google account sign-in flow will provide the following advantages:

- Preparation for future authentication solutions that complement passwords
- Reduced confusion among people who have multiple Google accounts
- A better experience for SAML SSO users, such as university students or corporate users that sign in with a different identity provider than Google

If you have any feedback about the new sign-in flow, please feel free to reply directly on this thread!

Thanks,

.Jordan

Sign in Google

Email

Password


[Sign in](#)

[Can't access your account?](#)



One account. All of Google.

Sign in with your Google Account



[Need help?](#)



[Create account](#)

One Google Account for everything Google



One account. All of Google.

Sign in with your Google Account



Sally Sample
seuresally@gmail.com

 Stay signed in [Need help?](#)

[Sign in with a different account](#)

One Google Account for everything Google



☆ Minor updates to your Google sign-in experience

Categories: [Discuss with others](#) [Account Access and Safety](#) [Desktop - Other \(please specify\)](#) [Google Chrome](#)



Jordan E.  

11 May

Images are hidden - [Show images](#)

Hi everyone,

Today, you sign in to Google on a page that includes both the 'email' and 'password' fields on the same page. We'll be gradually splitting those two fields into separate pages in the coming days; the sign-in process won't change otherwise.

As we've said many times, we're working towards introducing new authentication solutions that complement traditional passwords. We've already separated the 'username' and 'password' fields onto separate pages on a successful launch in Android last year. This change to our web sign-in page is another step in that direction.

To help make sign-in easier and more personal, you may see a screen with your profile picture and full name when signing in to Google. We'll only show this information if you are signing in from a location or device you've signed in from before, like your home computer.

This new Google account sign-in flow will provide the following advantages:

- Preparation for future authentication solutions that complement passwords
- ~~Reduced confusion among people who have multiple Google accounts~~
- A better experience for SAML SSO users, such as university students or corporate users that sign in with a different identity provider than Google

If you have any feedback about the new sign-in flow, please feel free to reply directly on this thread!

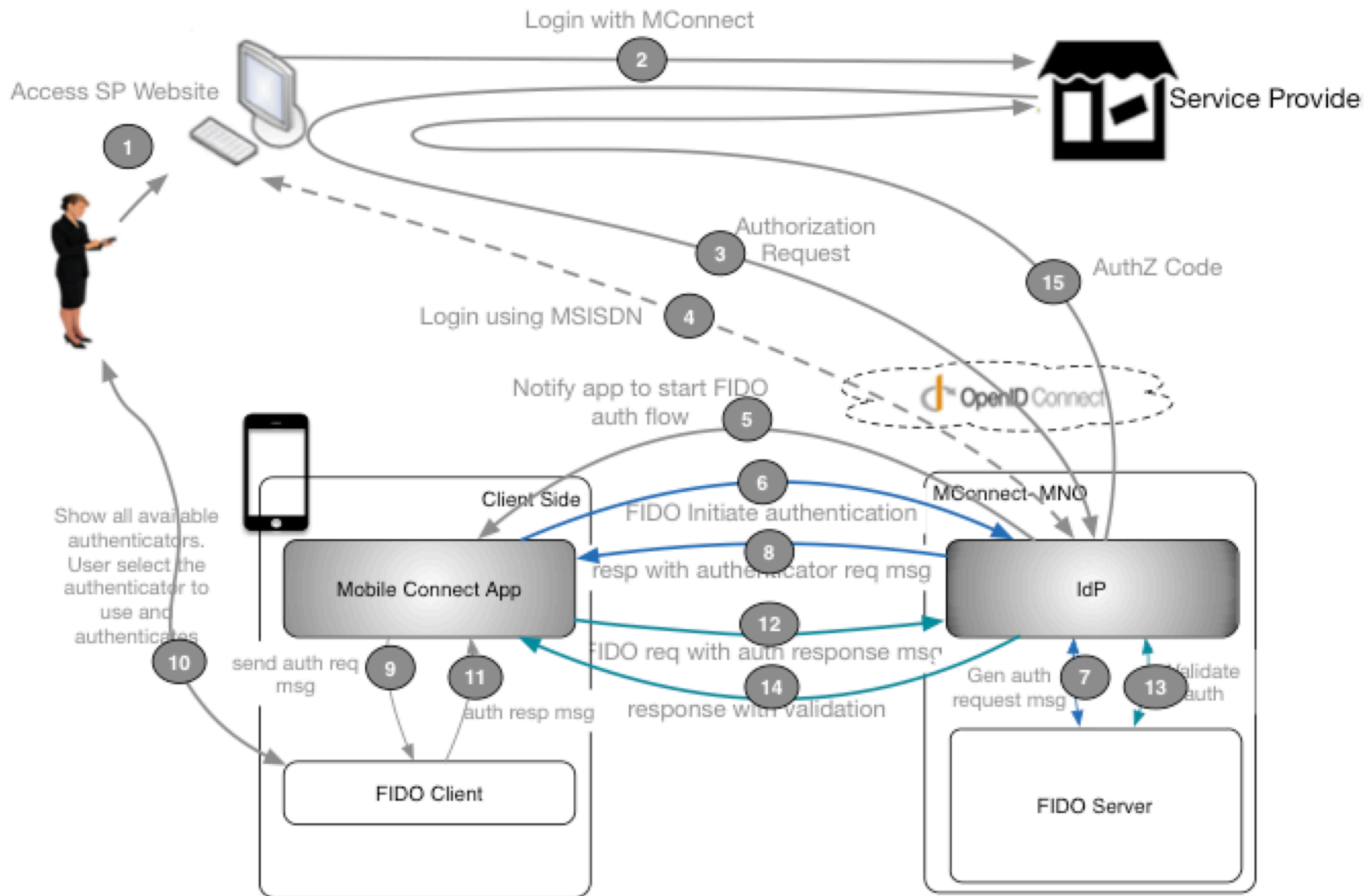
Thanks,

.Jordan

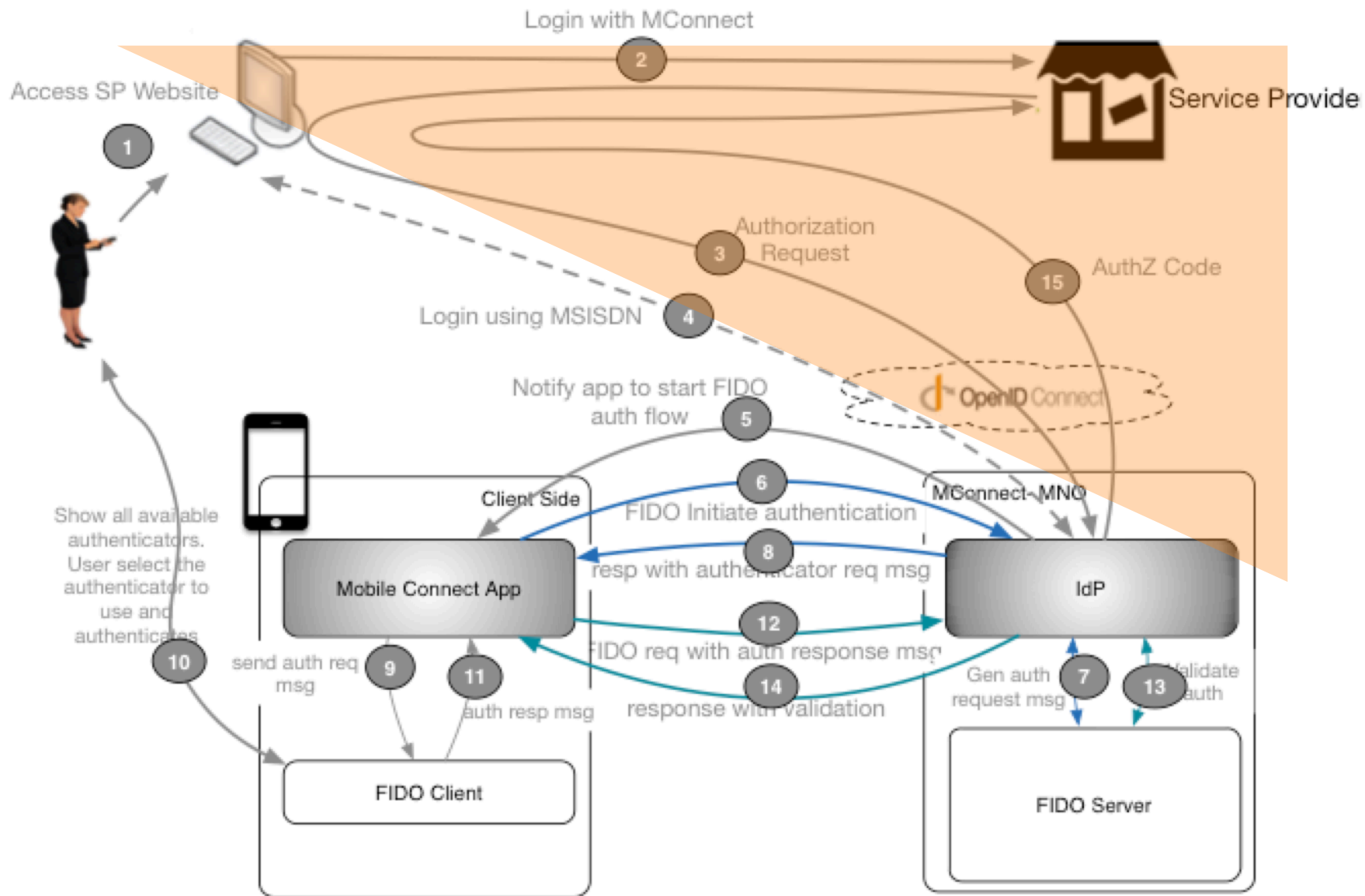
Advantages

- Breaking apart the login UX allows Google to personalize authentication
- Can use
 - password for some
 - FIDO for some (supporting FIDO as single factor)
 - federated SSO for some (like employees of Google Apps enterprise customers)
 - Future TBD authentication schemes

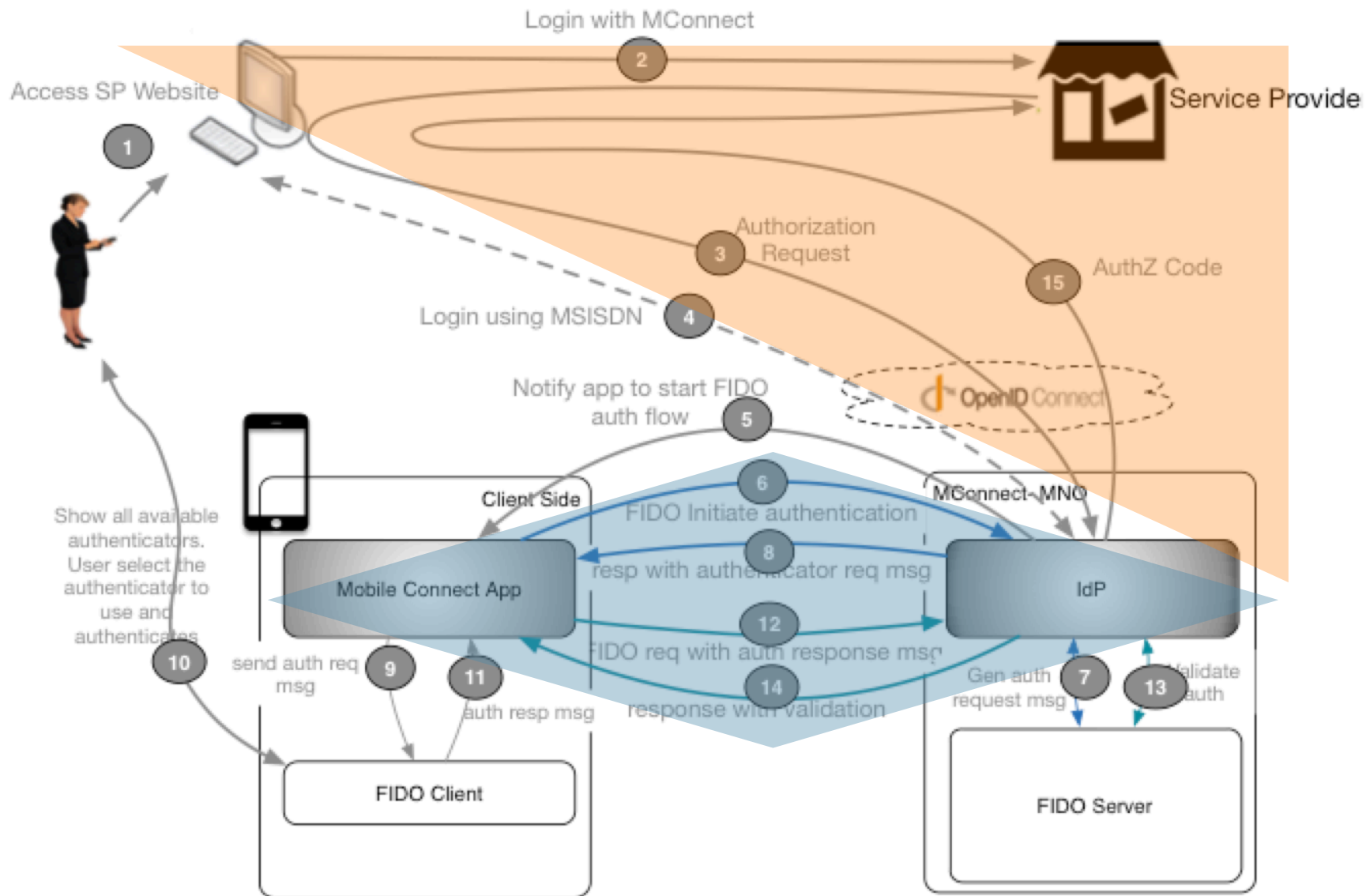
Integration



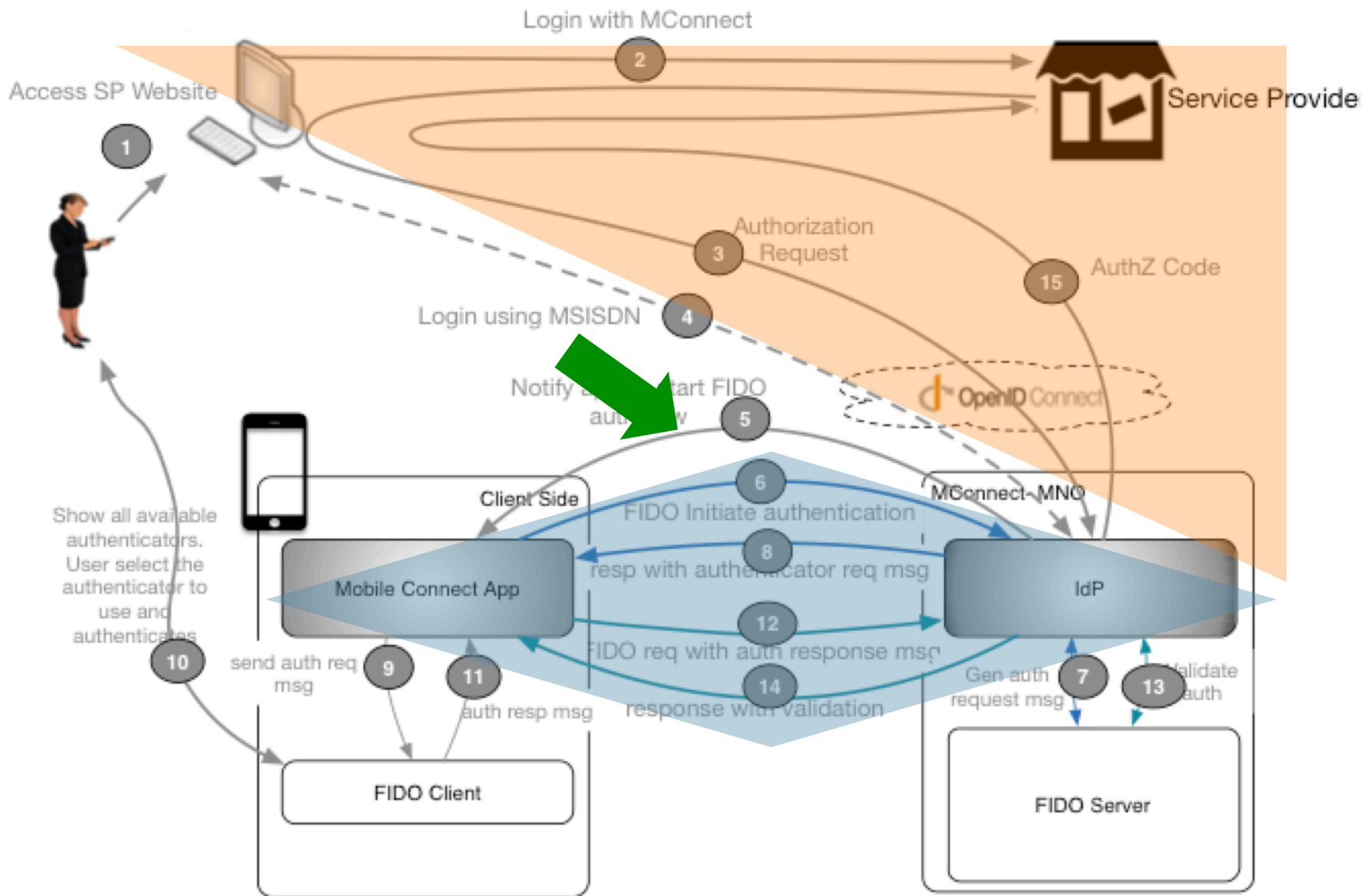
Integration



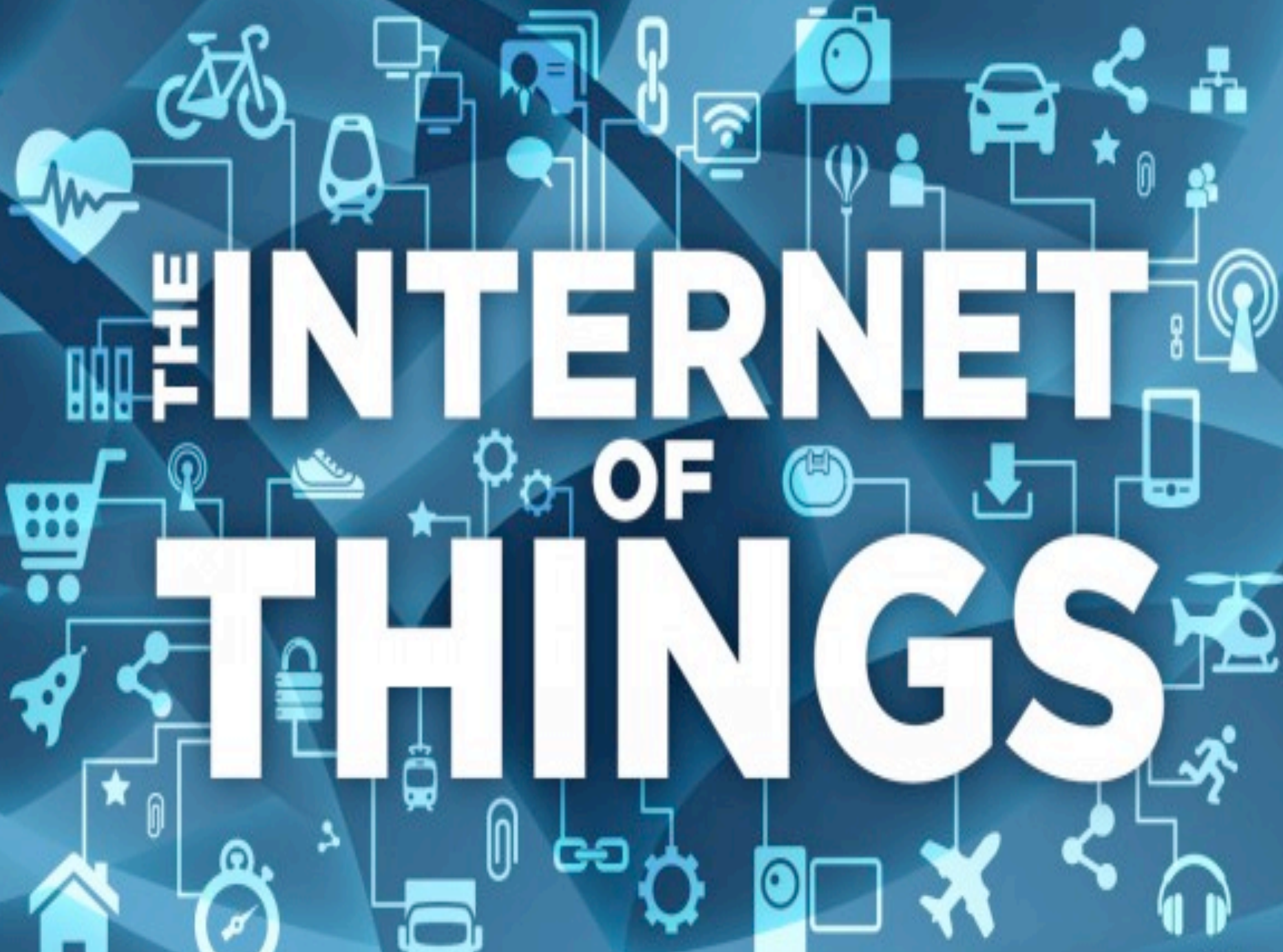
Integration



Integration

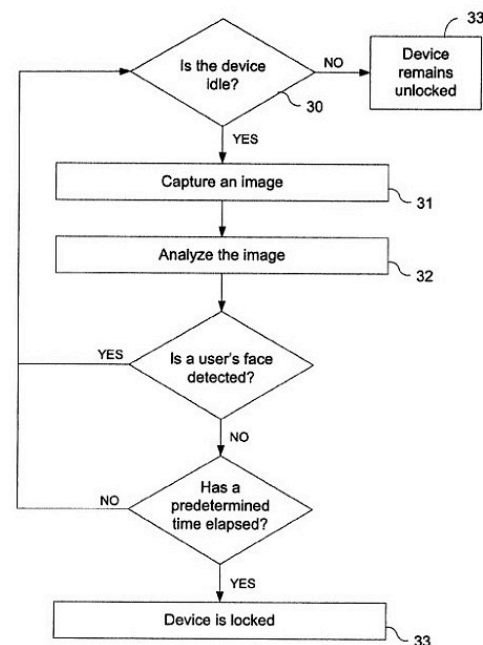


THE INTERNET OF THINGS

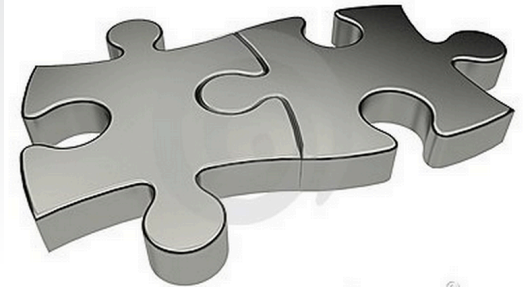


FIDO & IoT?

- FIDO model presumes devices with sensor capabilities (for the local authn)
- Phones are but first wave of such devices
- We'll soon be surrounded by devices that will be able to act as FIDO Client & Authenticator
- The local authentication can be either explicit (like an EKG reading) or implicit (like gait or facial recognition)



Summary



- FIDO server provides
 - Secure hardware-based authentication
 - Support for range of user authentication modalities, appropriate to capabilities of device
 - Abstraction layer between device login & server
- Federation server provides
 - Portable identity
 - Support for range of federation protocols, appropriate to capabilities of application
 - Abstraction layer between identity provider & application

Thank you