SECURING

MICRO-SERVICES

RED | VENTURES

Majid Fatemian

@majidfn

TECHNOLOGY-DRIVEN

CUSTOMER ACQUISITION

SALES & MARKETING

AT&T

verizon

AMERICAN EXPRESS

Frontier

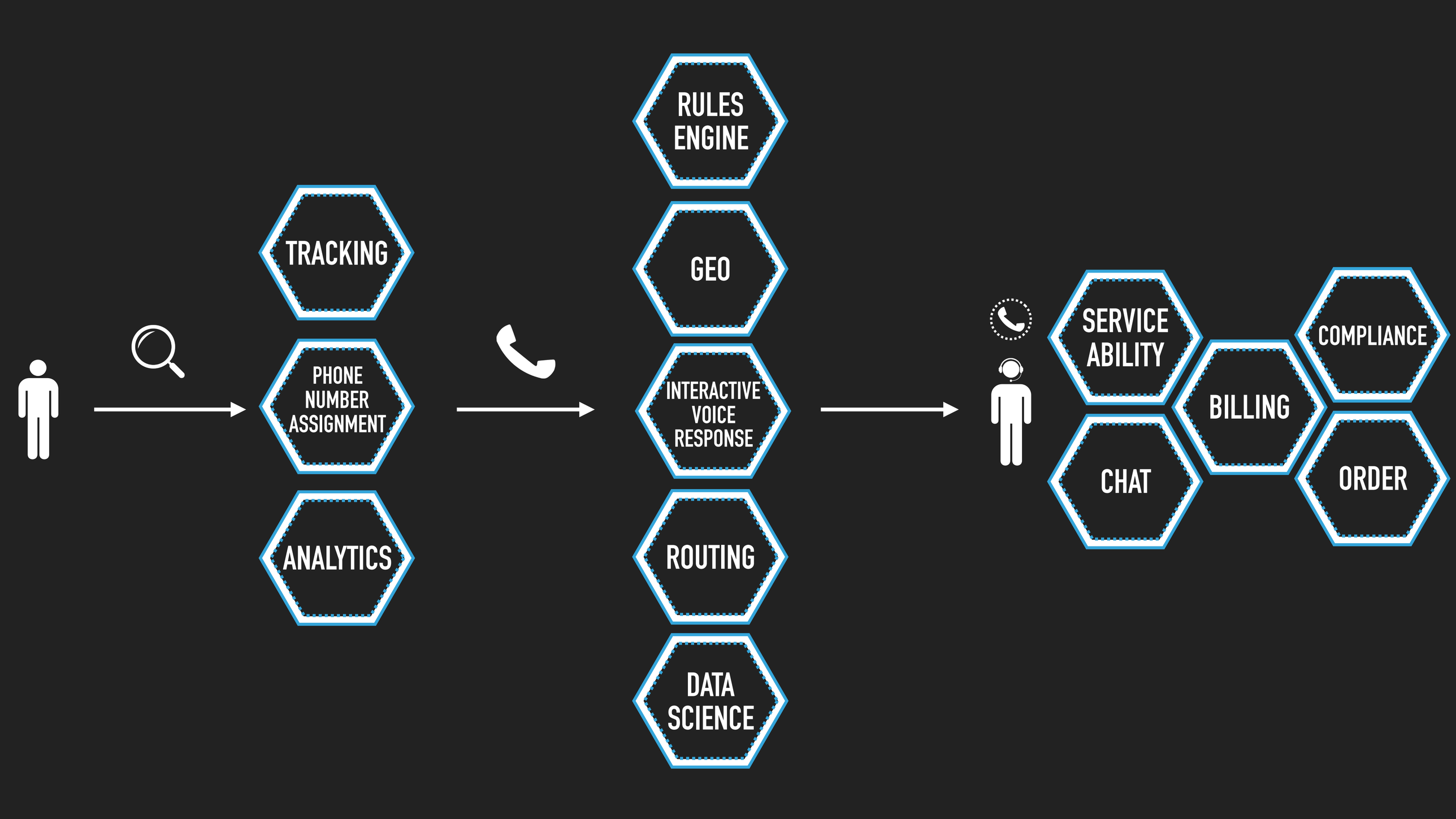
CenturyLink

HughesNet

FINE-GRAINED

TECHNOLOGY / PROTOCOL AGNOSTIC

ELASTIC, RESILIENT


TRACKING
PHONE NUMBER ASSIGNMENT
ANALYTICS
RULES ENGINE
GEO
INTERACTIVE VOICE RESPONSE
ROUTING
DATA SCIENCE
SERVICE ABILITY
BILLING
COMPLIANCE
CHAT
ORDER

AT&T

RED | VENTURES

AUTHENTICATION

VS.

AUTHORIZATION

AUTHENTICATION

VERIFYING THE IDENTITY OF A USER / PROCESS

AUTHORIZATION

PERMITTING ACCESS / ACTION TO RESOURCES

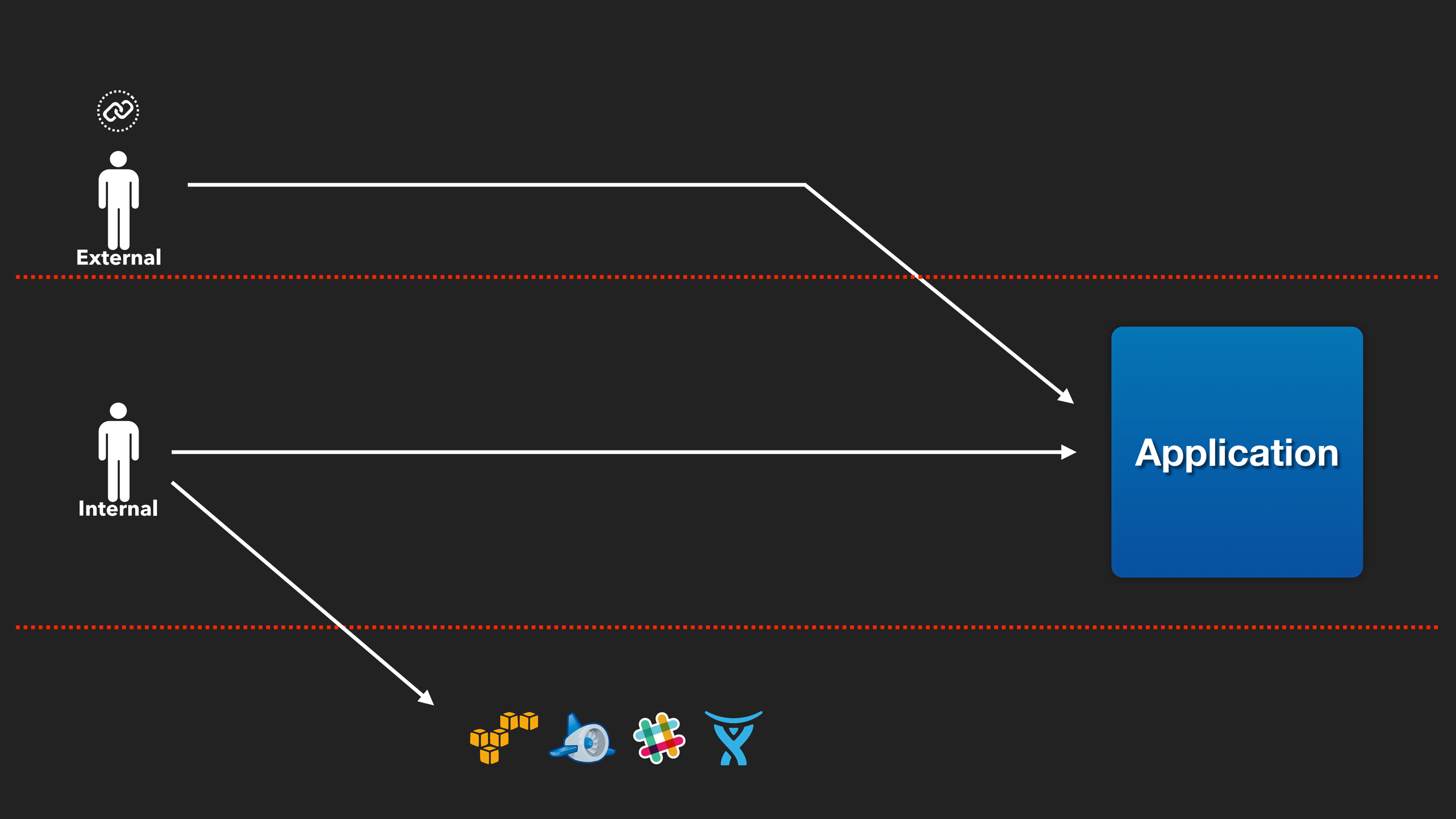
AUTHENTICATION

REUSE vs. BUILD

AUTHENTICATION

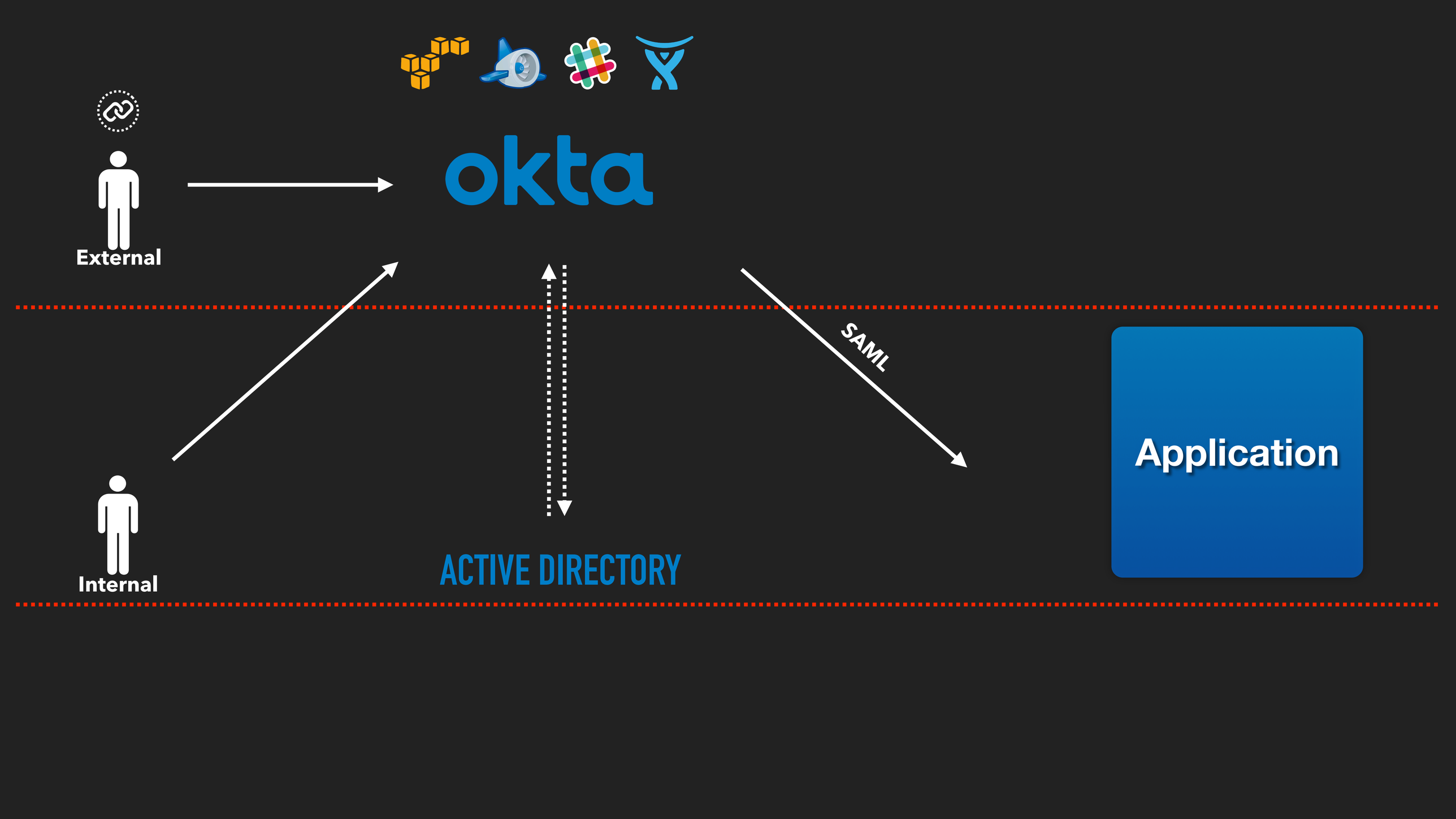
① ACTIVE DIRECTORY


ACTIVE DIRECTORY
Application

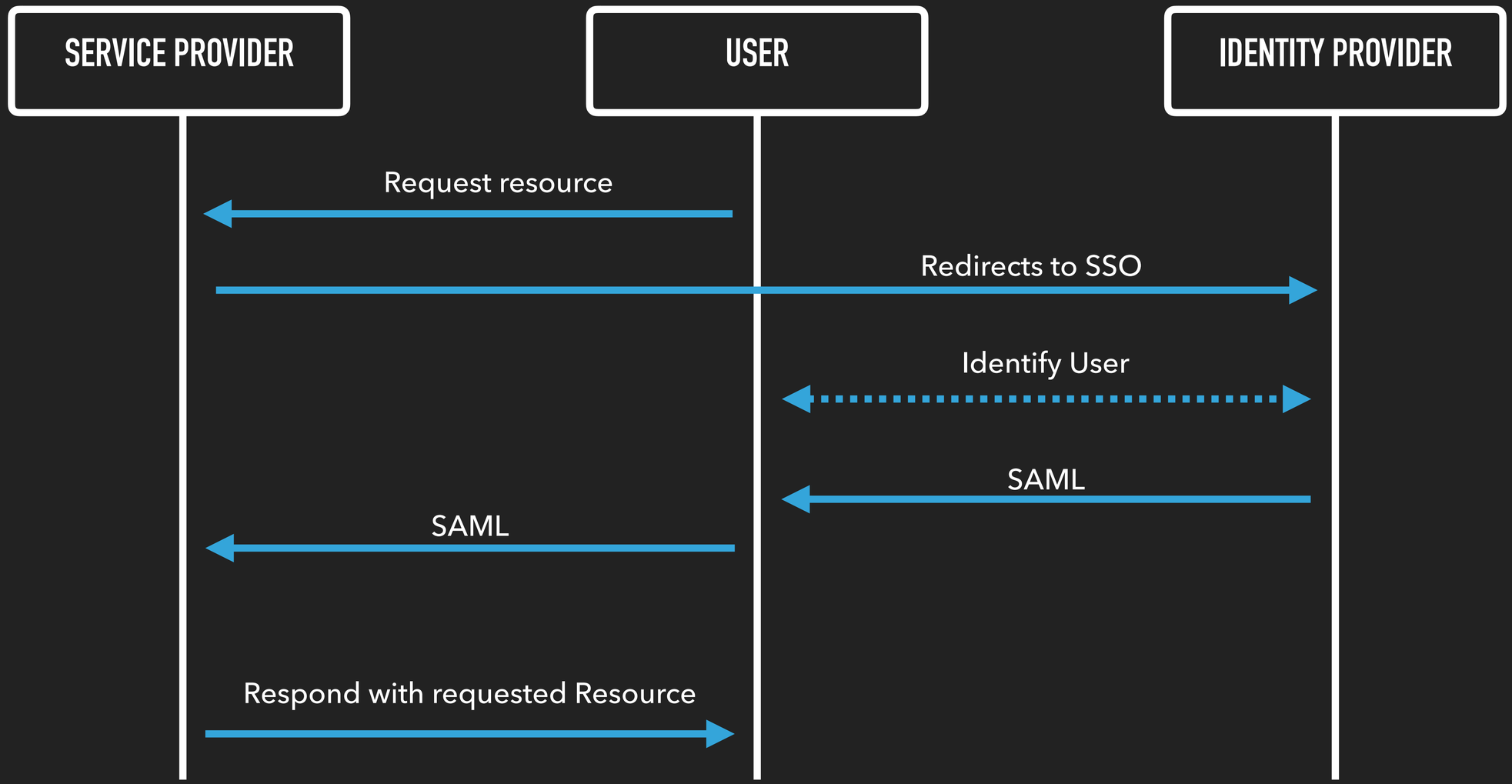

External
Internal
Application

AUTHENTICATION

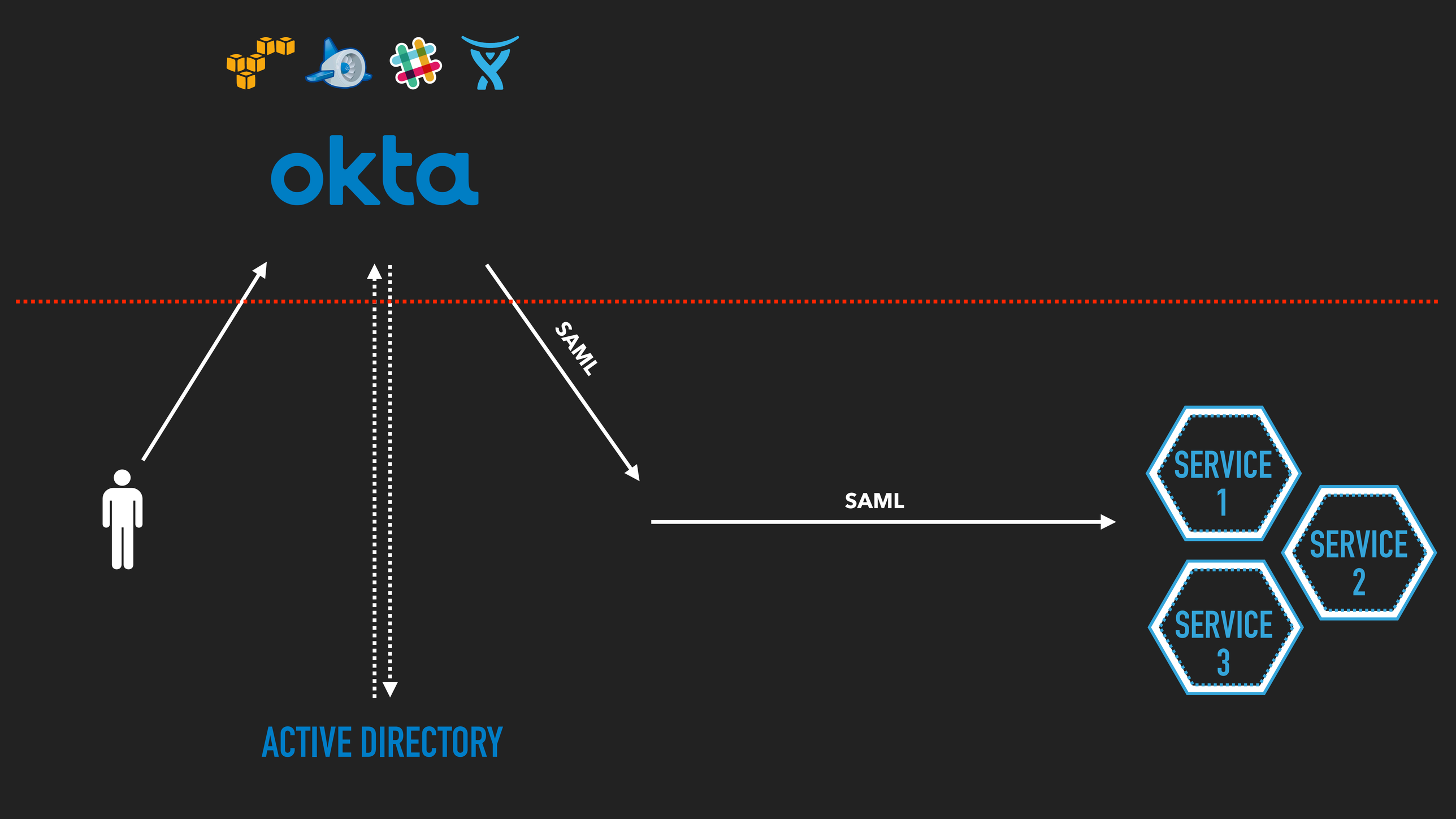
1. ACTIVE DIRECTORY
2. OKTA


okta
External
Internal
SAML
Application
ACTIVE DIRECTORY

SAML – SECURITY ASSERTION MARKUP LANGUAGE

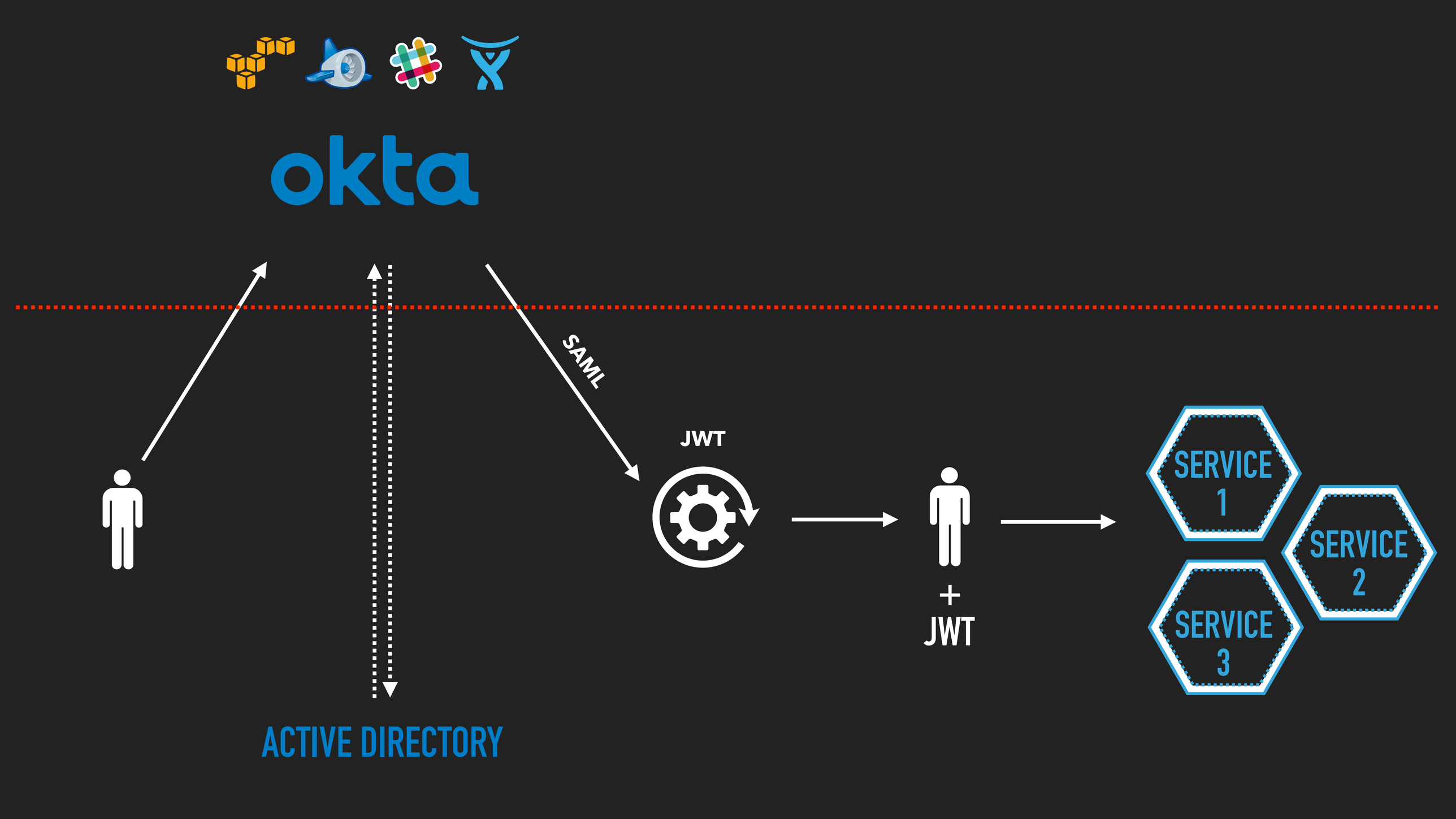


```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="pfx41d8ef22-
e612-8c50-9960-1b16f15741b3" Version="2.0" ProviderName="SP test" IssueInstant="2014-07-16T23:52:45Z" Destination="http://idp.example.com/
SSOService.php" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="http://sp.example.com/demo1/
index.php?acs">
  <saml:Issuer>http://sp.example.com/demo1/metadata.php</saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#pfx41d8ef22-e612-8c50-9960-1b16f15741b3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>yJN6cXUwQxTmMEsPesBP2NkqYFI=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>g5eM9yPnKsmmE/Kh2qS7nfK8HoF…3socPqAi2Qf97E=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
<ds:X509Certificate>MIICajCCAdOgAwIBAgIBADANBgkqhkiG9w0BAQQ…….BpspRYT+kAGiFomHop1nErV6Q==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" AllowCreate="true"/>
  <samlp:RequestedAuthnContext Comparison="exact">
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```


okta
SAML
SAML
SERVICE 1
SERVICE 2
SERVICE 3
ACTIVE DIRECTORY

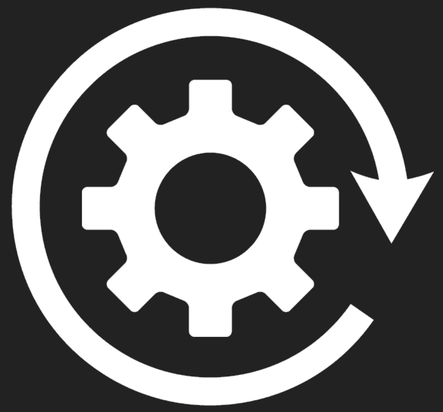
AUTHENTICATION

1. ACTIVE DIRECTORY
2. OKTA
3. JWT (JSON WEB TOKEN)

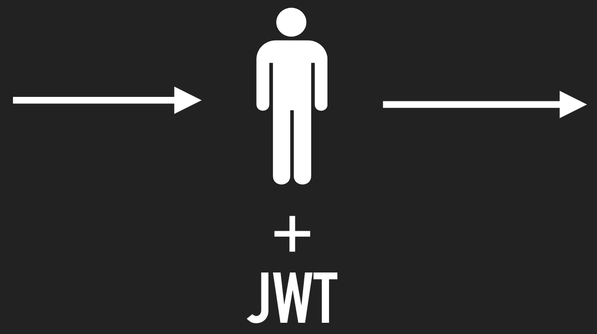

okta
SAML
JWT
+
JWT
SERVICE 1
SERVICE 2
SERVICE 3
ACTIVE DIRECTORY

Private

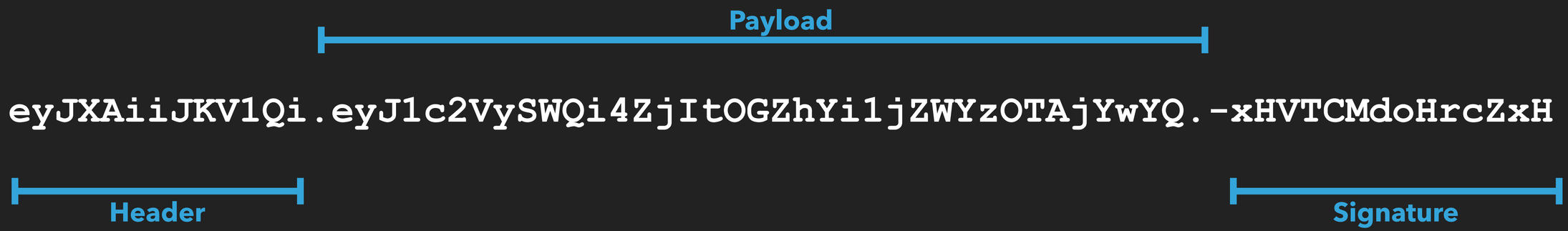
Public



JWT
Identity
Provider



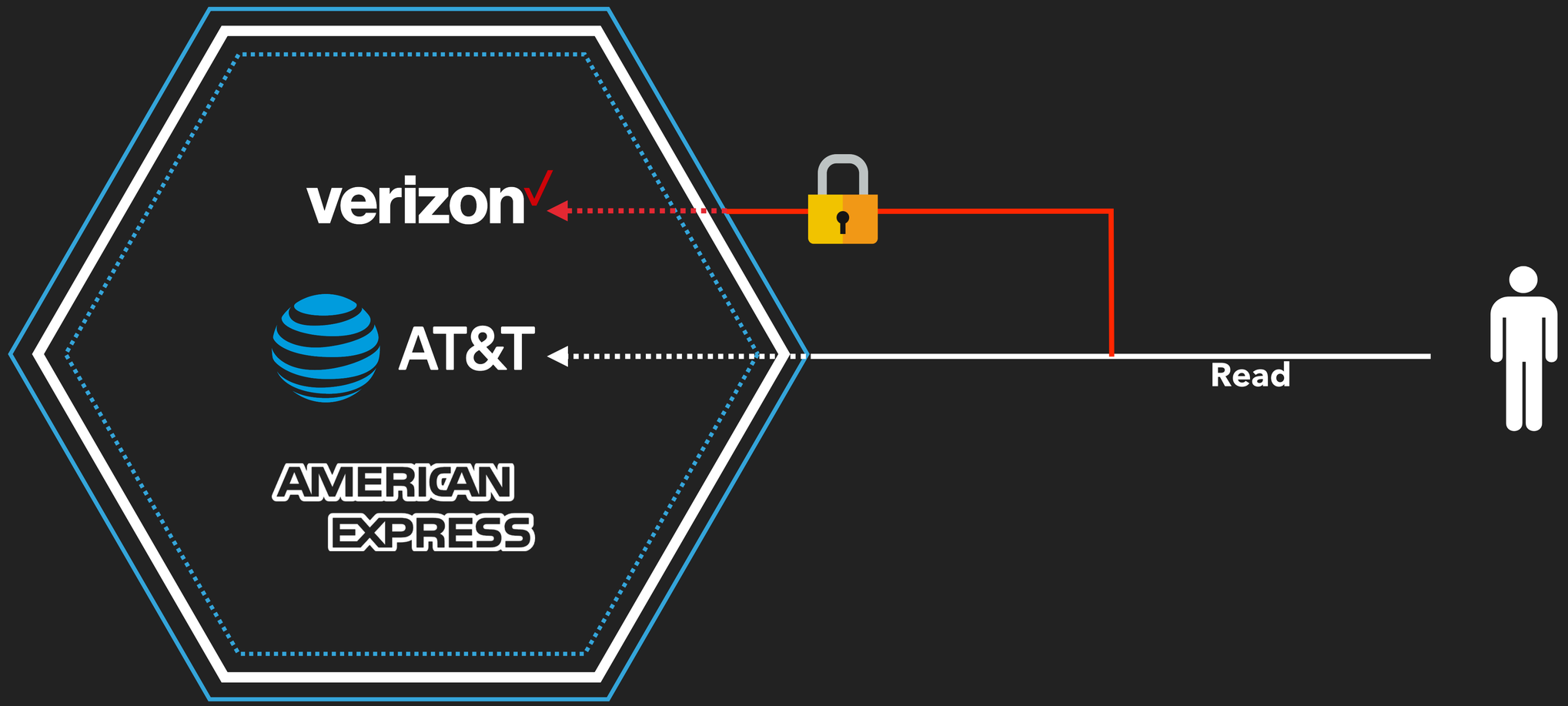
JWT


Payload
eyJXAiiJKV1Qi.eyJ1c2VySWQi4ZjItOGZhYi1jZWYzOTAjYwYQ.-xHVTCMdoHrcZxH
Header
Signature

JWT - PAYLOAD


```
{
  "email": "mfatemian@redventures.com",
  "userName": "mfatemian",
  "firstName": "Majid",
  "lastName": "Fatemian",
  "employeeID": "11520",
  "jti": "7bc4561ab-b6c8e2-76b1-31a3-a9bb90fb67c",
  "iat": 1487910598,
  "exp": 1487953798
}
```

AUTHORIZATION

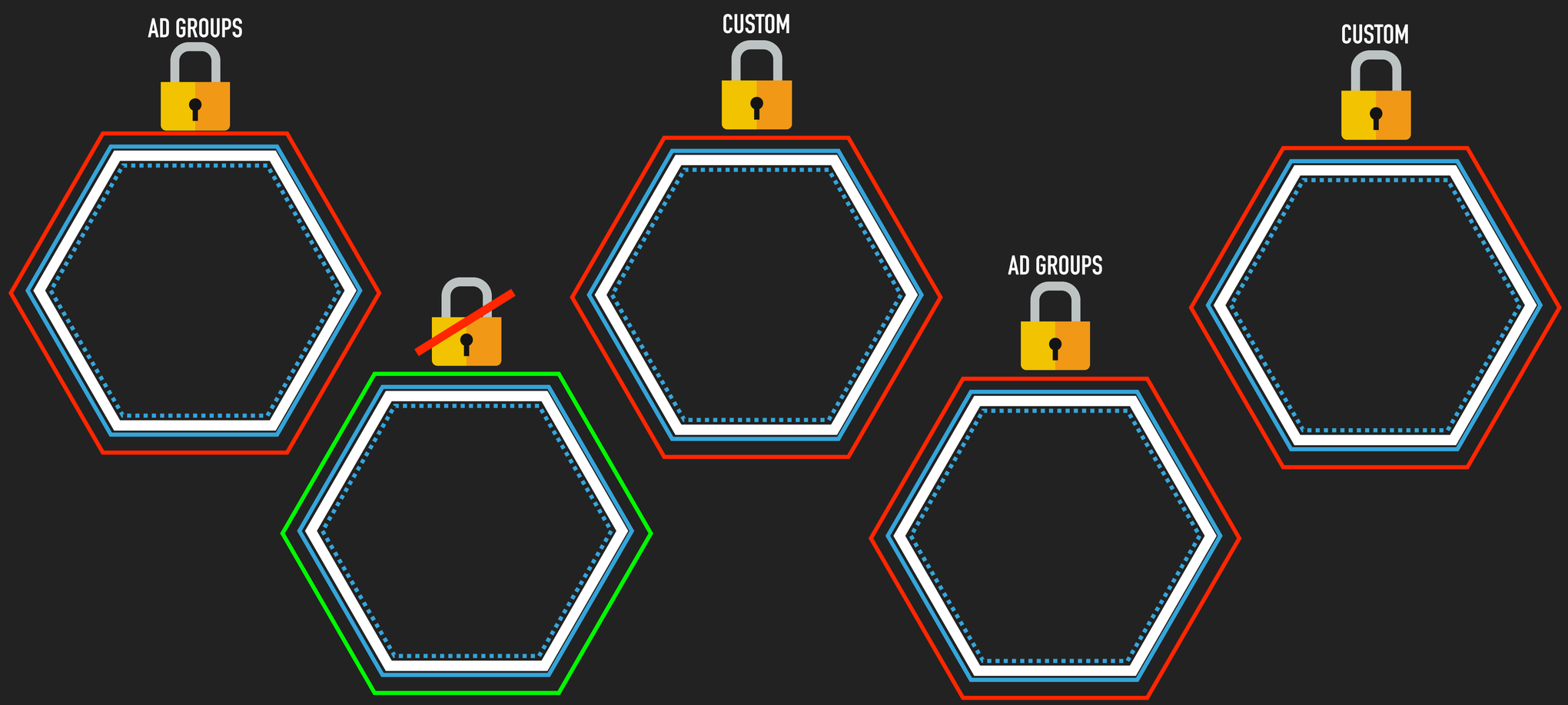

verizon
AT&T
AMERICAN EXPRESS
Read

AUTHORIZATION

CAN USER READ FROM ATT&T IN ANALYTICS? ✔

CAN USER READ FROM VERIZON IN ANALYTICS? ✘

THE PROBLEM

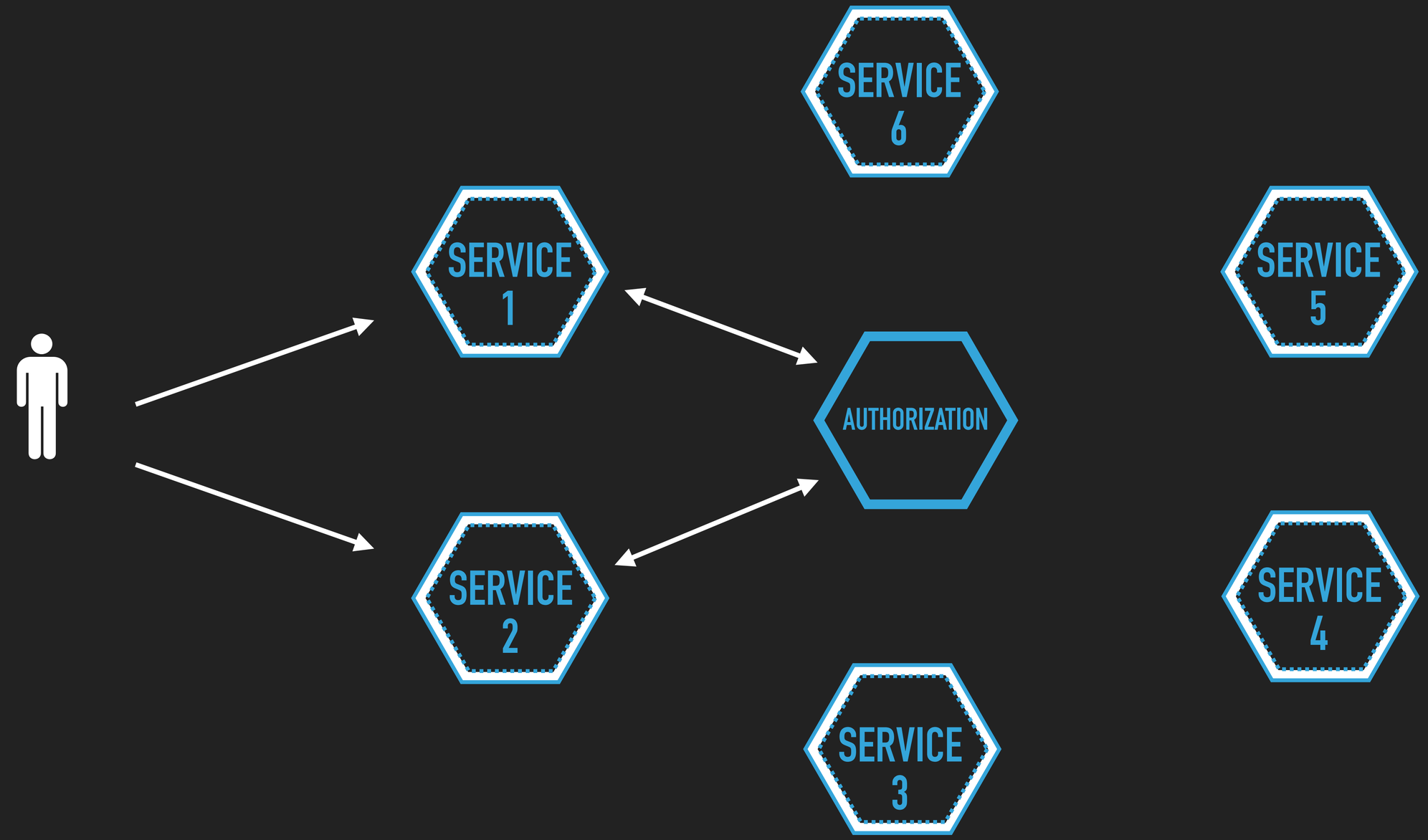


- Scattered
- Inconsistent
- No Monitoring
- No Centralized control

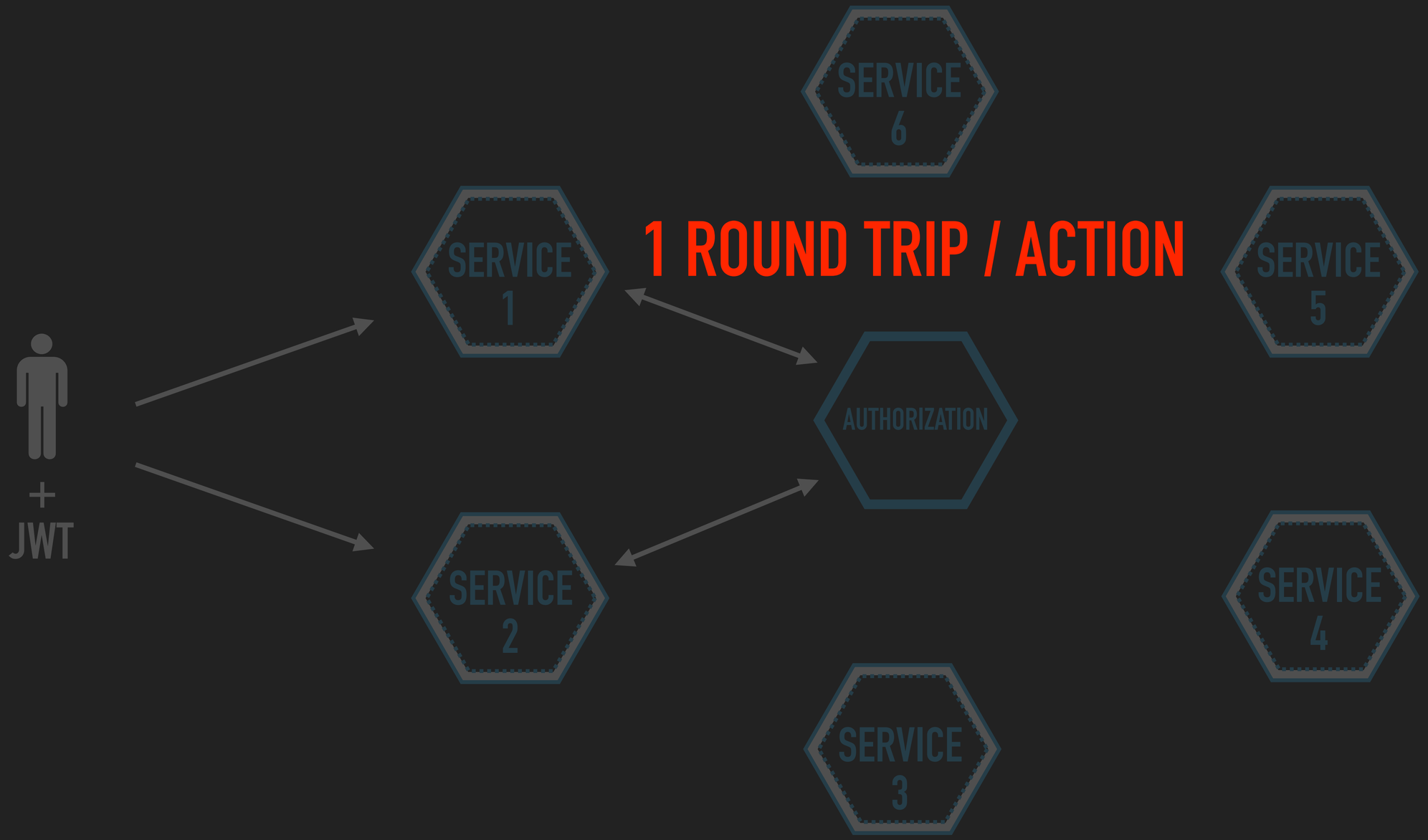
DESIRED SOLUTION

- Centralized
- Simple
- Scalable
- Monitoring
- Easily Manageable

EXISTING AUTHZ SOLUTIONS



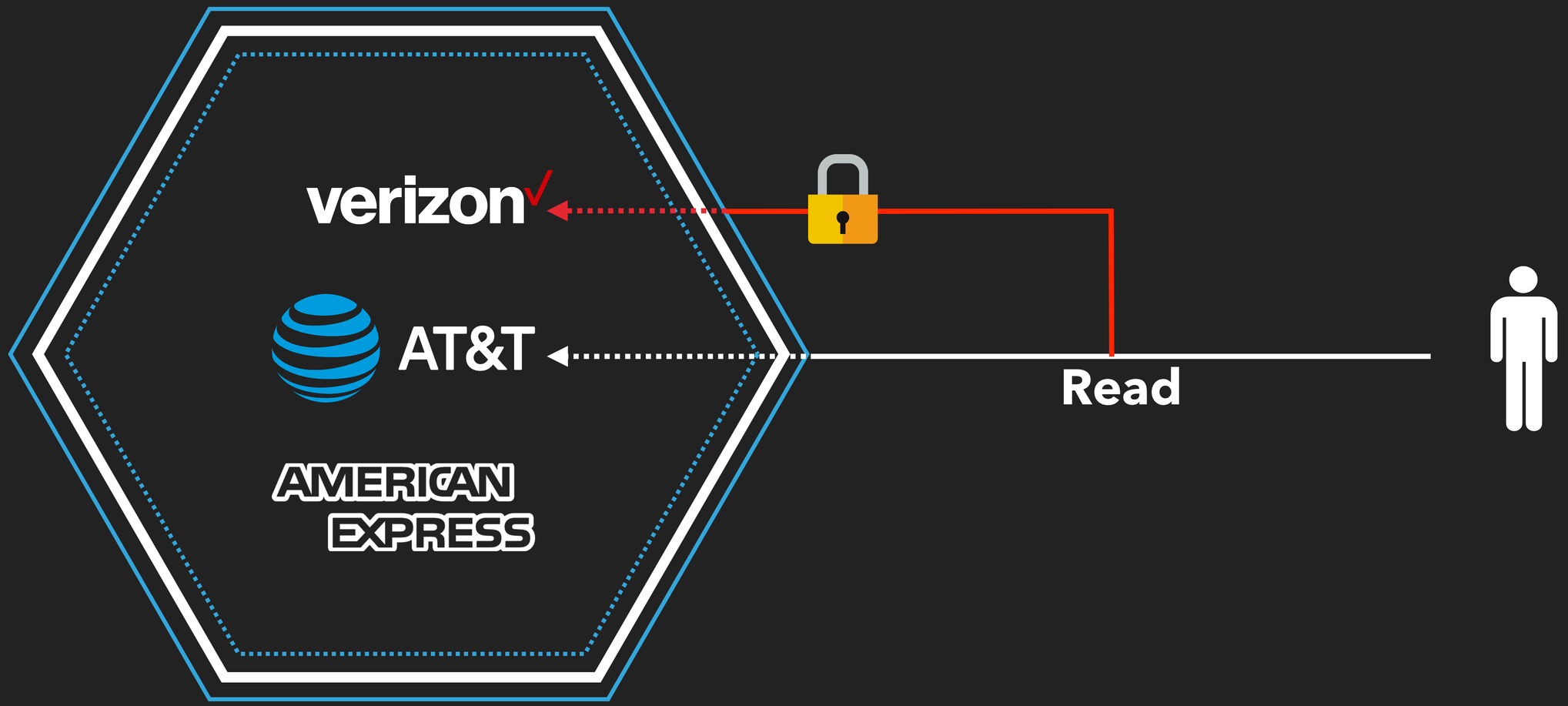
EXISTING AUTHZ SOLUTIONS

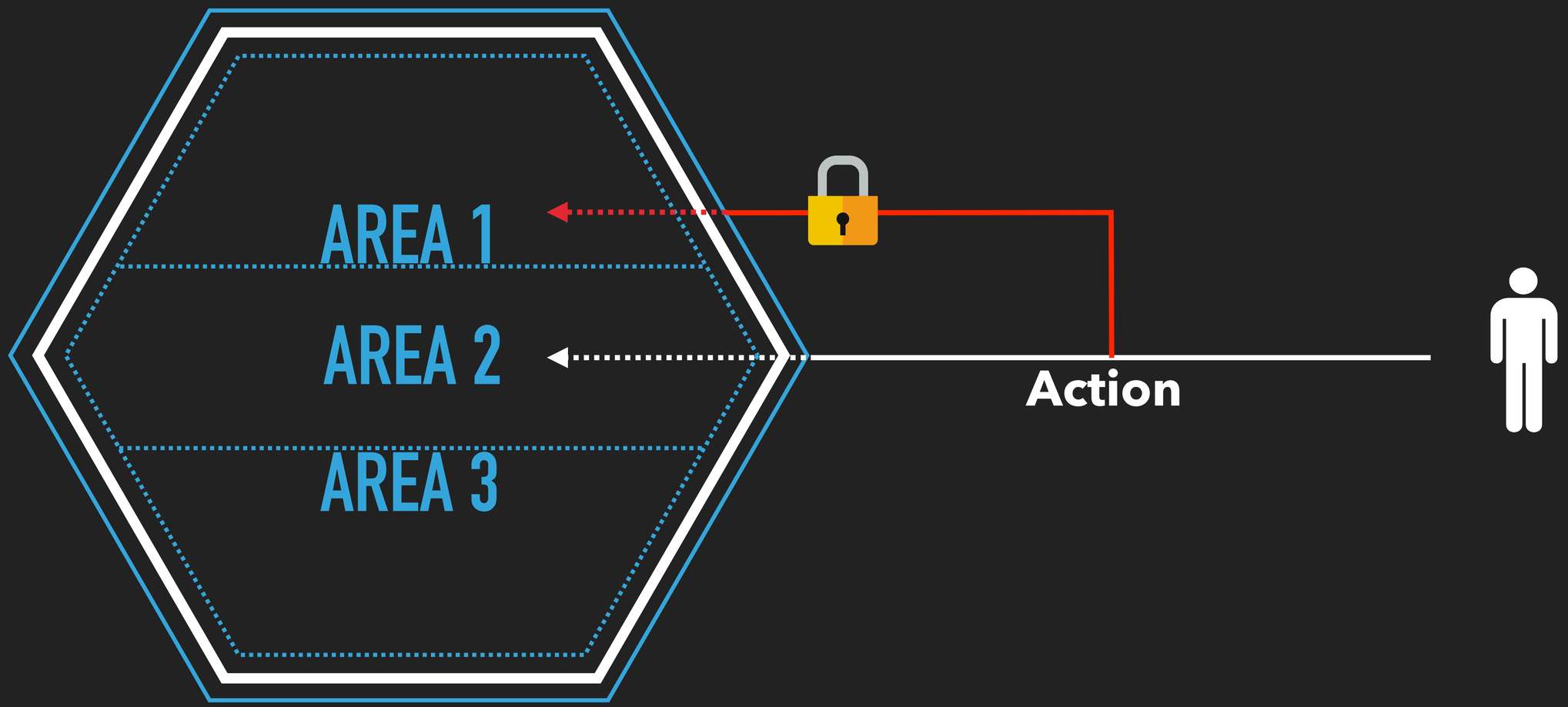


- Round-trips
- Roles, Groups, etc
- Complex

- ~~Round-trips~~
- ~~Roles, Groups, etc~~
- ~~Complex~~

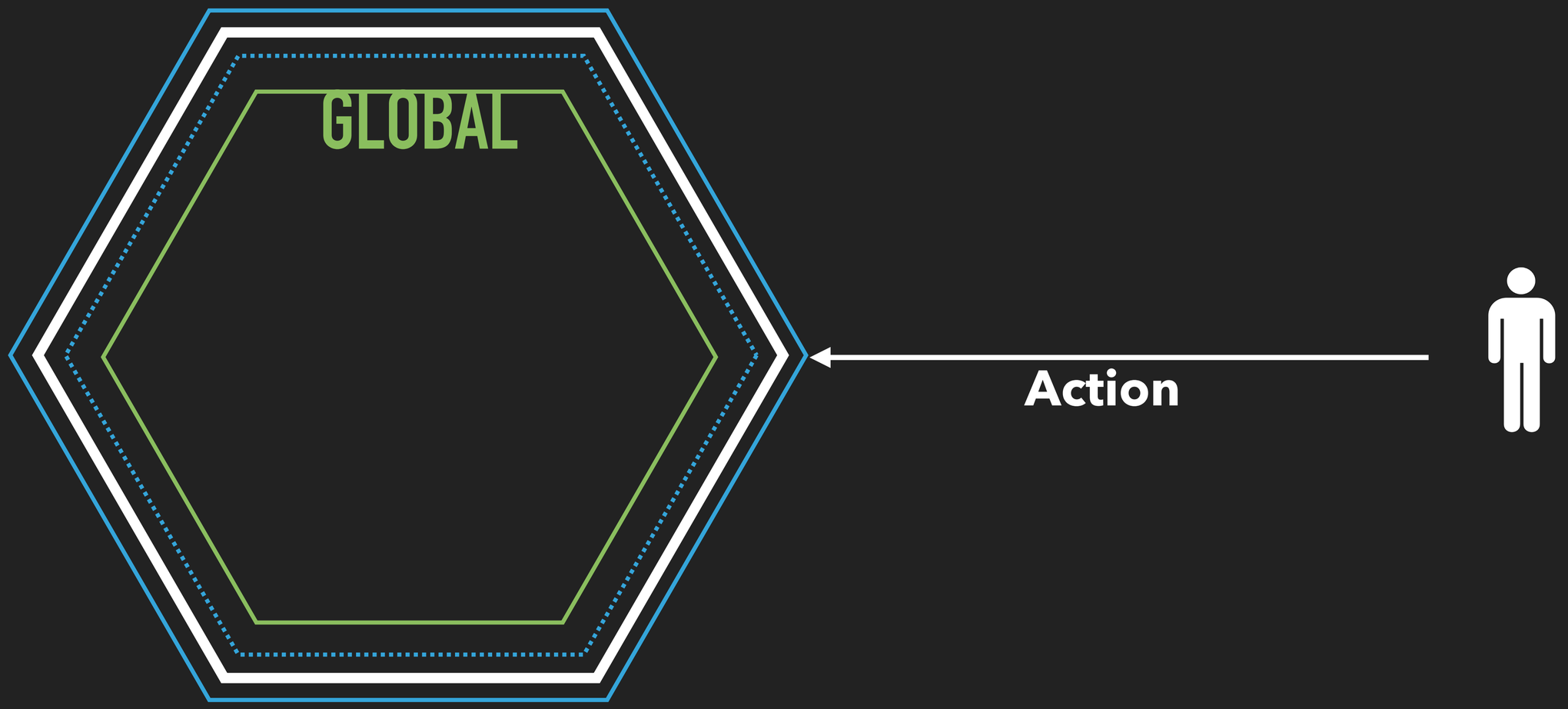
SIMPLIFIED AUTHORIZATION


verizon
AT&T
AMERICAN EXPRESS
Read


AREA 1
AREA 2
AREA 3
Action

SERVICE	AREA	ACTION
analytics	verizon	write

SERVICE	GLOBAL	ACTION
analytics	global	write


GLOBAL
Action


GLOBAL
AREA 1
AREA 2
AREA 3
Action

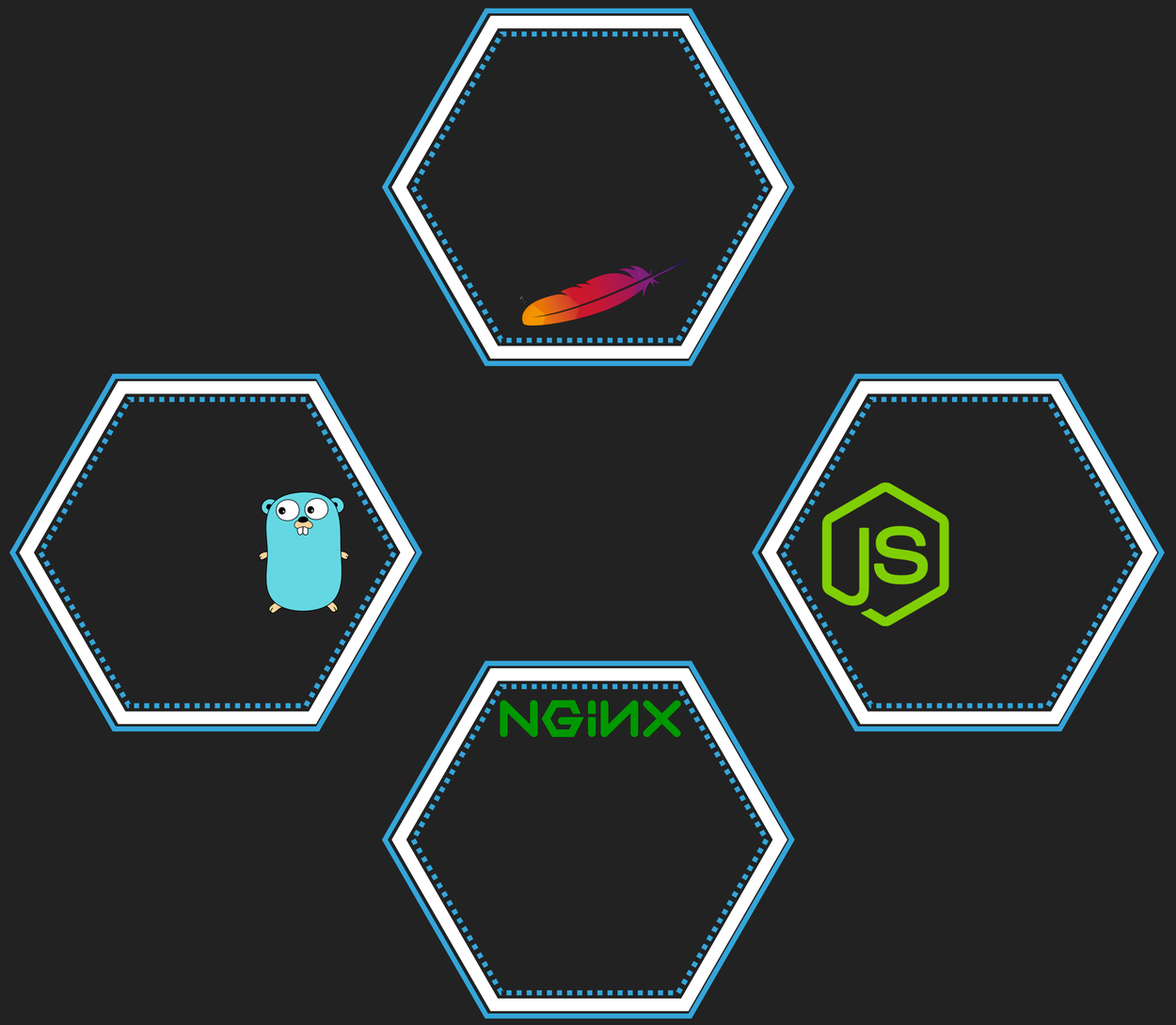
```
{
   "analytics": {
      "write": ["verizon", "att"],
      "read": ["global"]
   },
   "data_science": {
     "report": ["att"]
   }
}
```

JWT - PAYLOAD

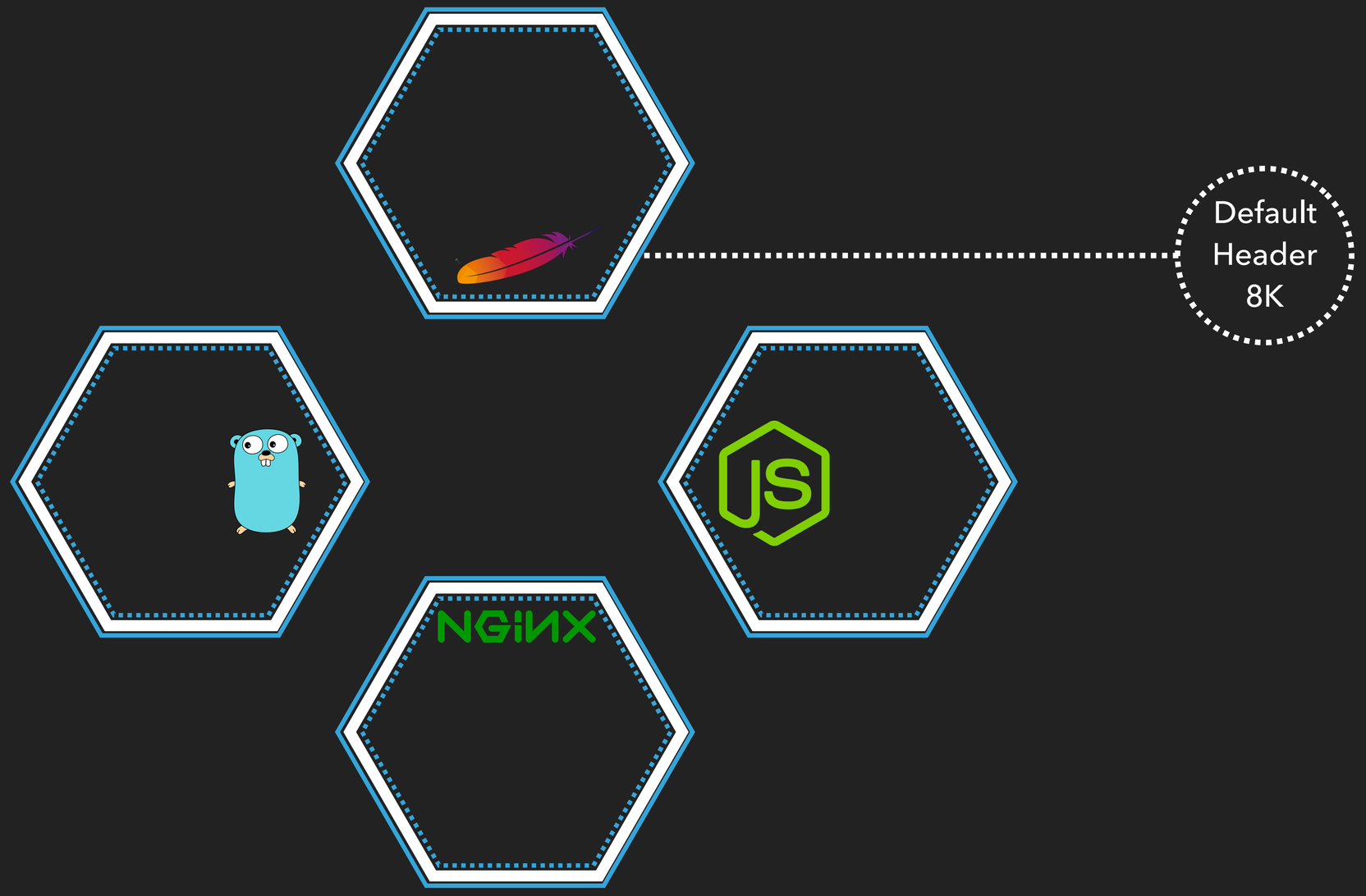

```
{
  "email": "mfatemian@redventures.com",
  "userName": "mfatemian",
  "firstName": "Majid",
  "lastName": "Fatemian",
  "employeeID": "11520",
  "permissions":{"analytics": {"write":
   ["verizon","att"],"read": ["global"]},"data_science":
   {"report": ["att"]}},
  "jti": "7bc4561ab-b6c8e2-76b1-31a3-a9bb90fb67c",
  "iat": 1487910598,
  "exp": 1487953798
}
```

JWT - PAYLOAD


```
{
  "email": "mfatemian@redventures.com",
  "userName": "mfatemian",
  "firstName": "Majid",
  "lastName": "Fatemian",
  "employeeID": "11520",
  "permissions":{"analytics": {"write":
   ["verizon","att"],"read": ["global"]},"data_science":
   {"report": ["att"]}},
  "jti": "7bc4561ab-b6c8e2-76b1-31a3-a9bb90fb67c",
  "iat": 1487910598,
  "exp": 1487953798
}
```


NGINX

HTTP 413 – REQUEST ENTITY TOO LARGE



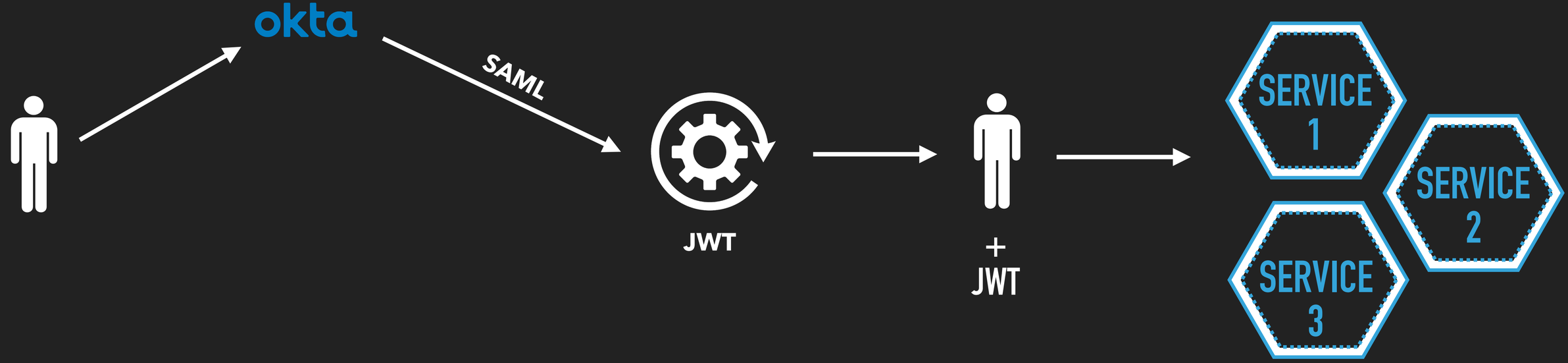
```
gzip | base64
```

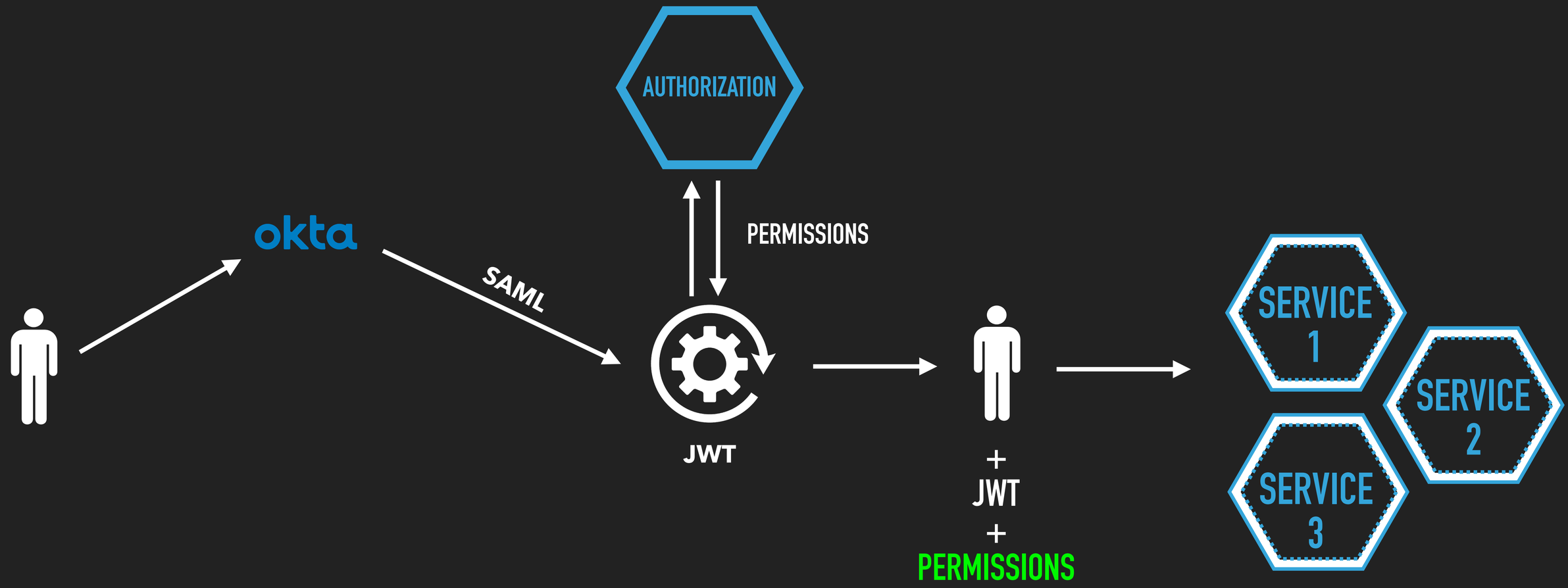
JWT - PAYLOAD

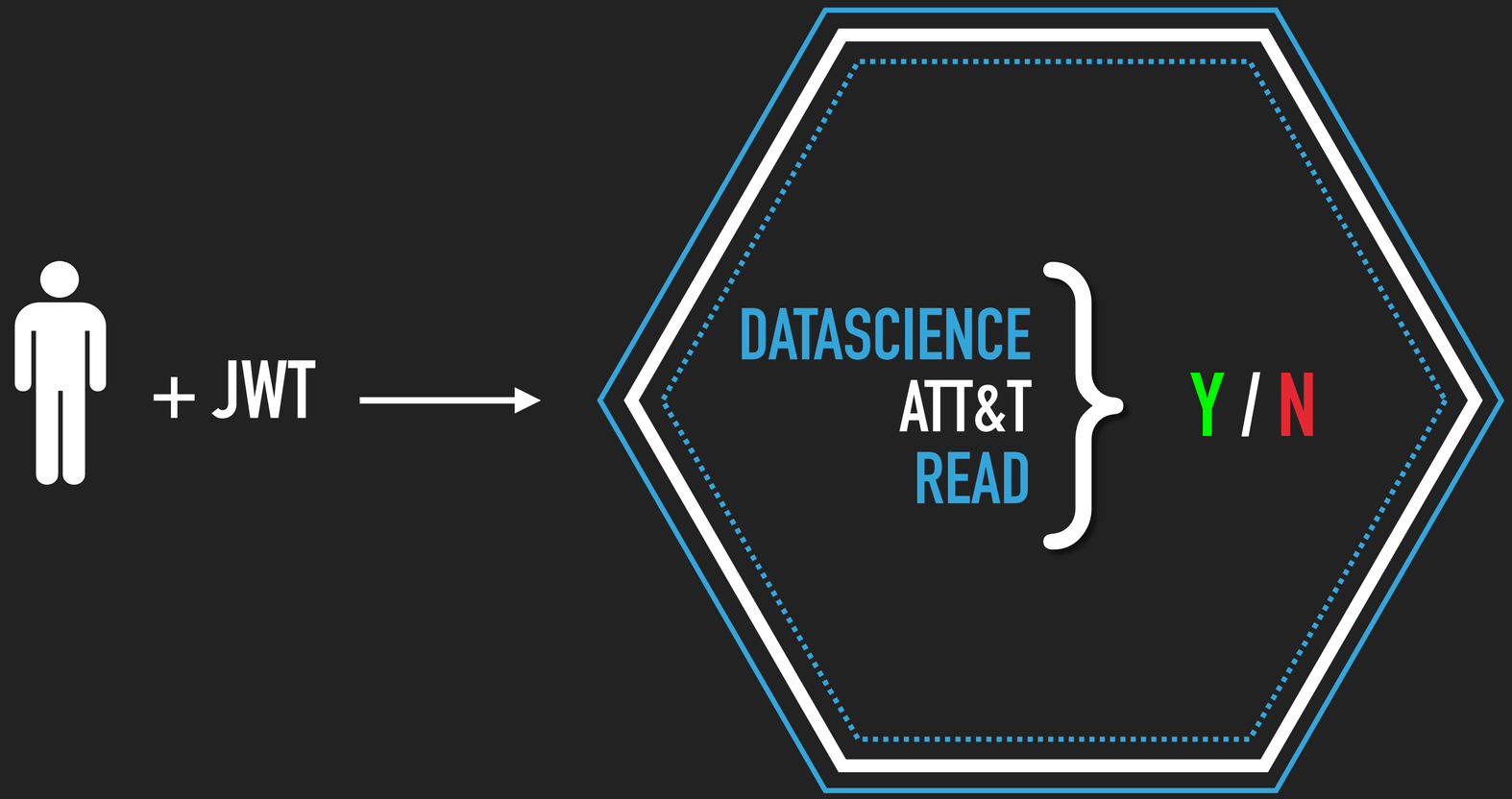

```
{
  "email": "mfatemian@redventures.com",
  "userName": "mfatemian",
  "firstName": "Majid",
  "lastName": "Fatemian",
  "employeeID": "11520",
  "permissions": "H4sIAAmrs1gAAx3L…qAIBRF0XnLeGN",
  "jti": "7bc4561ab-b6c8e2-76b1-31a3-a9bb90fb67c",
  "iat": 1487910598,
  "exp": 1487953798
}
```

JWT - PAYLOAD

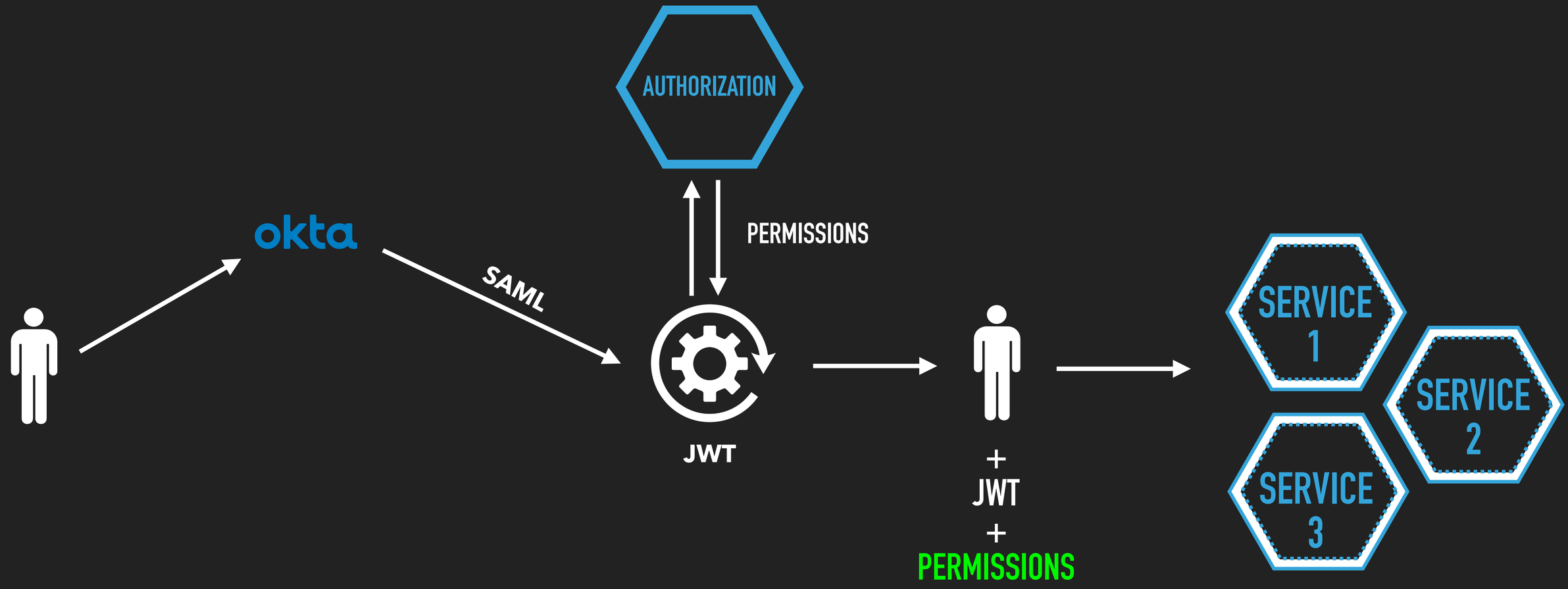

```
{
  "email": "mfatemian@redventures.com",
  "userName": "mfatemian",
  "firstName": "Majid",
  "lastName": "Fatemian",
  "employeeID": "11520",
  "permissions": "H4sIAAmrs1gAAx3L…qAIBRF0XnLeGN",
  "jti": "7bc4561ab-b6c8e2-76b1-31a3-a9bb90fb67c",
  "iat": 1487910598,
  "exp": 1487953798
}
```

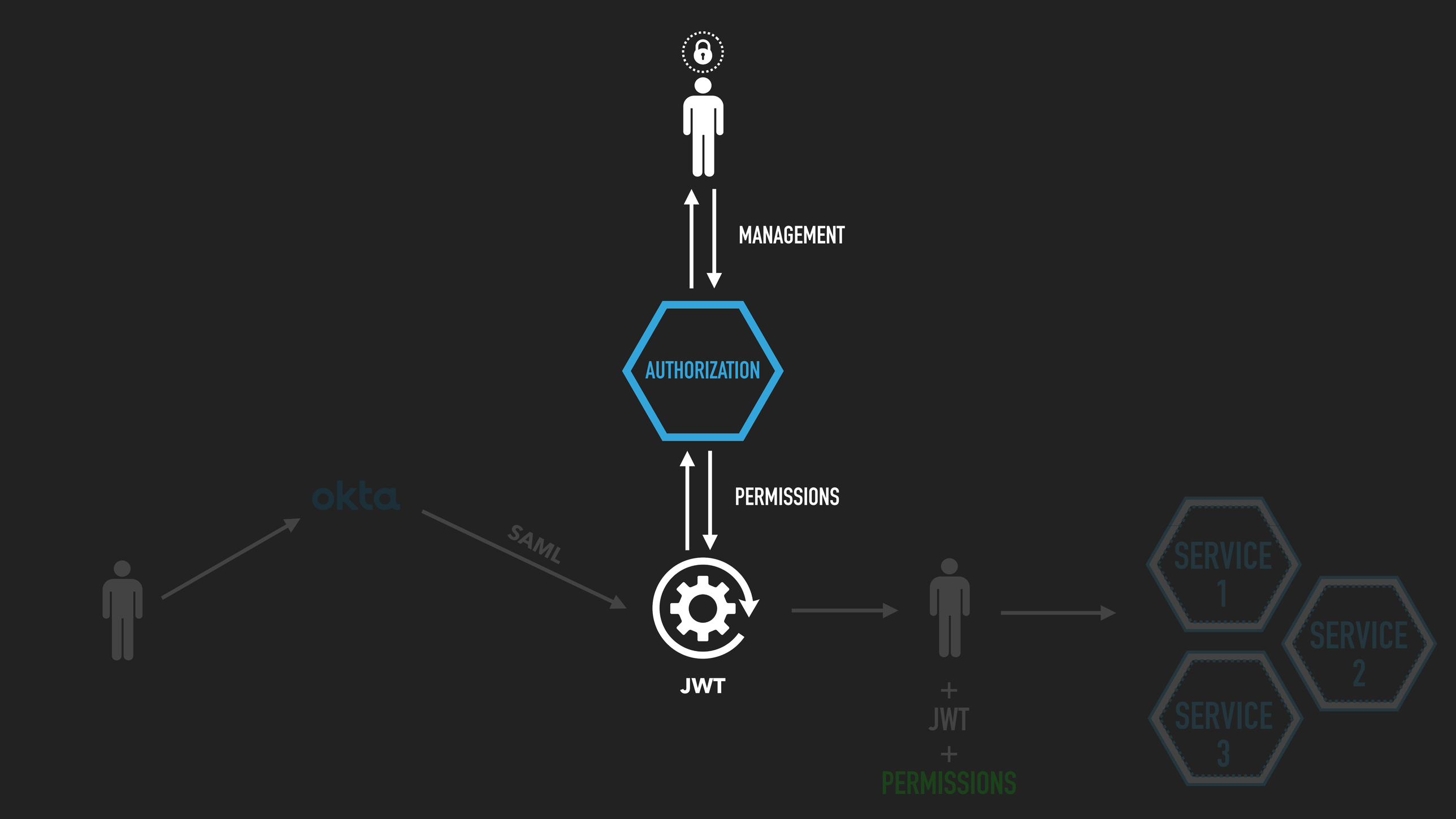

okta
SAML
JWT
+
JWT
SERVICE 1
SERVICE 2
SERVICE 3


AUTHORIZATION
PERMISSIONS
okta
SAML
JWT
+
JWT
+
PERMISSIONS
SERVICE 1
SERVICE 2
SERVICE 3

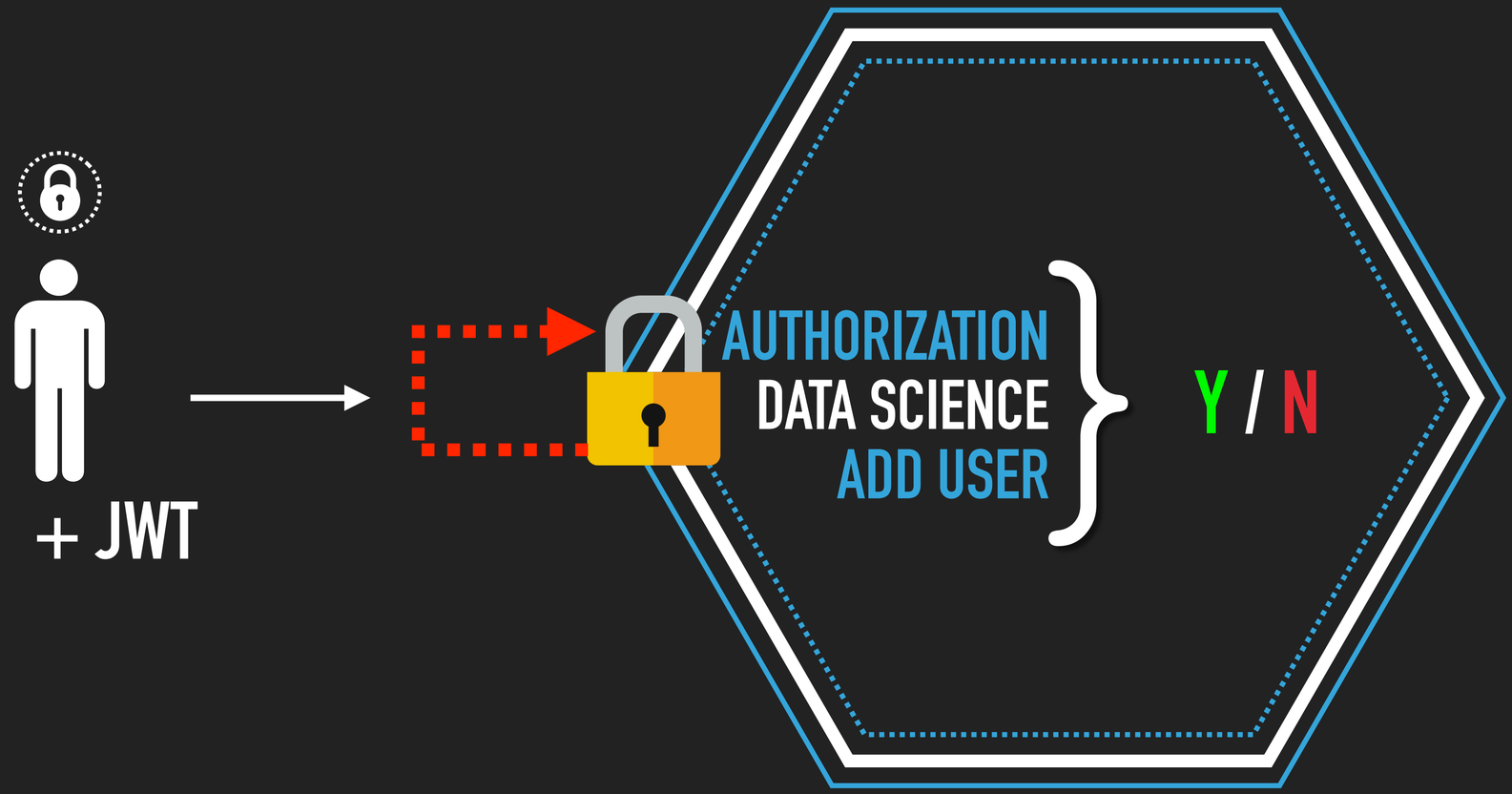

+ JWT
DATASCIENCE
ATT&T
READ
Y / N

- Centralized
- Simple
- Scalable
- Monitoring
- Easily Manageable


AUTHORIZATION
PERMISSIONS
okta
SAML
JWT
+
JWT
+
PERMISSIONS
SERVICE 1
SERVICE 2
SERVICE 3

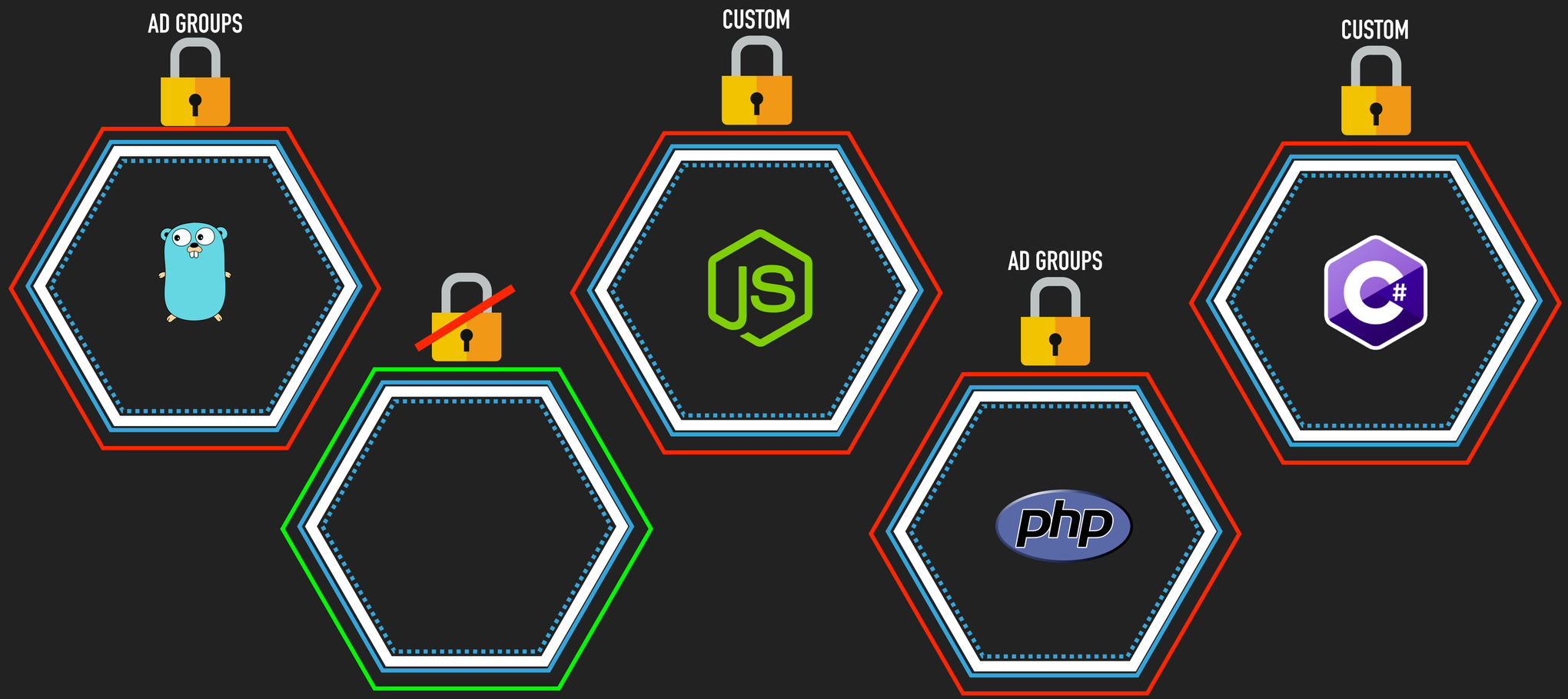

MANAGEMENT
AUTHORIZATION
PERMISSIONS
okta
SAML
JWT
+
JWT
+
PERMISSIONS
SERVICE 1
SERVICE 2
SERVICE 3

AUTHORIZATION SERVICE, AUTHORIZES ITSELF



INTEGRATION

THE PROBLEM

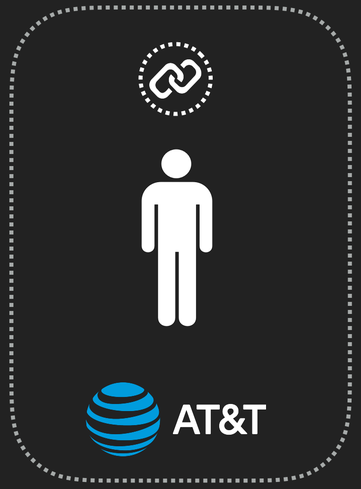


CLIENT LIBS

- golang
- C#
- JavaScript
- PHP

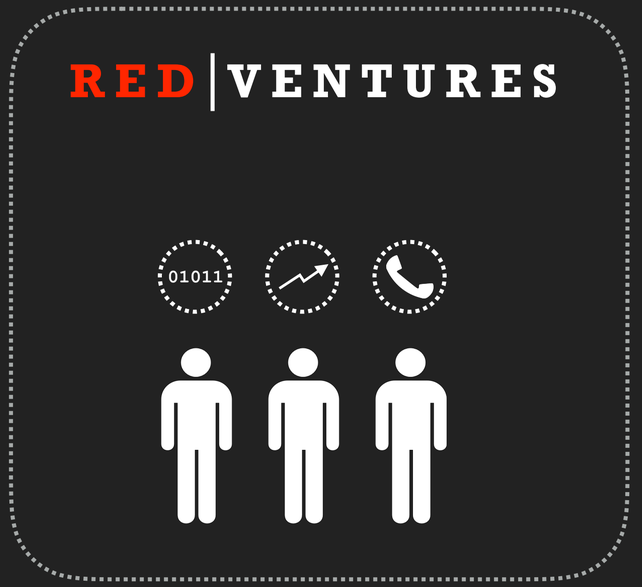
```
IsAuthorized(JWT, "data_science", "verizon", "read")
```

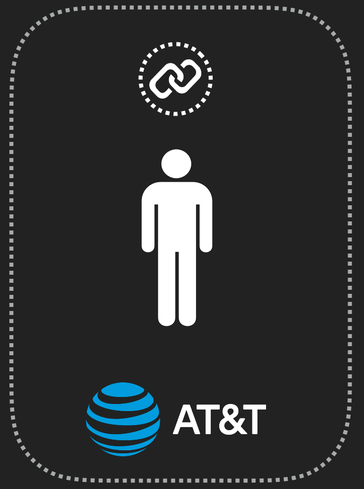
True | **False**


AT&T


verizon

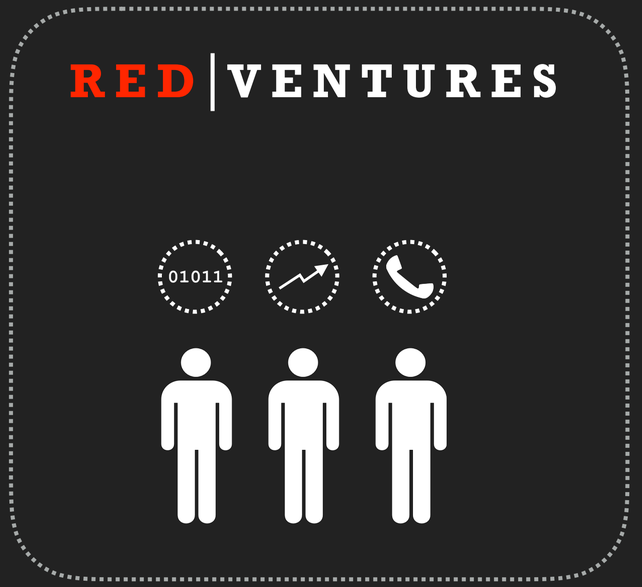

GEO
TRACKING
BILLING
DATA SCIENCE
CHAT
ANALYSIS
ORDERING
SERVICE ABILITY


RED | VENTURES
01011

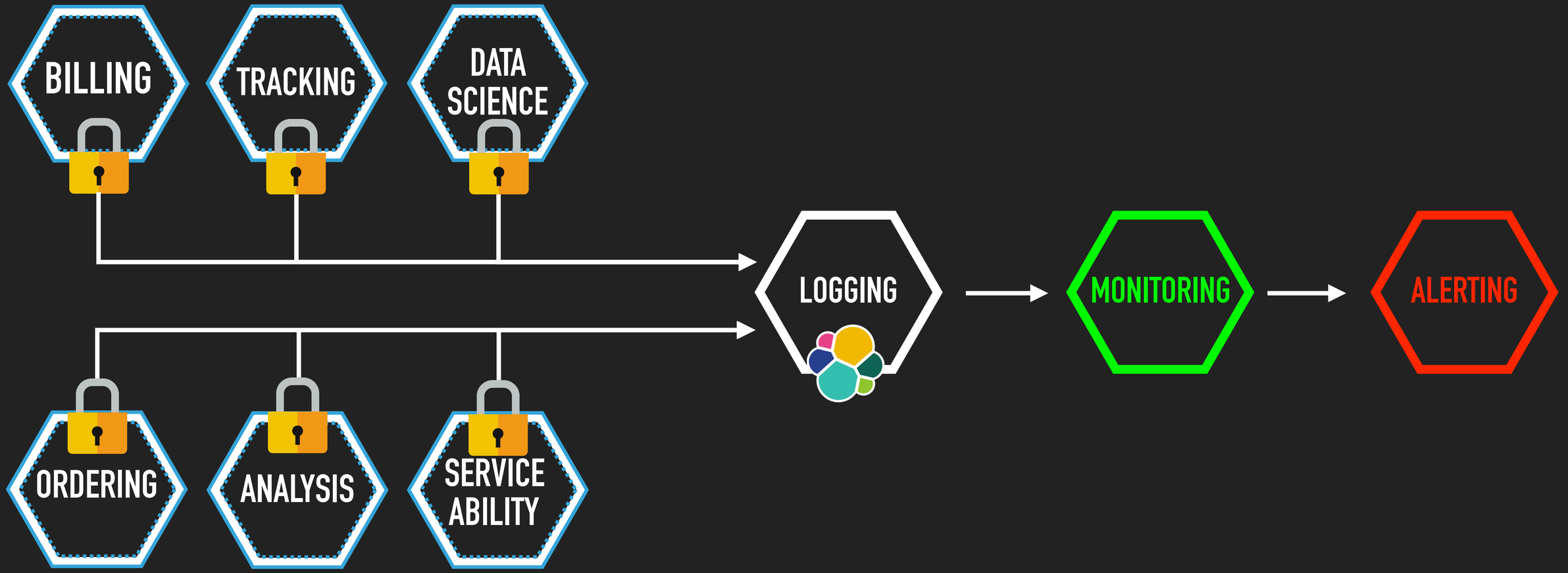

AT&T


verizon


GEO
BILLING
TRACKING
DATA SCIENCE
CHAT
ANALYSIS
ORDERING
SERVICE ABILITY


RED | VENTURES
01011

MONITORING & ALERTING



- Centralized
- Simple
- Scalable
- Monitoring
- Easily Manageable

FUTURE WORK

- Open source
- Okta dependency

1. REUSE > BUILD
2. TOKEN BASED AUTH
3. SIMPLE ≠ INSECURE

THANK YOU!
QUESTIONS?