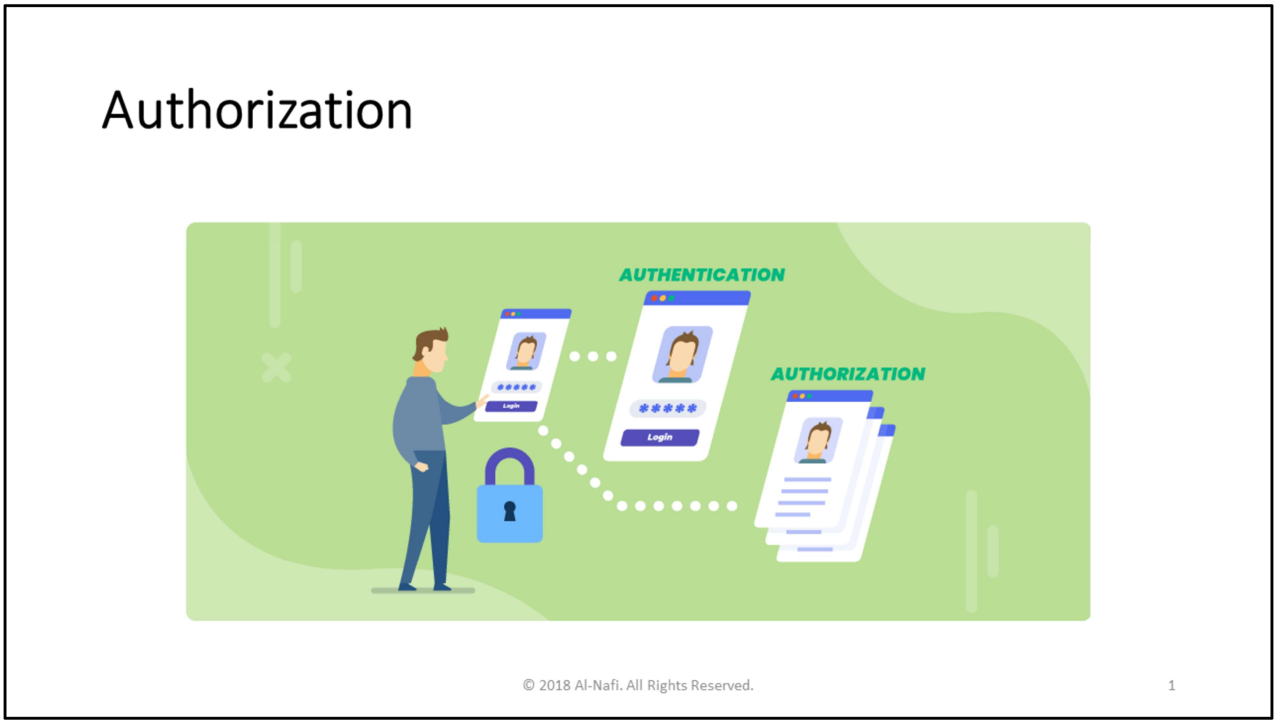
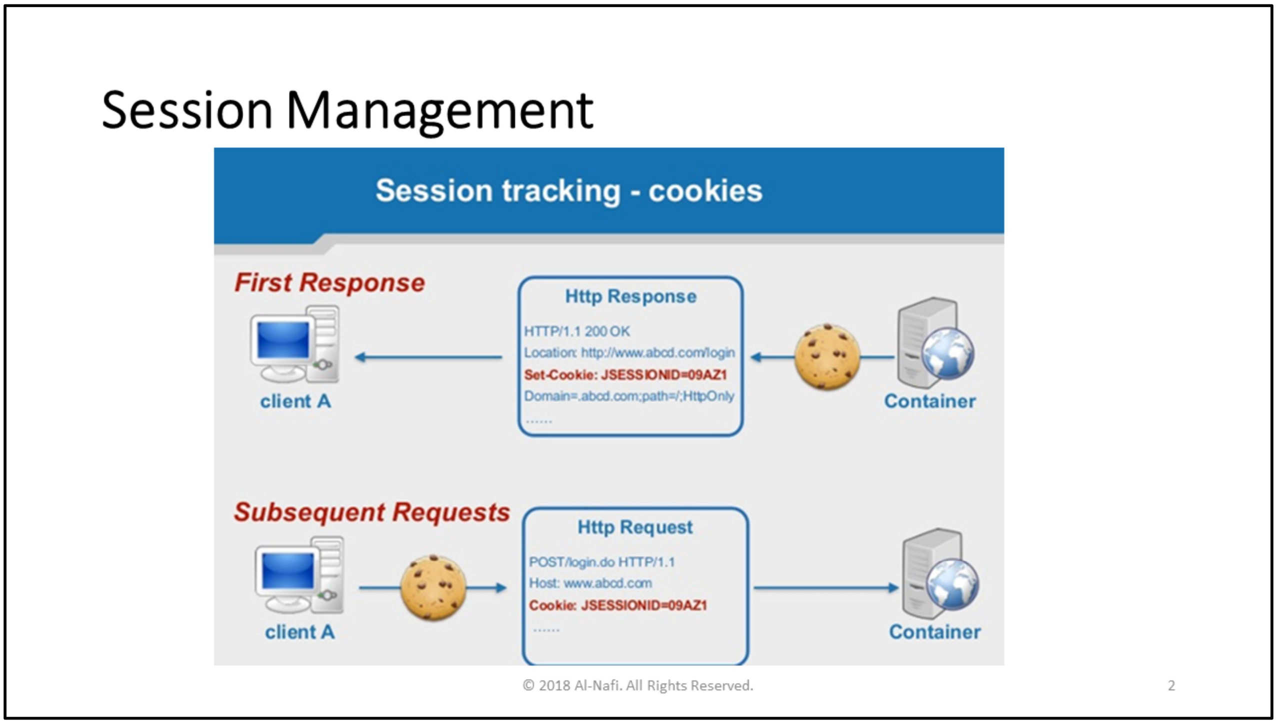


Authorization

Authorization defines what resources users may have access to.

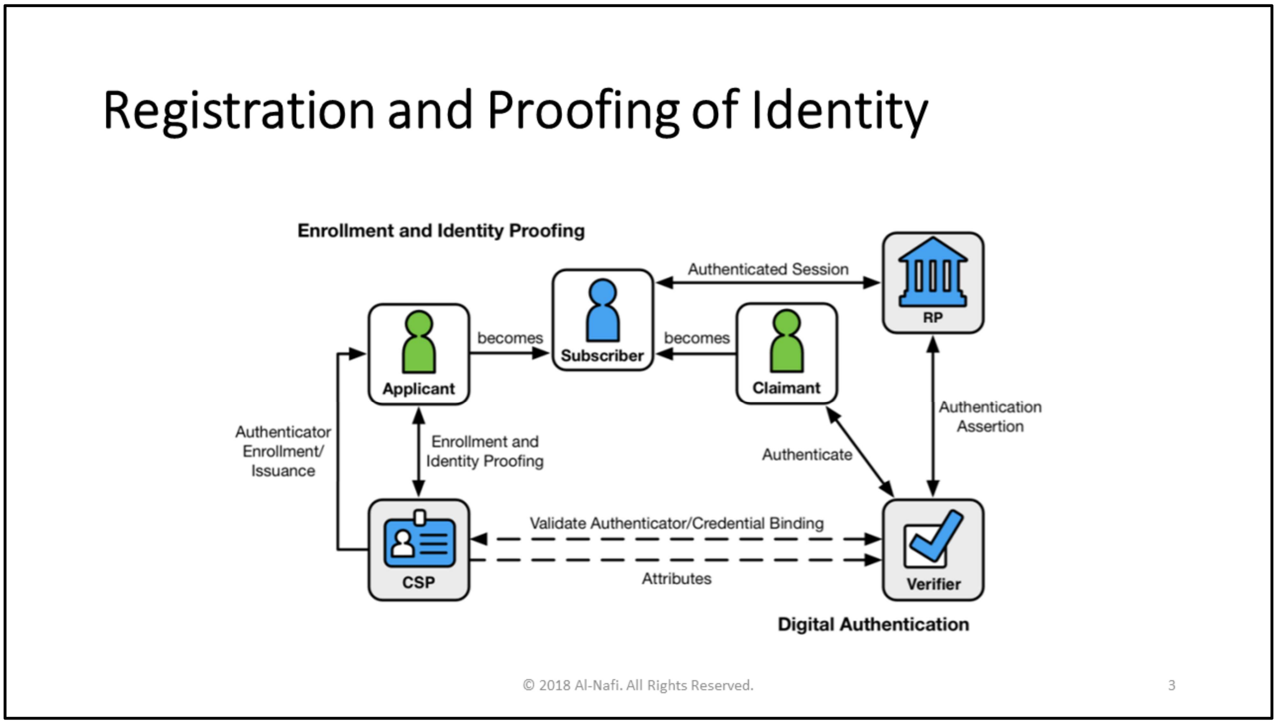


Session Management

```
HTTP/1.1 200 OK
Location: http://www.abcd.com/login
Set-Cookie: JSESSIONID=09AZ1
Domain=.abcd.com;path=/;HttpOnly
......
```

```
POST/login.do HTTP/1.1
Host: www.abcd.com
Cookie: JSESSIONID=09AZ1
......
```

Session management is related to when a user is authenticated, authorized, and held accountable for using system resources. The system must maintain an uninterrupted path of protection of resources by means of system management. Open Web Application Security Project (OWASP) Top 10 number 2 threat is broken authentication and session management. RFC 2965 provides an example of how to maintain session managements with cookies. When a user accesses a website, the user’s actions and identity are tracked across various requests from that website. A state of these interactions is maintained in a session cookie. Evidence of this state is maintained by linking all new connections across the entirety of a session to the cookie. Cookie handling achieves non-repudiation; effectively leveraging an audit trail of session activity.



Registration and Proofing of Identity

3

Registration and proofing of an identity are processes that connect an entity or user identity to an access control system that creates a confirmed relationship of trust that an entity is who he or she claims to be. The process of proving that a person is authentically the person that is being claimed can be challenging and even serve as an opening for impersonation. If a user is valid, there is also the threat that the user can be a malicious or bad actor. Writing for the *New Yorker*, Peter Steiner stated succinctly, “On the Internet no one knows that you are a dog.”

Herein lies the crux of the concern; balancing the needs of controlling access to valued assets and the simplicity of registering and proofing the credentials of the potential user of a system.

The Digital Identity Guidelines of NIST SP 800-63-3 contains recommendations to support, among other items, requirements for identity proofing and registration. These requirements are the following:

Identity Assurance Level (IAL) refers to the identity proofing process. A category that conveys the degree of confidence that the applicant’s claimed identity is their real identity

Identity Assurance Levels

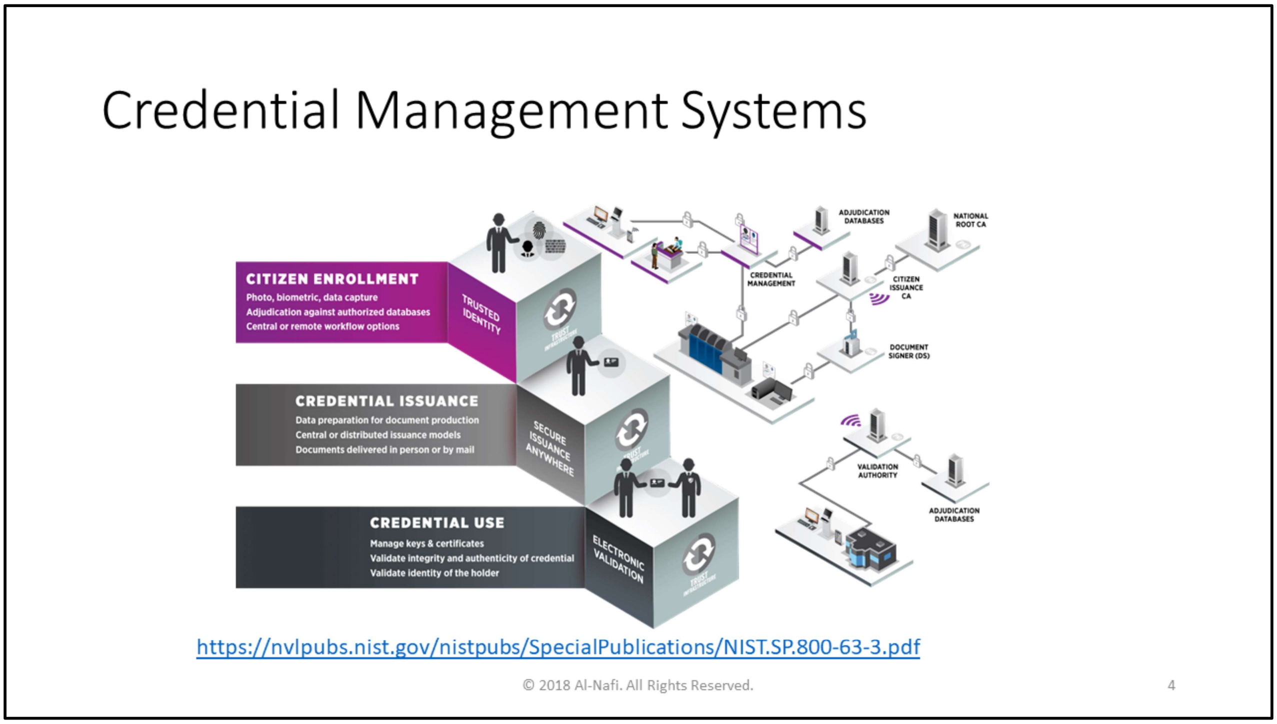
IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.

IAL2: At IAL2, either remote or in-person identity proofing is required.

IAL2 requires identifying attributes to have been verified in person or remotely, using, at a minimum, the procedures given in SP 800-63A.

IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized Credential Service Provider (CSP) representative through examination of physical documentation as described in SP 800-63A.

- Authenticator Assurance Level (AAL) refers to the authentication process.
- Federation Assurance Level (FAL) refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).



Credential Management Systems

CITIZEN ENROLLMENT
Photo, biometric, data capture
Adjudication against authorized databases
Central or remote workflow options

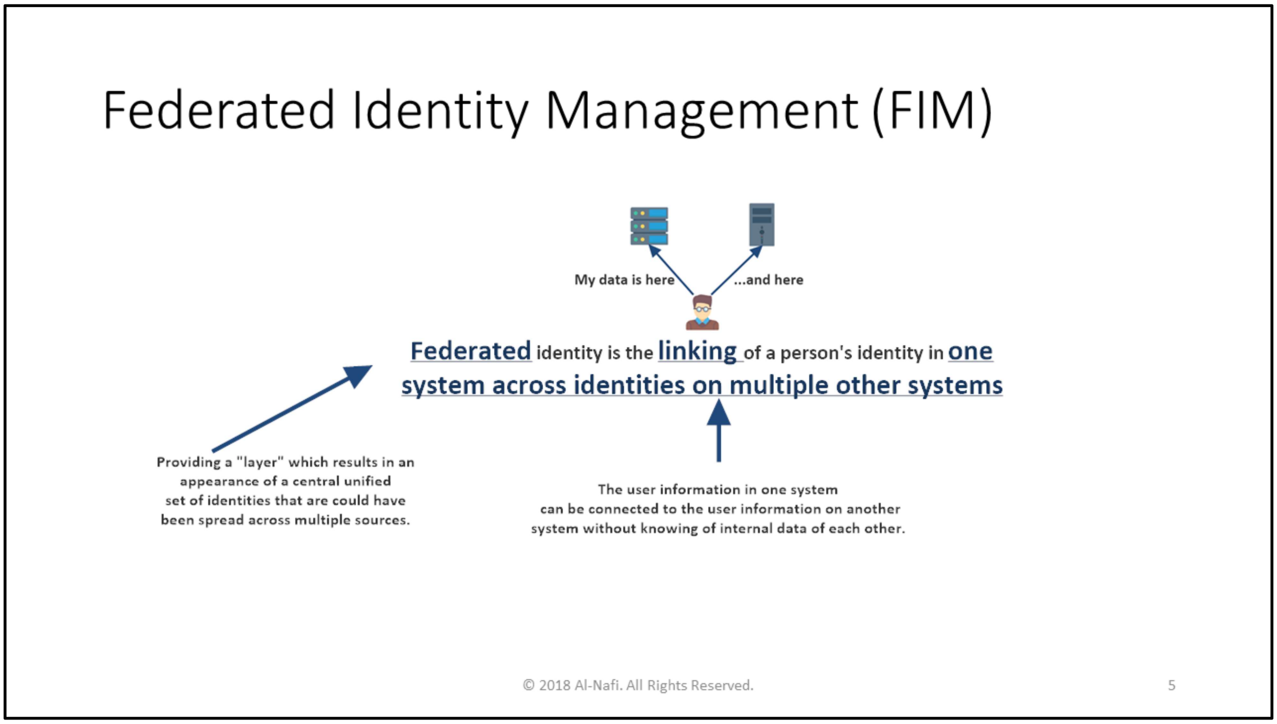
CREDENTIAL ISSUANCE
Data preparation for document production
Central or distributed issuance models
Documents delivered in person or by mail

CREDENTIAL USE
Manage keys & certificates
Validate integrity and authenticity of credential
Validate identity of the holder

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

NIST SP 800-63-3 describes a credential as a binding between an authenticator and a subscriber by means of an identifier. The credential may be collected and managed by the CSP, although it is possessed by the claimant. Credential examples include but are not limited to smart cards, private/public cryptographic keys, and digital certificates. The FICAM Roadmap and Implementation Guidance Version 2.0 within the U.S. federal government has the following five-step enrollment process:

1. Sponsorship: An authorized entity sponsors claimant for a credential with a CSP.
2. Enrollment: The sponsored claimant enrolls for the credentials from a CSP. This step would include identity proofing, which might include capture of biographic and biometric data.
3. Credential Production: Credentials are produced in the form of smart cards, private/public cryptographic keys, and digital certificates.
4. Issuance: Claimant is issued credential.
5. Credential Lifecycle Management: Credentials are maintained through activities that includes revocation, reissuance, re-enrollment, expiration, suspension, or reinstatement.

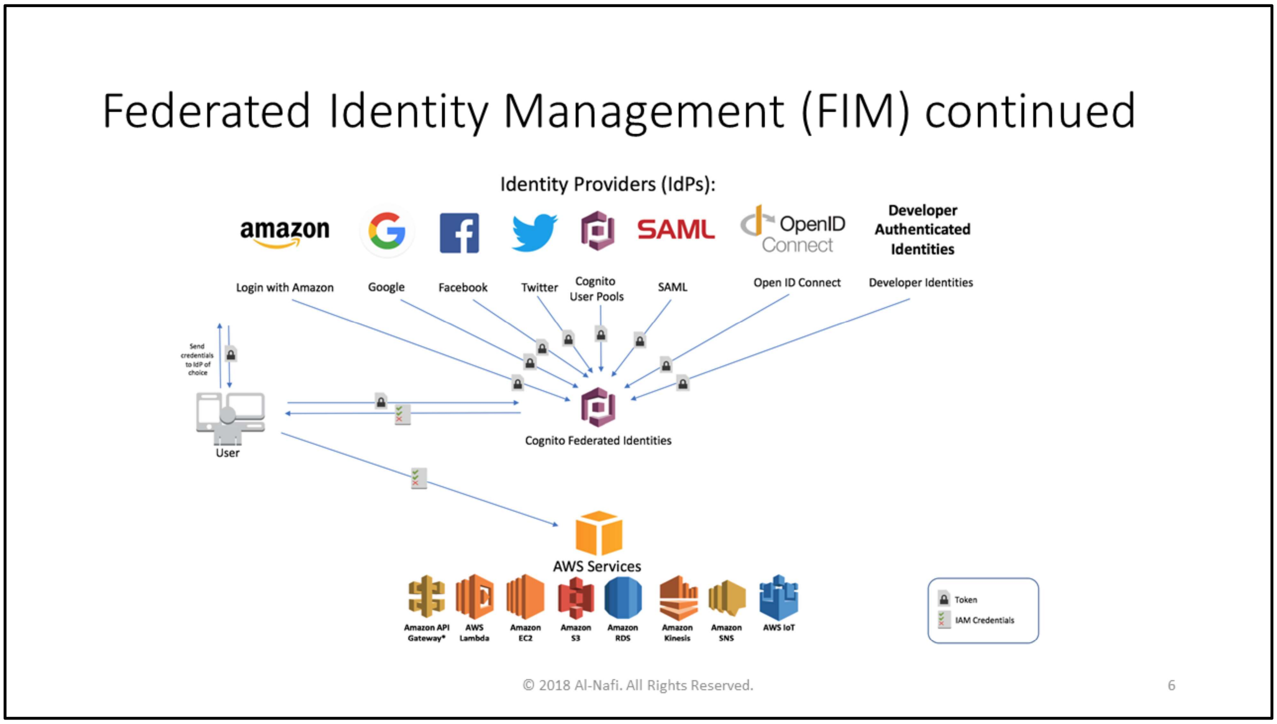


Federated Identity Management (FIM)

Federated identity is the **linking** of a person's identity in **one system across identities on multiple other systems**

Providing a "layer" which results in an appearance of a central unified set of identities that are could have been spread across multiple sources.

The user information in one system can be connected to the user information on another system without knowing of internal data of each other.

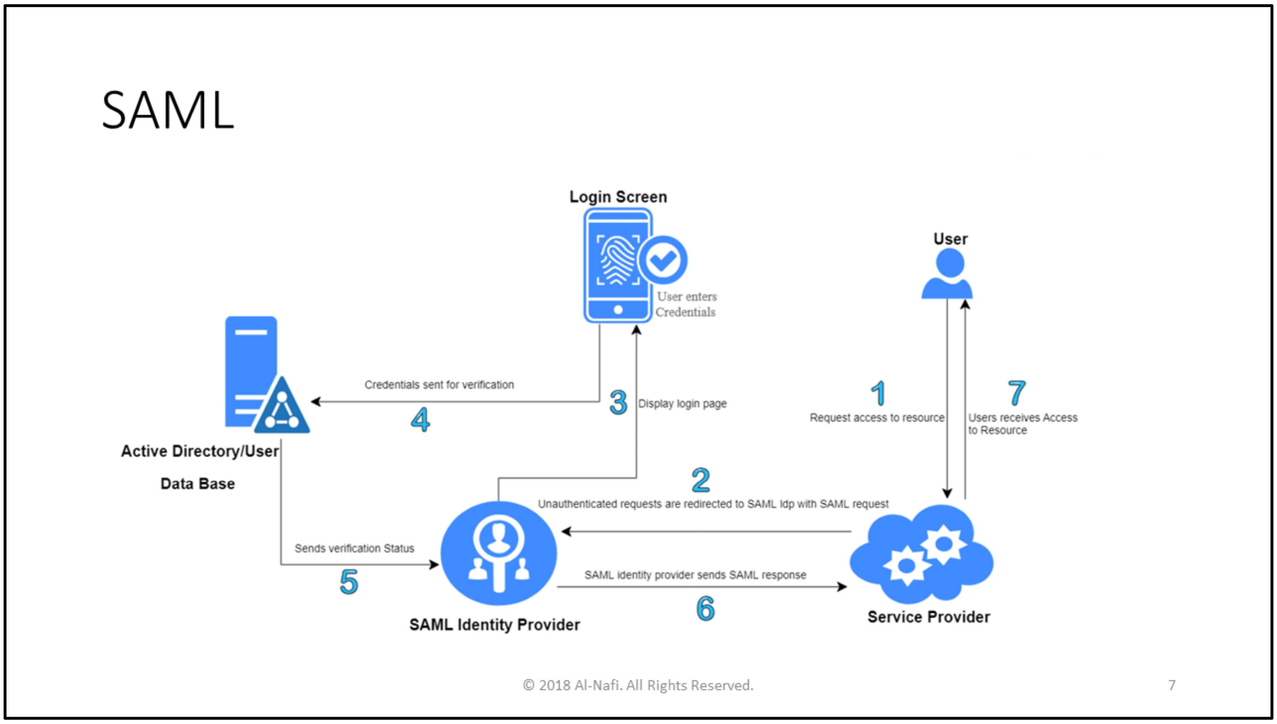


Federated Identity Management (FIM) continued

When disparate organizations have a need to share common information, federated identity management (FIM) solutions are sought. Think of businesses that use social media platforms such as Linkedin and Twitter but have different business models and corporate goals and missions.

Twitter:
“Twitter is what’s happening in the world and what people are talking about right now.”

Linkedin:
“Creating a digital map of the global economy to connect talent with opportunity at massive scale.” Although Linkedin and Twitter are markedly different in their mission statements, they share a common customer base. The common customers between Linkedin and Twitter may at times want the information that is resident on one service provider platform to appear automatically and synchronously on another service provider platform.



SAML

Login Screen
User enters Credentials
User
Active Directory/User Data Base
SAML Identity Provider
Service Provider
1
Request access to resource
2
Unauthenticated requests are redirected to SAML Idp with SAML request
3
Display login page
4
Credentials sent for verification
5
Sends verification Status
6
SAML identity provider sends SAML response
7
Users receives Access to Resource

7

Security Assertion Markup Language (SAML) and Open Authorization (OAuth)

SAML and OAuth 2.0 are two protocols that support the access and authorization that is required to link disparate organizations.

SAML defines an XML-based framework for describing and exchanging security information between online business relationships. This security information is maintained in SAML assertions that work between trusted security domain boundaries.

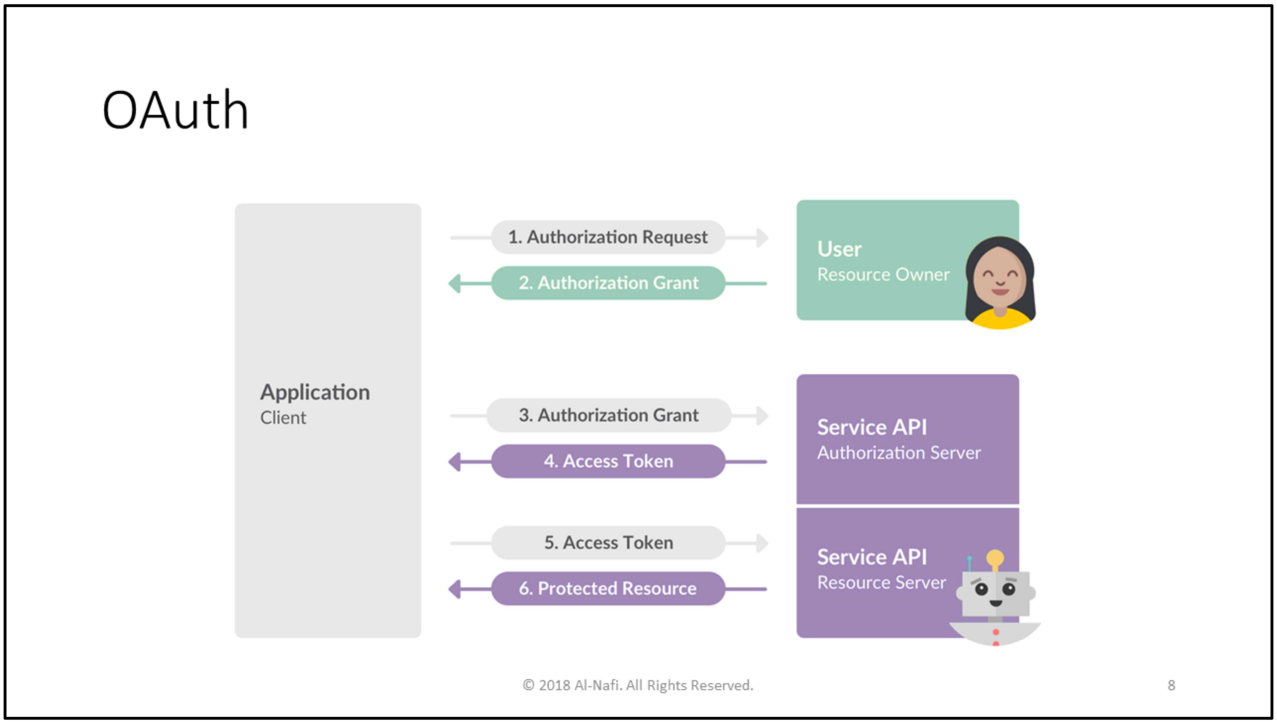
The SAML standard follows a prescribed set of rules for requesting, creating, communicating, and using SAML assertions. SAML has three roles and four primary components.

SAML roles:

1. Identity provider (IdP)
2. Service provider / relying party
3. User/principal

SAML components:

1. Assumptions-defines how SAML attributes, authentication, and authorization request-response protocol messages can be exchanged between systems using common underlying communication protocols and frameworks.
2. Bindings-defines how SAML assertions and protocol message exchanges are conducted with response/request pairs.
3. Protocols-defines what protocols are used, which include SOAP and HTTP.
4. Profiles-defines specific sets of rules for a use case for attributes, bindings, and protocols for a SAML session.



OAuth

Application
Client

1. Authorization Request

2. Authorization Grant

User
Resource Owner

3. Authorization Grant

4. Access Token

Service API
Authorization Server

5. Access Token

6. Protected Resource

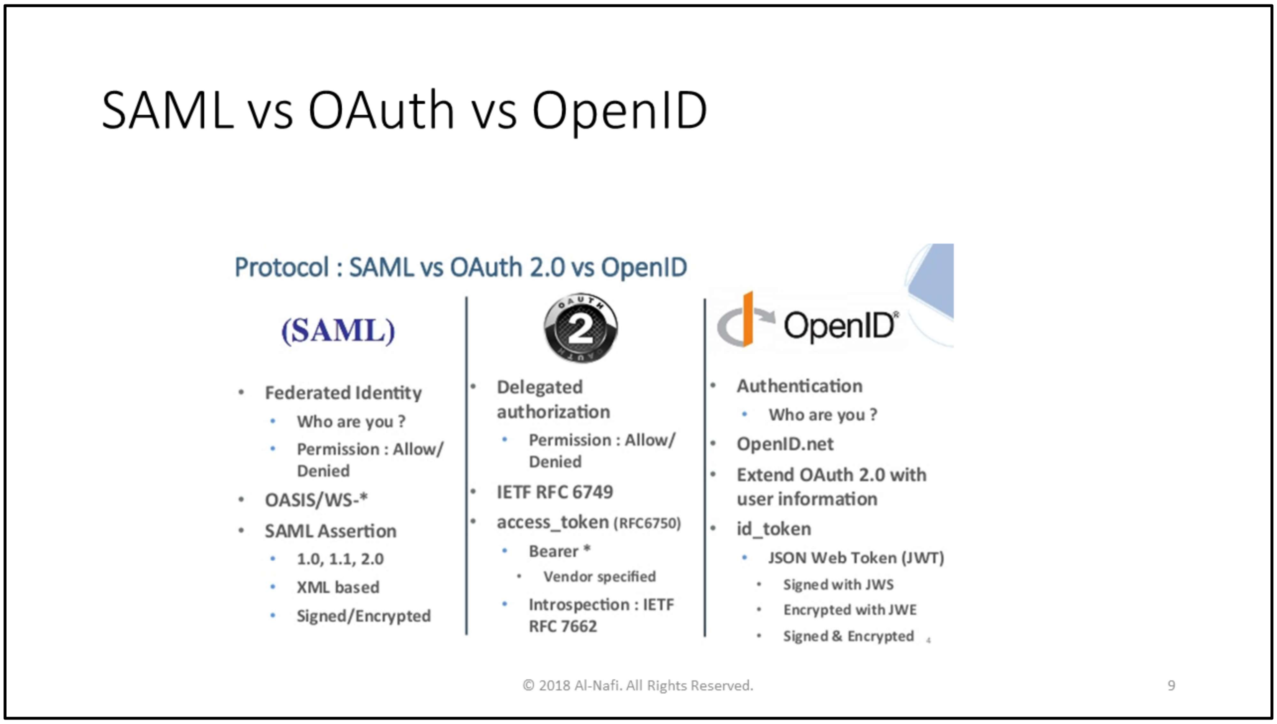
Service API
Resource Server

© 2018 Al-Nafi. All Rights Reserved.

8

Internet Engineering Task Force (IETF) rfc 6749 states: The Open Authorization (OAuth) 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

OAuth standard has four roles:
1. Resource owner: An entity capable of granting access to a protected resource. When the resource owner is a person, the entity is referred to as an end-user.
2. Resource server: The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
3. Client application: An application making protected resource requests on behalf of the resource owner and with its authorization. The term “client” does not imply any implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices).
4. Authorization server: The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.



SAML vs OAuth vs OpenID

Protocol : SAML vs OAuth 2.0 vs OpenID

(SAML)

- Federated Identity
  - Who are you ?
  - Permission : Allow/ Denied
- OASIS/WS-*
- SAML Assertion
  - 1.0, 1.1, 2.0
  - XML based
  - Signed/Encrypted

- Delegated authorization
  - Permission : Allow/ Denied
- IETF RFC 6749
- access_token (RFC6750)
  - Bearer *
    - Vendor specified
  - Introspection : IETF RFC 7662

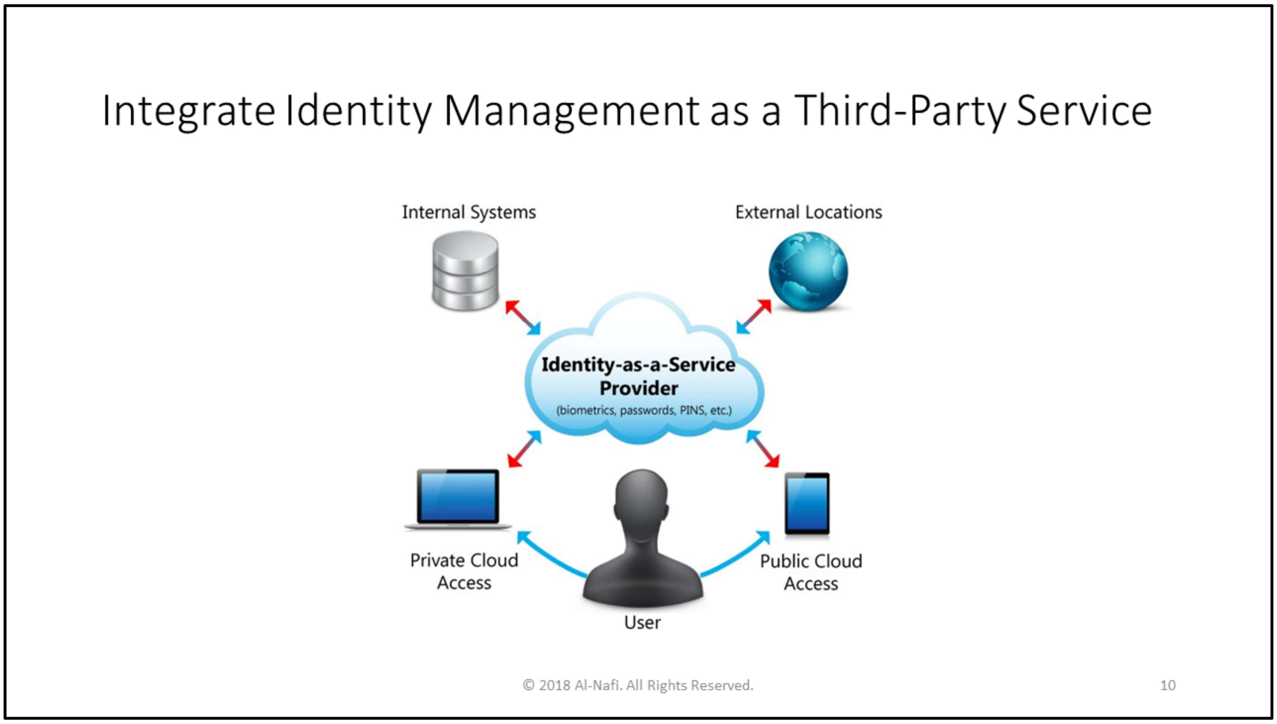
OpenID

- Authentication
  - Who are you ?
- OpenID.net
- Extend OAuth 2.0 with user information
- id_token
  - JSON Web Token (JWT)
    - Signed with JWS
    - Encrypted with JWE
    - Signed & Encrypted

Review this link https://developers.onelogin.com/saml

https://oauth.net/2/

https://openid.net/



Integrate Identity Management as a Third-Party Service

Gartner defines identity as a service (IDaaS) as, “a predominantly cloud-based service in a multi-tenant or dedicated and hosted delivery model that brokers core identity governance and administration (IGA), access and intelligence functions to target systems on customers’ premises and in the cloud.”

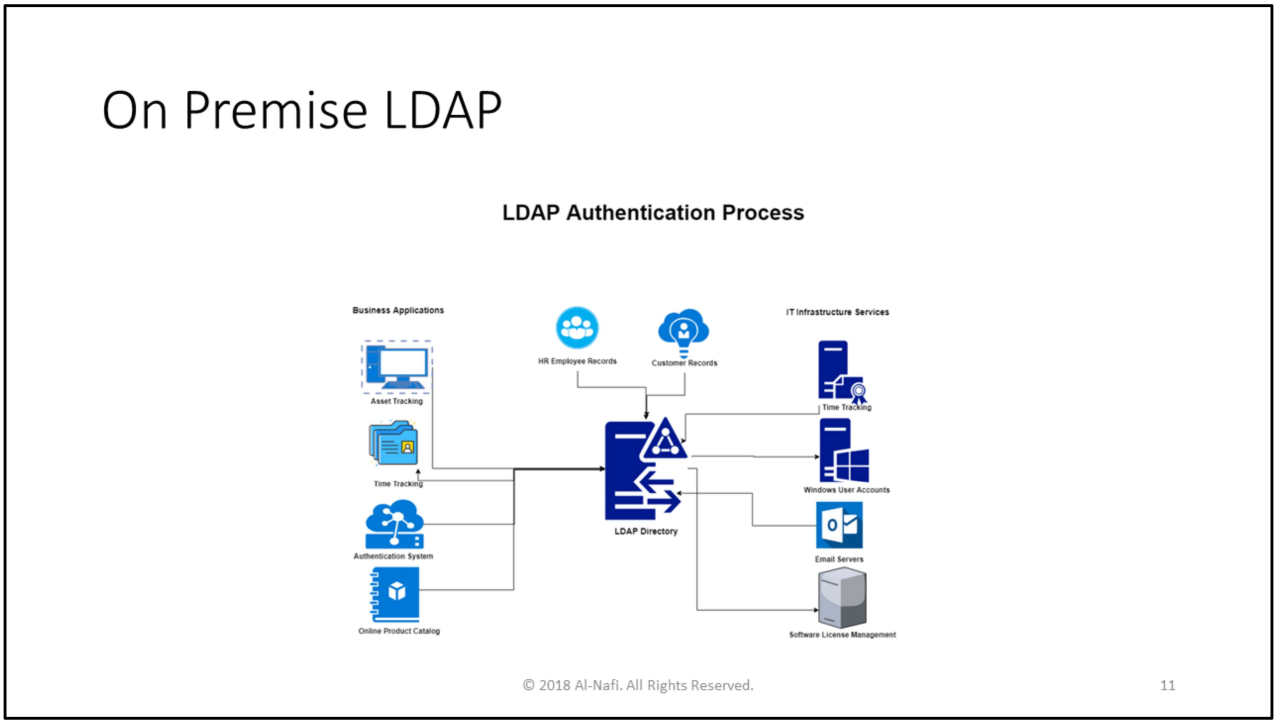
Gartner states that the core aspects of IDaaS are:

- IGA: Provisioning of users to cloud applications and password reset functionality.
- Access: User authentication, single sign-on (SSO), and authorization, supporting federation standards such as SAML.
- Intelligence: Identity access log monitoring and reporting.

The modern convergence of various business needs (that include ubiquitous access to services, reduced effort with sign-on, and greater support with federated standards) have driven adoption of IDaaS. These are some of the top performers in the IDaaS space that are part of Gardner’s Magic Quadrant:

- Centrify
- Okta

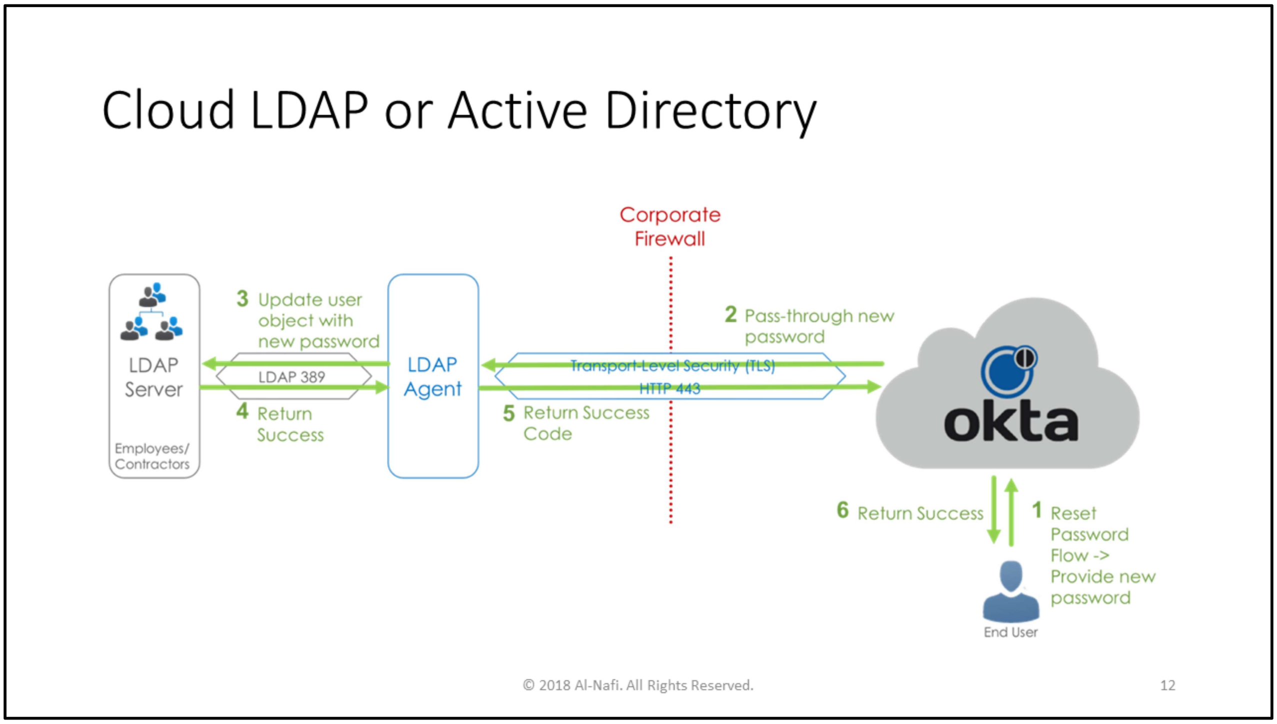
- Windows Active Directory Federated Services



On Premise LDAP

LDAP Authentication Process

On-premise organizations can use existing infrastructure that manages identities through LDAP services like Windows Active Directory to connect and login to a service provider that extends their internal identities to authenticate to consume services that are in the cloud. An example of extending internal services related to ID management to integrate with cloud services would be an enterprise Windows Active Directory connecting to Windows Azure (public cloud) AD to consume services related to Office 365. Office 365 represents a service that the enterprise is seeking to consume as software as a service (SaaS) that would be facilitated through linking an enterprise directory to a provider directory. While the service is provided externally, the passwords and IDs would be managed internal, thus on-premise.



Cloud LDAP or Active Directory

Corporate Firewall

LDAP Server

Employees/ Contractors

LDAP Agent

LDAP 389

Transport-Level Security (TLS)

HTTP 443

okta

End User

1 Reset Password Flow -> Provide new password

2 Pass-through new password

3 Update user object with new password

4 Return Success

5 Return Success Code

6 Return Success

If the previous scenario is managed by creating and storing the identities within an instance of Office 365 and Windows Active Directory in Windows Azure, then the third-party service is completely managed in the cloud.