OAUTH

March 25, 2014

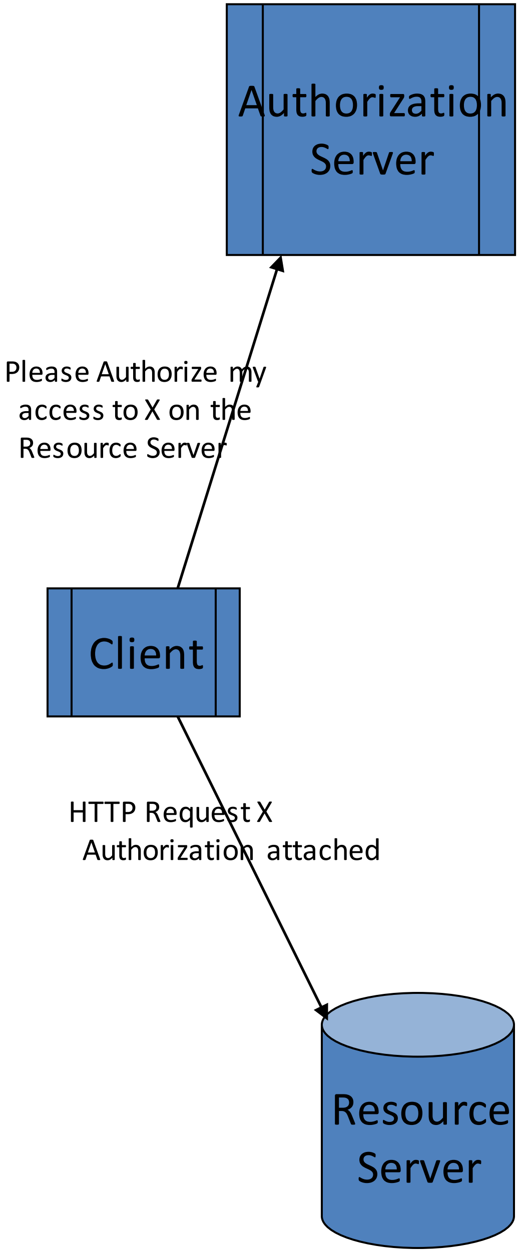
John Moehrke

OAuth 2.0 & OpenID Connect

- Used by many REST APIs and Internet web sites
- Authorization – OAuth
  - Application – that code needs to be authorized
  - Authorization service – aka Identity Provider (IDP)
  - Resource Server (RP) – aka Relying Party – needs protection
  - Very similar to Kerberos flow, some SAML patterns
- Authentication and Identity Management – OpenID Connect
  - Next generation beyond OpenID 2.0
  - Treats Identity as a protected RESTful resource
  - Leverages OAuth as authorizing access to identity
  - User controls what gets exposed to each app
  - RESTful service (API) - JSON encoded

OAuth

- REST web services include an AUTH header with signed token
  - can also be passed by parameter
- Secrets are issued to application (client) developers, trust framework
- Authorization service makes authorization decisions, passing results in tokens
  - identity, authentication, roles
  - Context: resource for which access is being requested
- Relying Parties checks ‘scope’ and signatures to assure trustable
- Relying Party ‘enforces’ authorization decision

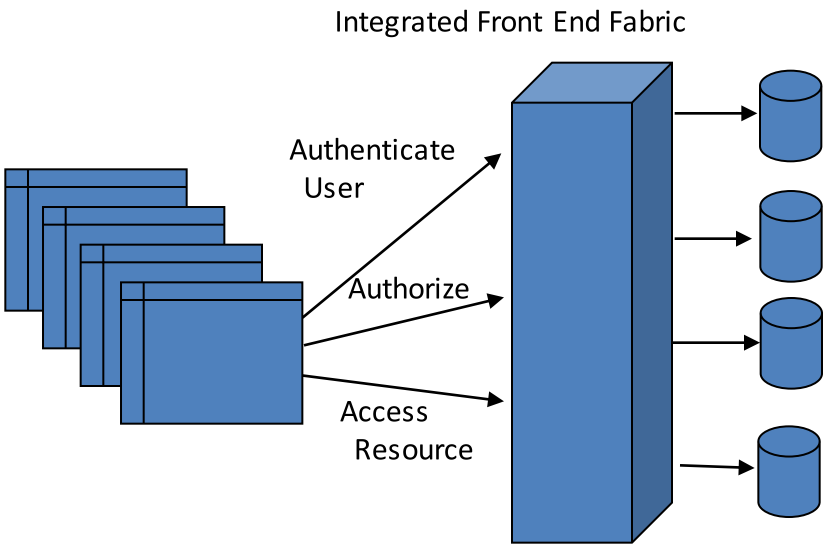

Authorization Server
Please Authorize my access to X on the Resource Server
Client
HTTP Request X Authorization attached
Resource Server

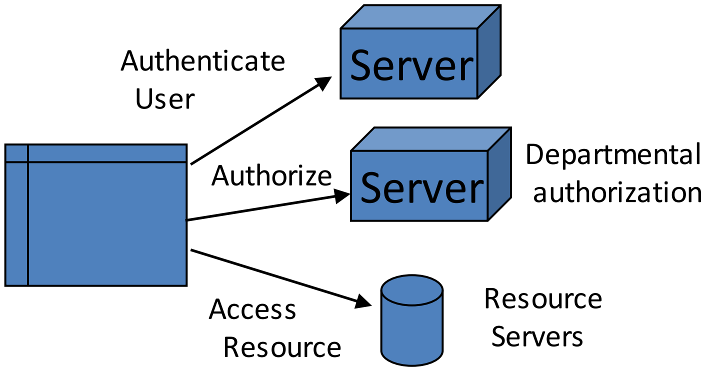
OAuth flow

- Access Token – Long-lived token, issued to an application once the user indicates they trust it.
    - Only used in conversation between Application and IDP
    - User involved in authorization decision
    - Usually Time limited, but large time
    - May be revoked by User actions
- Request Token – Short-lived token, issued for specific scope and timeframe. This is the one used on all requests to the Resource Service (RP)
    - This is the Authorization Decision

Internet User Authorization (IUA)

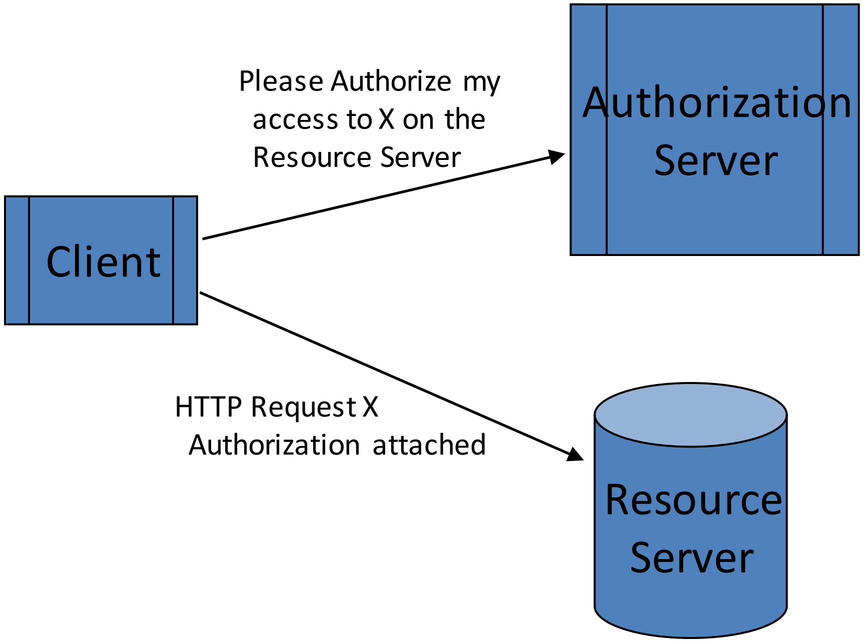
- Most Internet facing services integrate the user authentication, authorization, load sharing, and access control into a front end system (google, facebook).
- Internal enterprise systems can split authorization, authentication and access control services.
  - Authentication is handled by HR
  - Authorization is handled by the operational department.
- Both modes of operation use OAuth for authorization.
- IUA works in both of these environments.





Internet User Authorization (IUA)

- Profiles OAuth 2.0, the current leading Internet authorization framework
- Needed Most when Resource Server needs to make 'more' or 'their own' access control decisions
- Pass attributes via JWT
- Authorization token can optionally be the SAML assertion defined as part of the XUA profile.
- Fundamental to access control, privacy, and security


Please Authorize my access to X on the Resource Server
Authorization Server
Client
HTTP Request X Authorization attached
Resource Server

Integrating the Healthcare Enterprise

IUA token

- Native JWT attributes

Parameter	Req	Definition	RFC Reference
iss	R	Issuer of token	Draft json-web-token Section 4
sub	R	Subject of token (e.g., user)	Draft json-web-token Section 4
aud	R	Audience of token	Draft json-web-token Section 4
exp	R	Expiration time	Draft json-web-token Section 4
nbf	O	Not before time	Draft json-web-token Section 4
iat	O	Issued at time	Draft json-web-token Section 4
typ	O	Type	Draft json-web-token Section 4
jti	R	JWT ID	Draft json-web-token Section 4

-

XUA Attribute	XUA Definition	JWT Parameter
SubjectID	Plain text user's name	SubjectID
SubjectOrganization	Plain text description of the Organization	SubjectOrganization
SubjectOrganizationID		SubjectOrganizationID
HomeCommunityID	Home Community ID where request originated	HomeCommunityID
NationalProviderIdentifier		NationalProviderIdentifier
Subject:Role		SubjectRole
docid	Patient Privacy Policy Acknowledgement Document ID	docid
acp	Patient Privacy Policy Identifier	acp
PurposeOfUse	Purpose of Use for the request	PurposeOfUse
Resource-ID	Patient ID related to the Patient Privacy Policy Identifier	resourceID
	Patient ID, Citizen ID, or other similar public ID used for health identification purposes.	personID