MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

BRIDGING THE PROTOCOL GAP ON CLOUD IDENTITY PROJECTS

Jeff Bohren

Chief Software Engineer, Optimal IdM

Jeff.Bohren@optimalidm.com

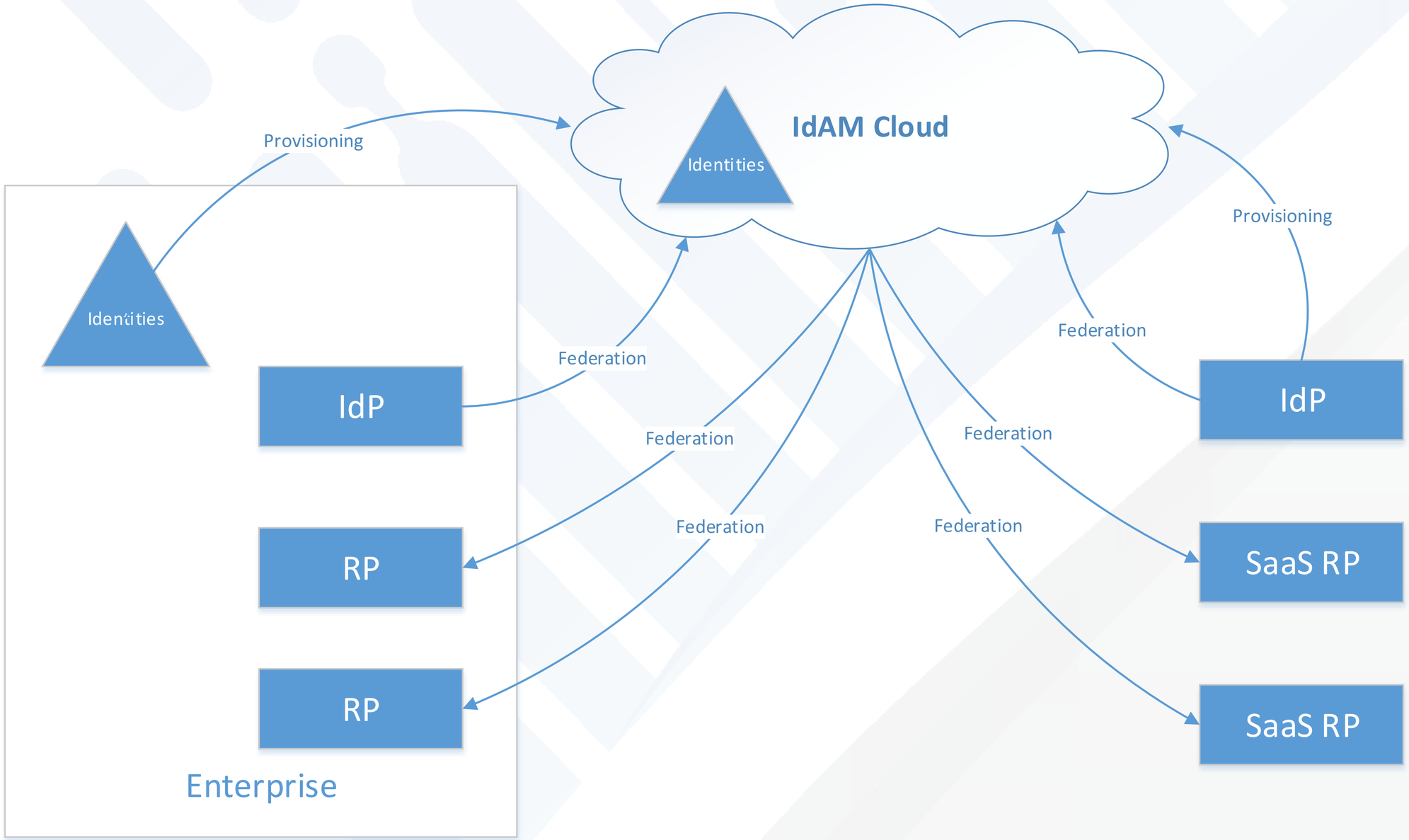
AGENDA

- Introduction
- Cloud IdAM Architectures
  - Traditional
  - Broker
- Federation Protocols
  - Authentication vs Authorization
  - Passive vs Active
  - Tokens
- Protocol transition
  - WS-Fed and SAML 2
  - WS-Fed, SAML 2, OAuth2, and OpenID Connect (OIC)
- Web Services
- Social Media Authentication

WHAT IS THE PROTOCOL GAP?

- Chain of identity
  - Multiple levels
- Protocol Transition
  - Identity Provider (IdP) to IdP
  - Identity Provider (IdP) to Relying Party (RP)
- Why do we need to bridge the GAP
  - SSO to heterogenous relying parties (both on premise and SaaS)
  - Provisioning

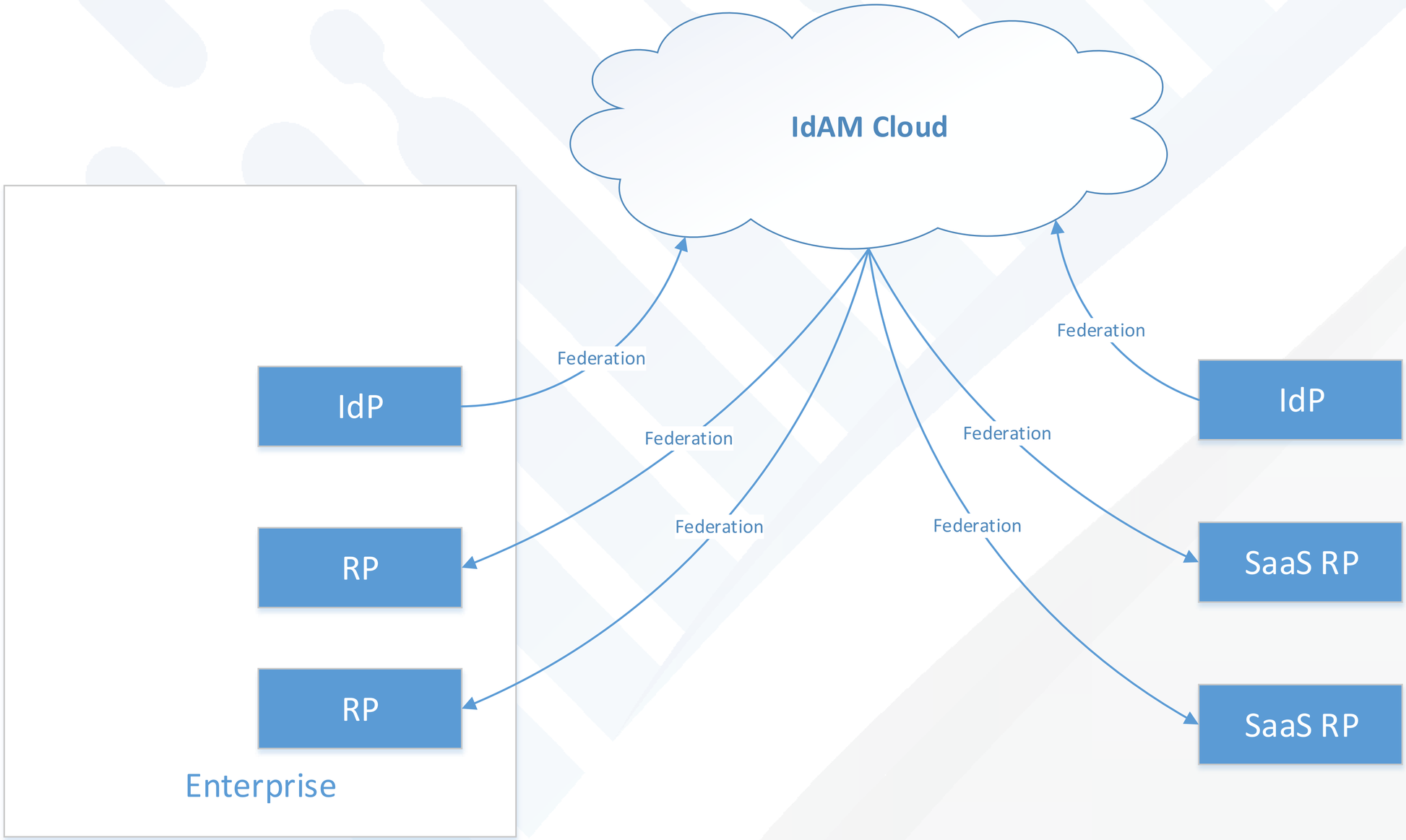
IDAM CLOUD ARCHITECTURES - TRADITIONAL



IDAM CLOUD ARCHITECTURES - TRADITIONAL

- Identities in the Cloud
  - Can support mixture of internal and external identities
  - Supports federation to on premise and SaaS applications
  - Supports pre-provisioning or JIT provisioning
  - Centralized auditing of identities

IDAM CLOUD ARCHITECTURES - BROKER



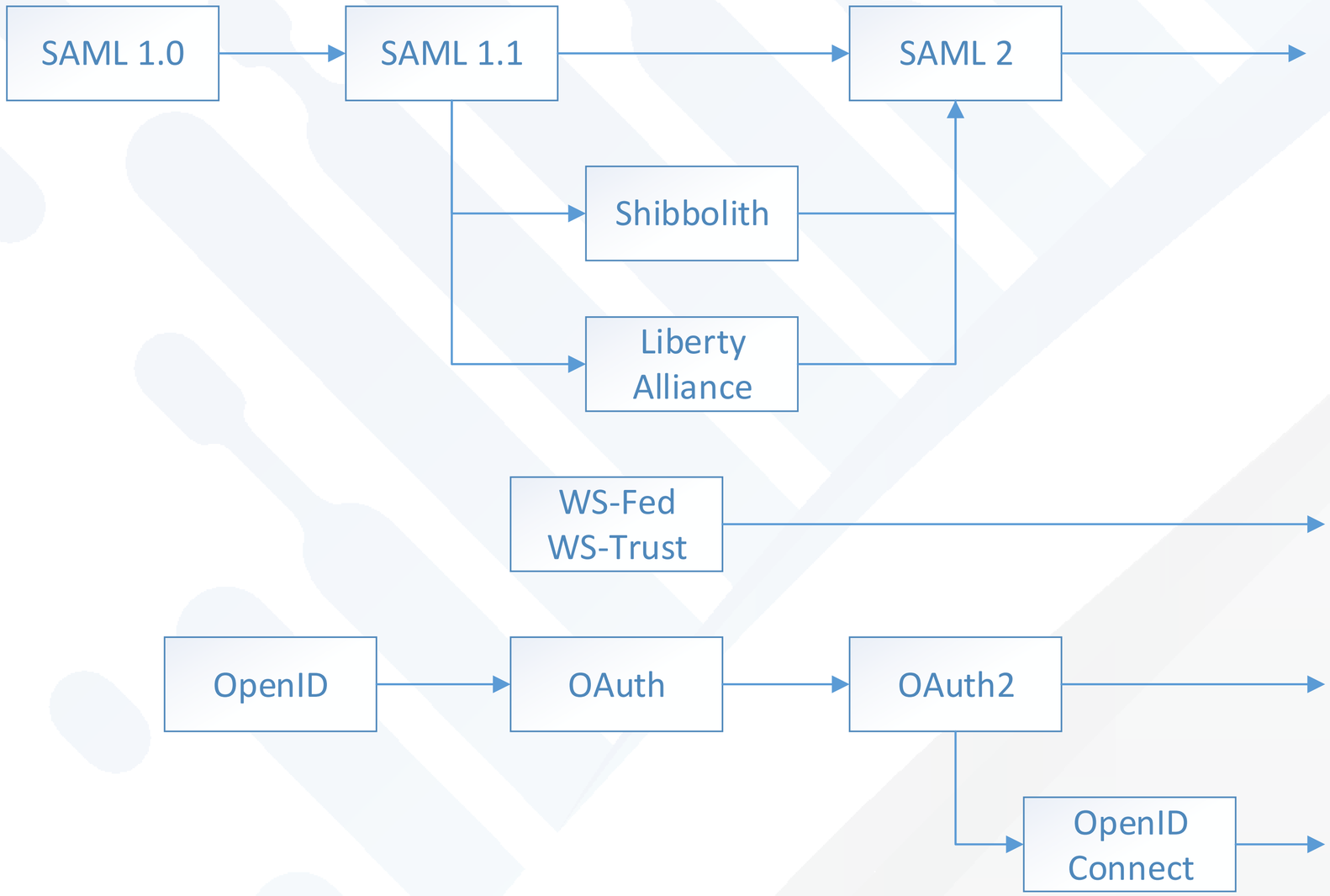
IDAM CLOUD ARCHITECTURES - BROKER

- No identities in the Cloud
  - Can support mixture of internal and external identities
  - Supports federation to on premise and SaaS applications
  - Supports JIT provisioning only
  - No centralized auditing of identities
  - Data protection and privacy advantages

FEDERATION PROTOCOLS

- Older XML and SOAP based protocols
  - SAML2
  - WS-Federation
  - WS-Trust
- Newer JSON and REST based protocols
  - OAuth2
    - Often referred to as an Authorization Protocol
  - OpenID Connect (OIC)
    - Built on top of OAuth2

HOW DID WE GET HERE?



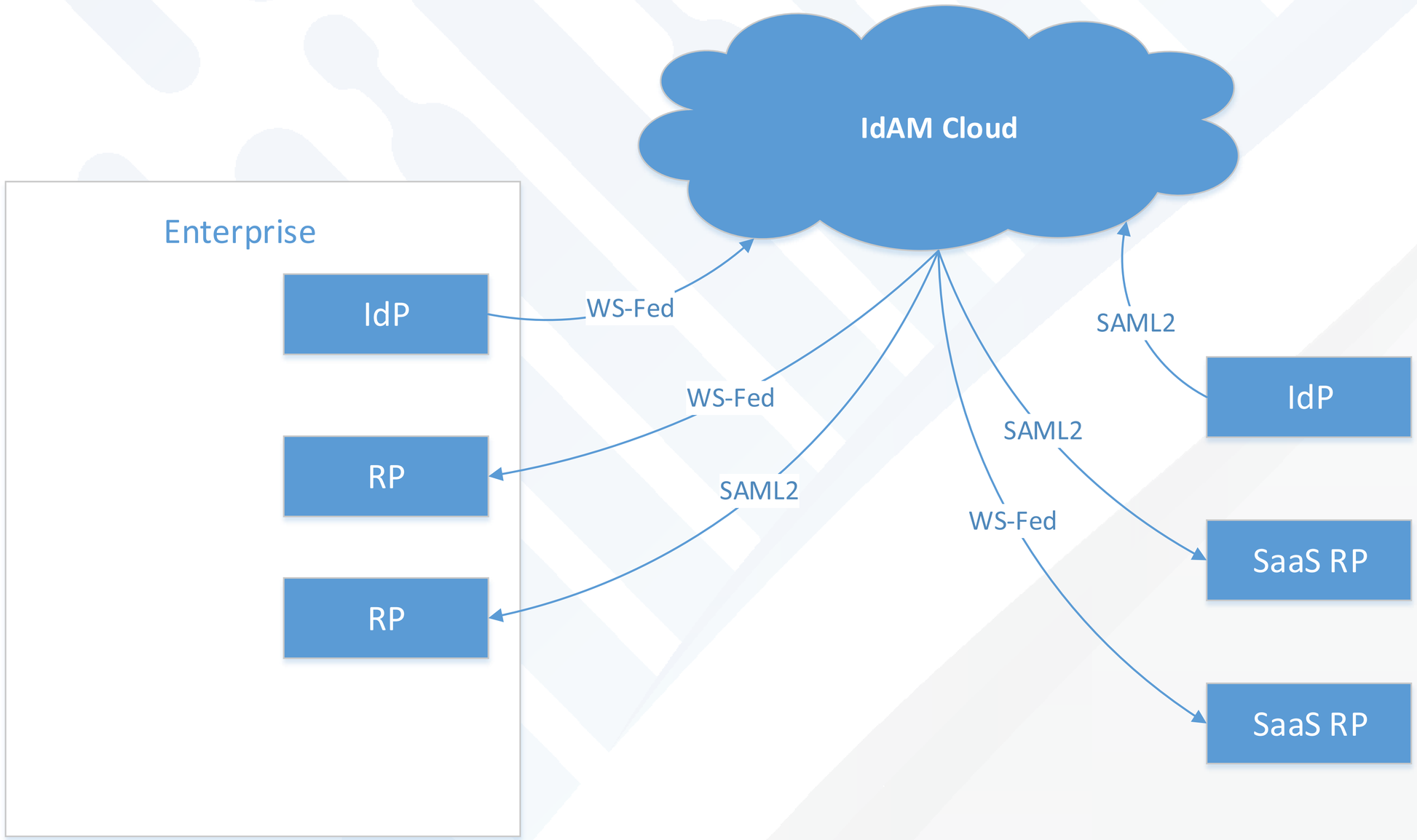
TOKENS

- WS-Federation and WS-Trust are token agnostic
  - Mostly used with SAML 1.1 and SAML 2.0 tokens
- SAML 2.0 uses SAML 2.0 tokens (as expected)
- OAuth 2
  - Access Codes
  - Access Tokens
  - Refresh Tokens
- OpenID Connect
  - JSON Web Tokens (Jwt)

OAUTH2/OIC GRANTS

- Access Code Grant
  - Passive and Active
  - Not well suited for thick clients and SPAs
  - Supports SSO and MFA
  - Supports end user authorization of scope
- Implicit Grant
  - Passive Only
  - Not well suited for thick clients and SPAs
  - Supports SSO and MFA
  - Supports end user authorization of scope
- Resource Owner Password Grant
  - Active only
  - Ideal for thick clients and SPAs
  - Does not support SSO or MFA

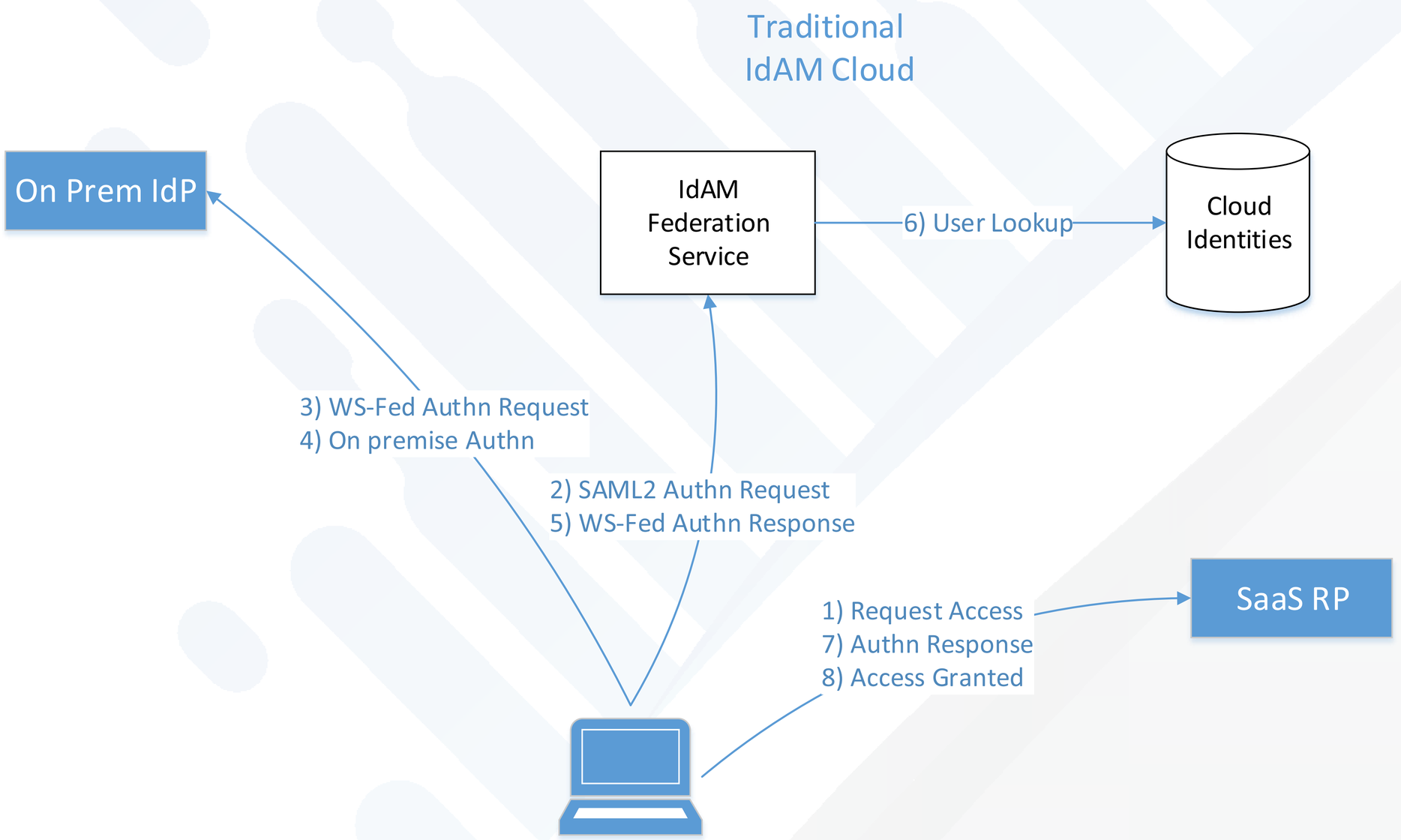
WS-FED/SAML2 PROTOCOL TRANSITION



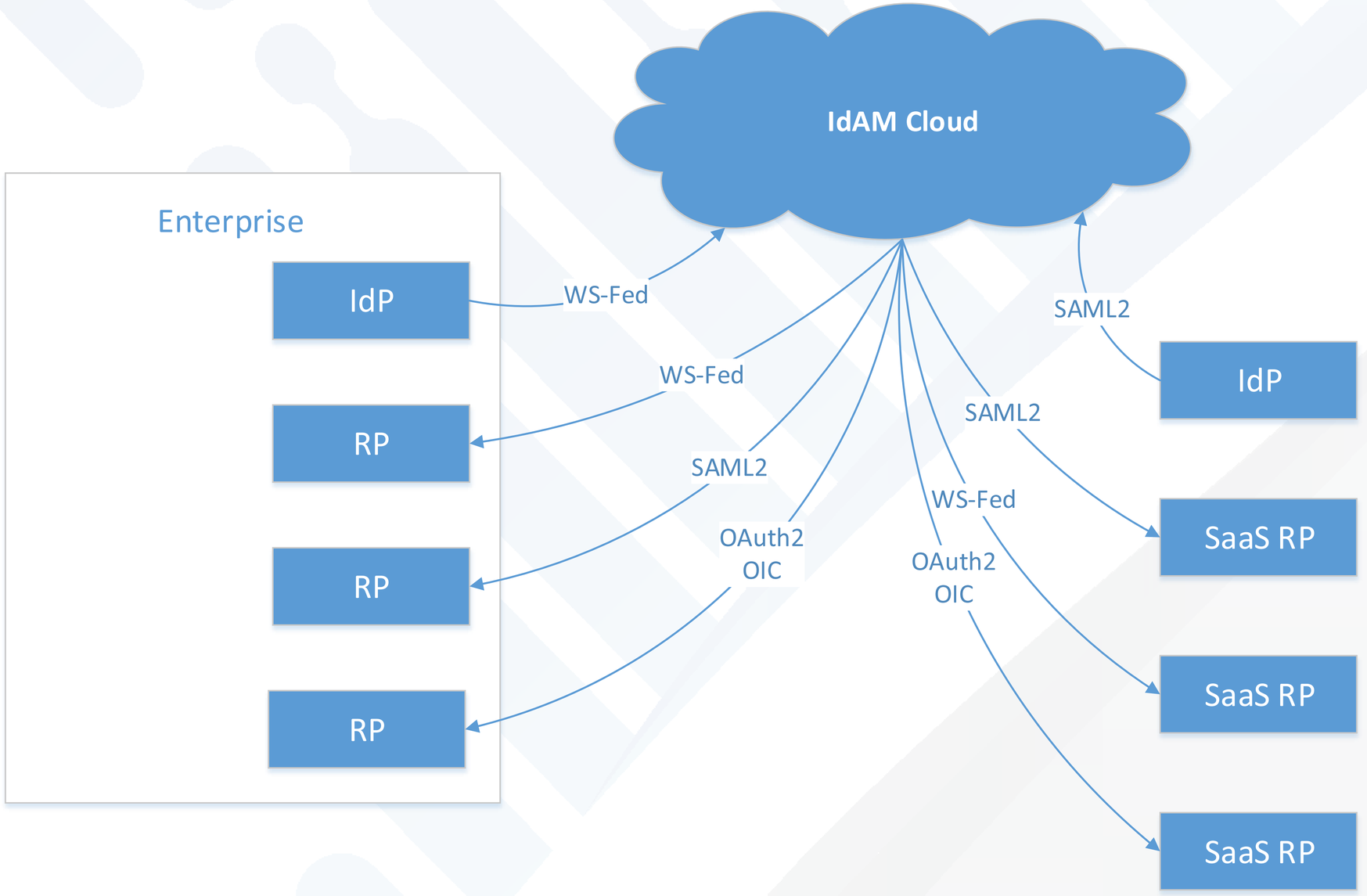
PROTOCOL TRANSITION CONSIDERATIONS

- Identity mapping
- Attribute mapping
- Traditional vs Broker cloud architectures
- Single Sign-on (SSO)
- Single logout (SLO)
- Context or Relay State must be preserved

SSO


Traditional
IdAM Cloud
On Prem IdP
IdAM
Federation
Service
6) User Lookup
Cloud
Identities
3) WS-Fed Authn Request
4) On premise Authn
2) SAML2 Authn Request
5) WS-Fed Authn Response
1) Request Access
7) Authn Response
8) Access Granted
SaaS RP

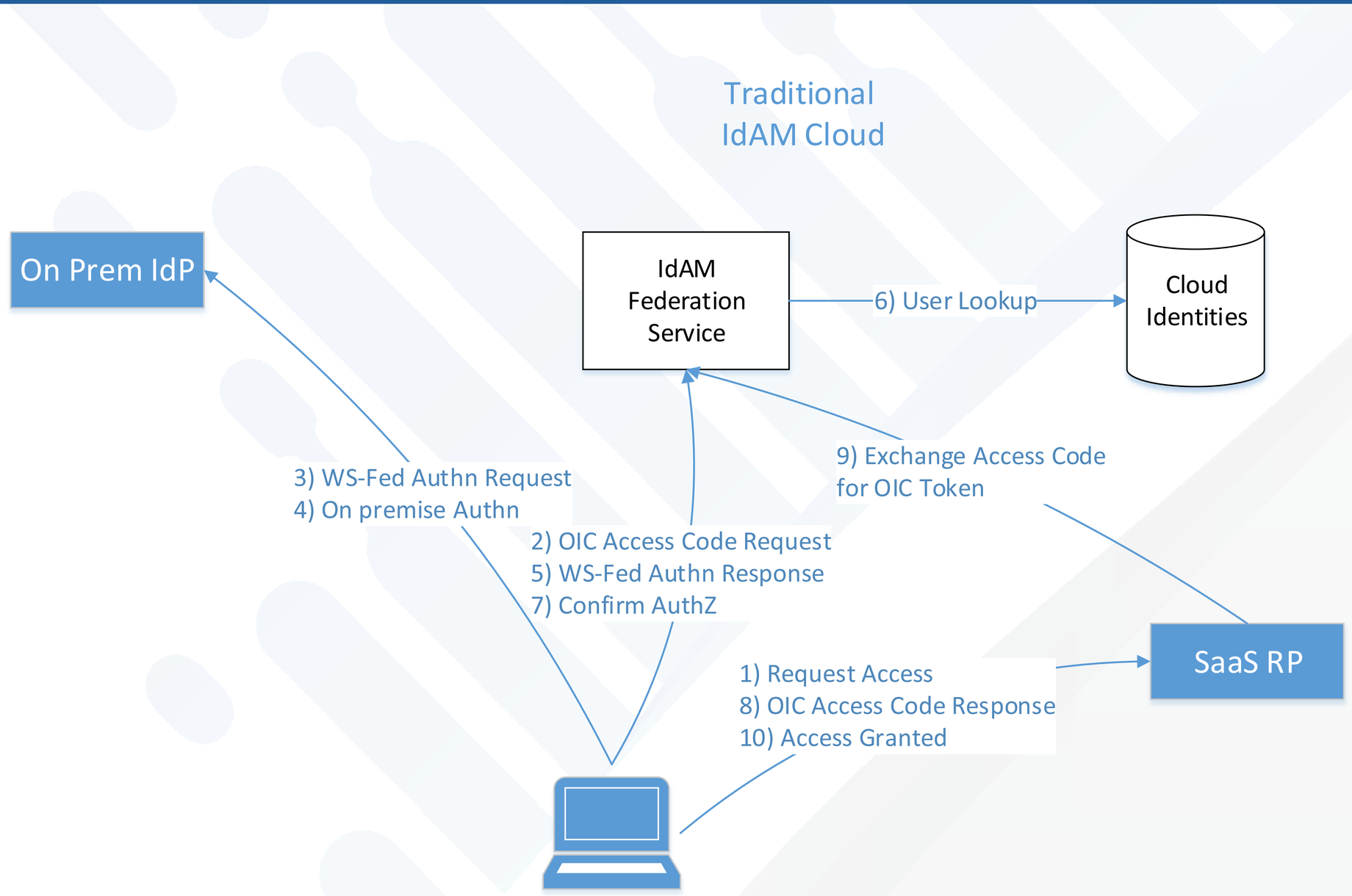
WS-FED/SAML2/OAUTH2/OIC PROTOCOL TRANSITION



WS-FED/SAML2/OAUTH2/OIC PROTOCOL TRANSITION

- Why is this needed?
- What are the unique challenges?
- OAuth2 and OIC do not support SLO
- OAuth2 and OIC support end user authorization, WS-Fed and SAML2 do not

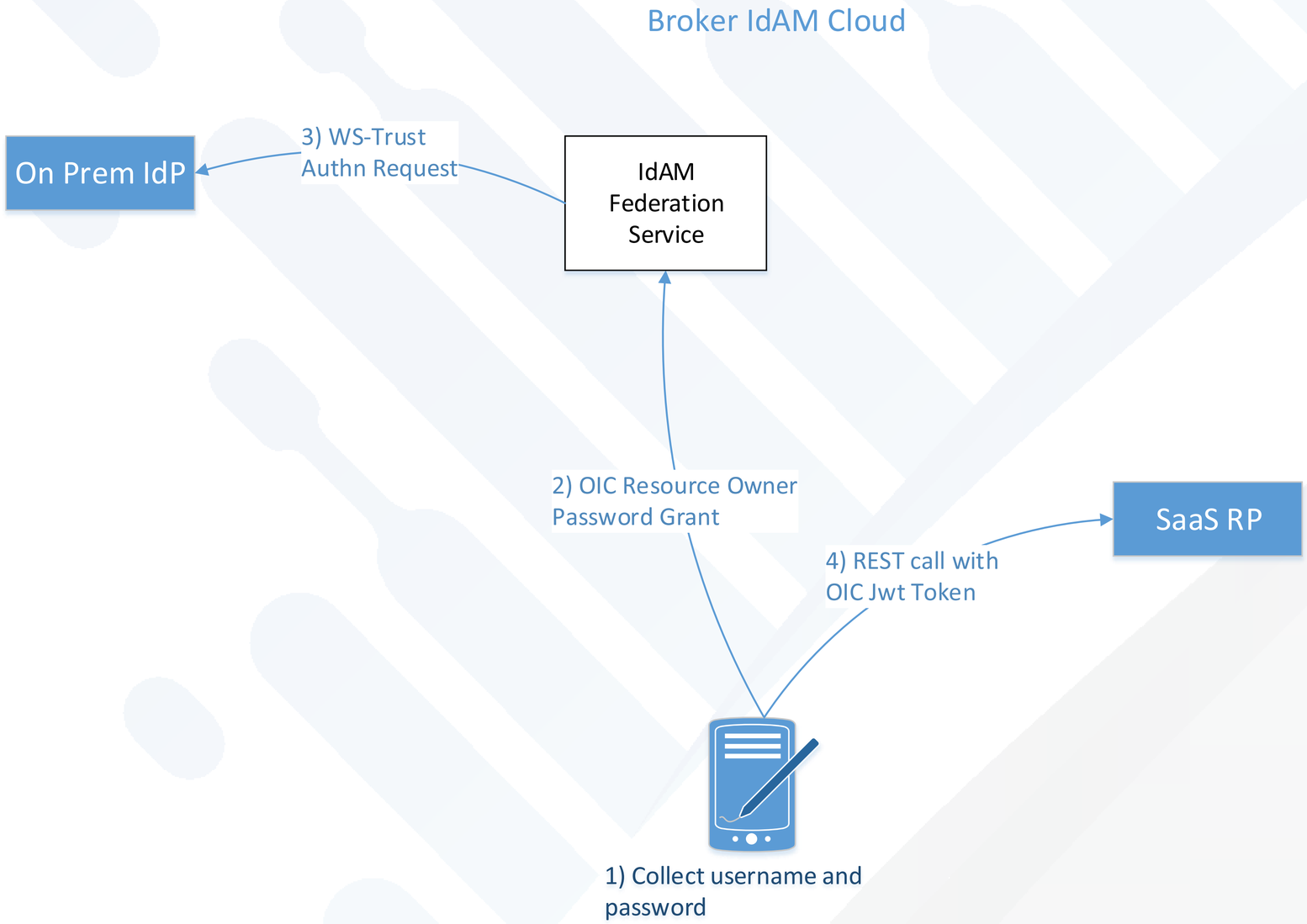
TYPICAL SCENARIO - SSO



ACTIVE AUTHENTICATION

- Mostly used with single page applications (SPAs), devices, and thick clients
- WS-Trust
  - SOAP Protocol
  - Most common is username and password authN
  - Windows integrated authN also supported
- OAuth 2\OIC
  - REST
  - Resource Owner Password Grant (username and password)
- AuthN only, no explicit AuthZ
- MFA not supported

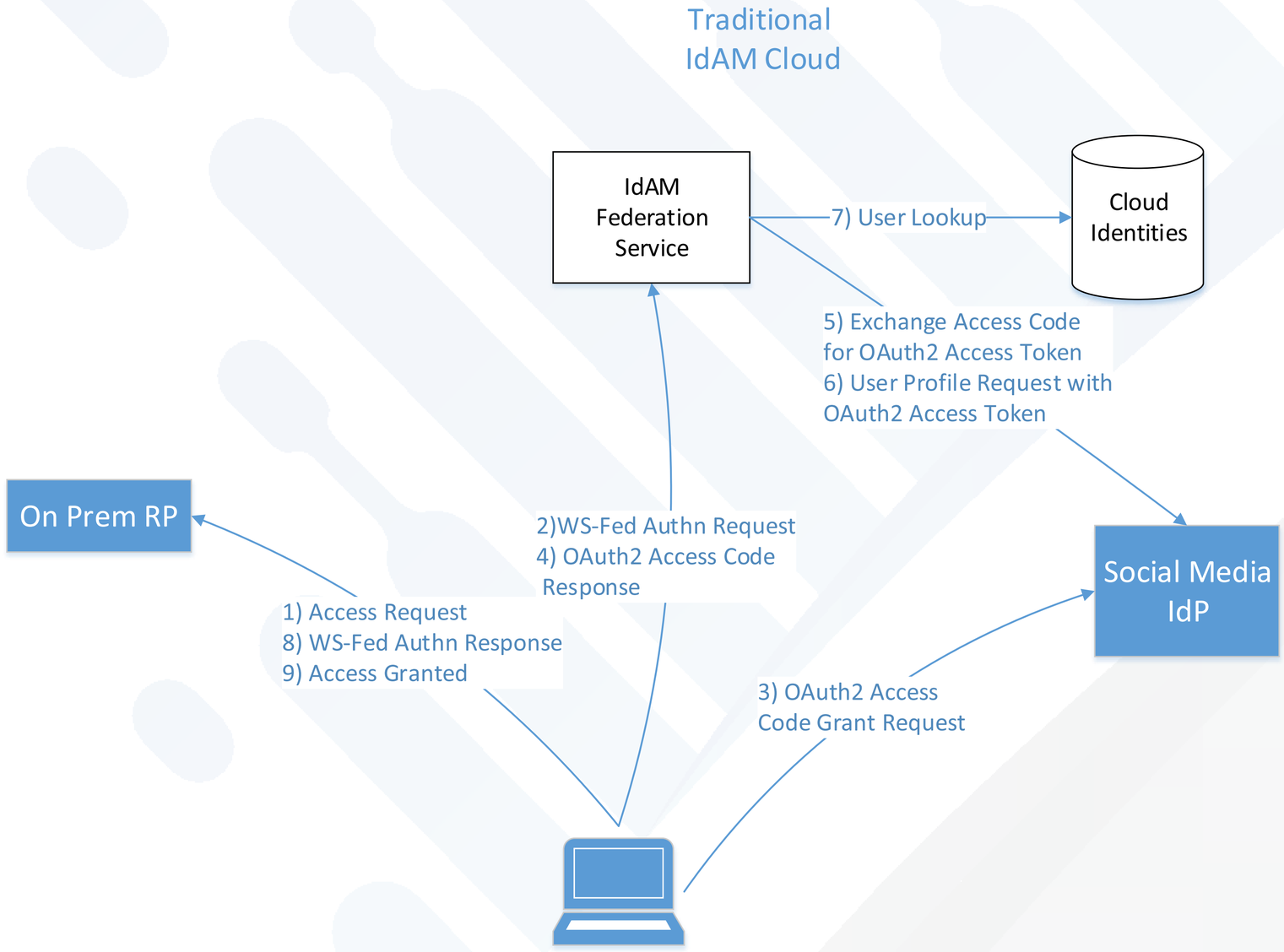
ACTIVE AUTHENTICATION



SOCIAL MEDIA

- Why is this a good idea?
  - Ubiquitous
  - Gets you out of the password reset business
  - Shifts the data privacy concerns to a third party
- Why is a bad idea?
  - Lack of institutional control
- Challenges
  - May require registration or identity proofing step
  - Most social media IdPs support OAuth2 but not OpenID Connect
  - SLO is non-standard

SOCIAL MEDIA



MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Jeff Bohren

Chief Software Engineer, Optimal IdM

Jeff.Bohren@optimalidm.com