SWAMID OIDC
VARFÖR ?

Roland Hedberg @ SUNETdagarna 2017

AGENDA

- OIDC intro
- OIDC vs SAML2
- OIDC federation
- Native apps
- Device flow

OIDC INTRO

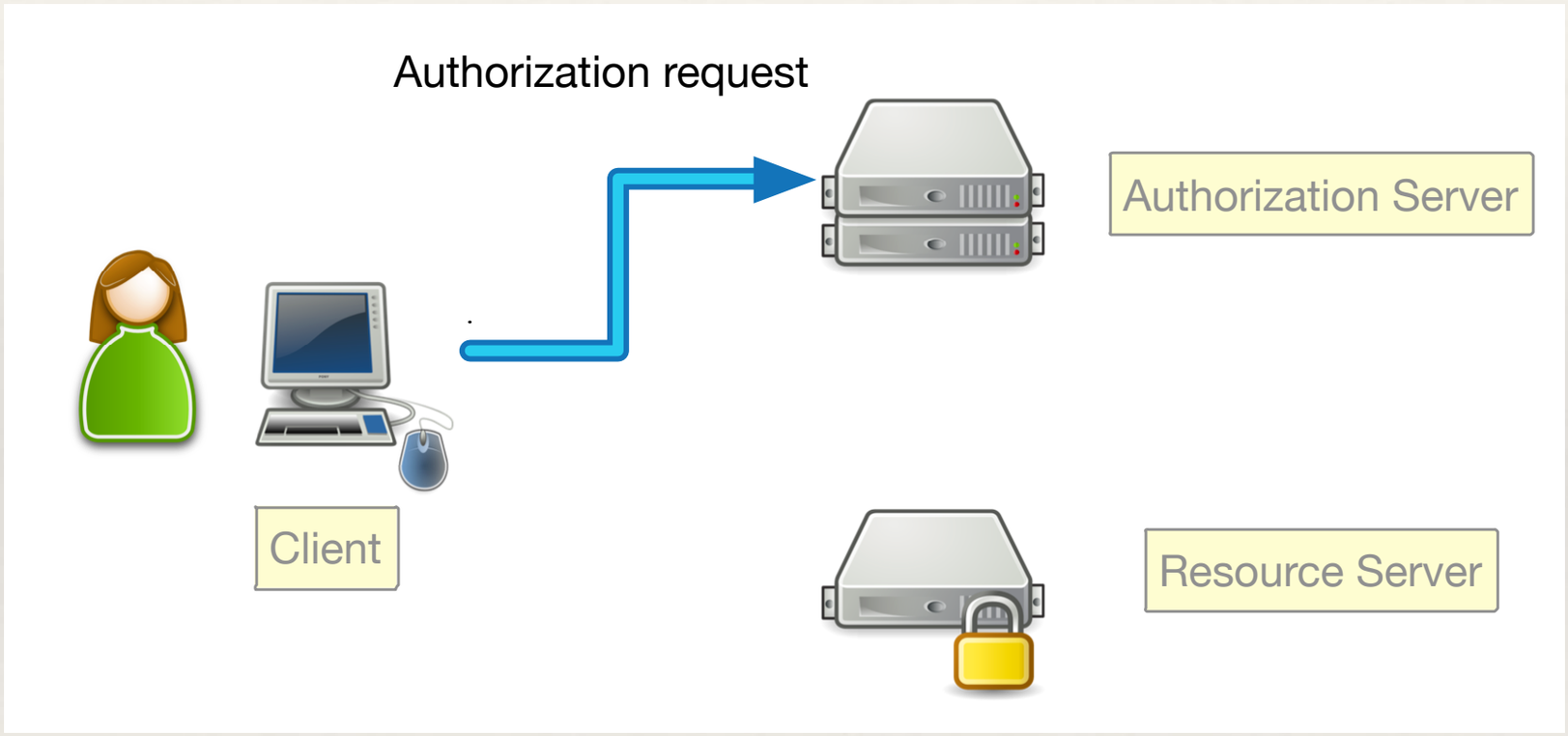
- OpenID Connect
  - Core
  - Discovery
  - Dynamic registration
- owned by OpenID Foundation
- based on OAuth2 RFC6749/6750

Differences

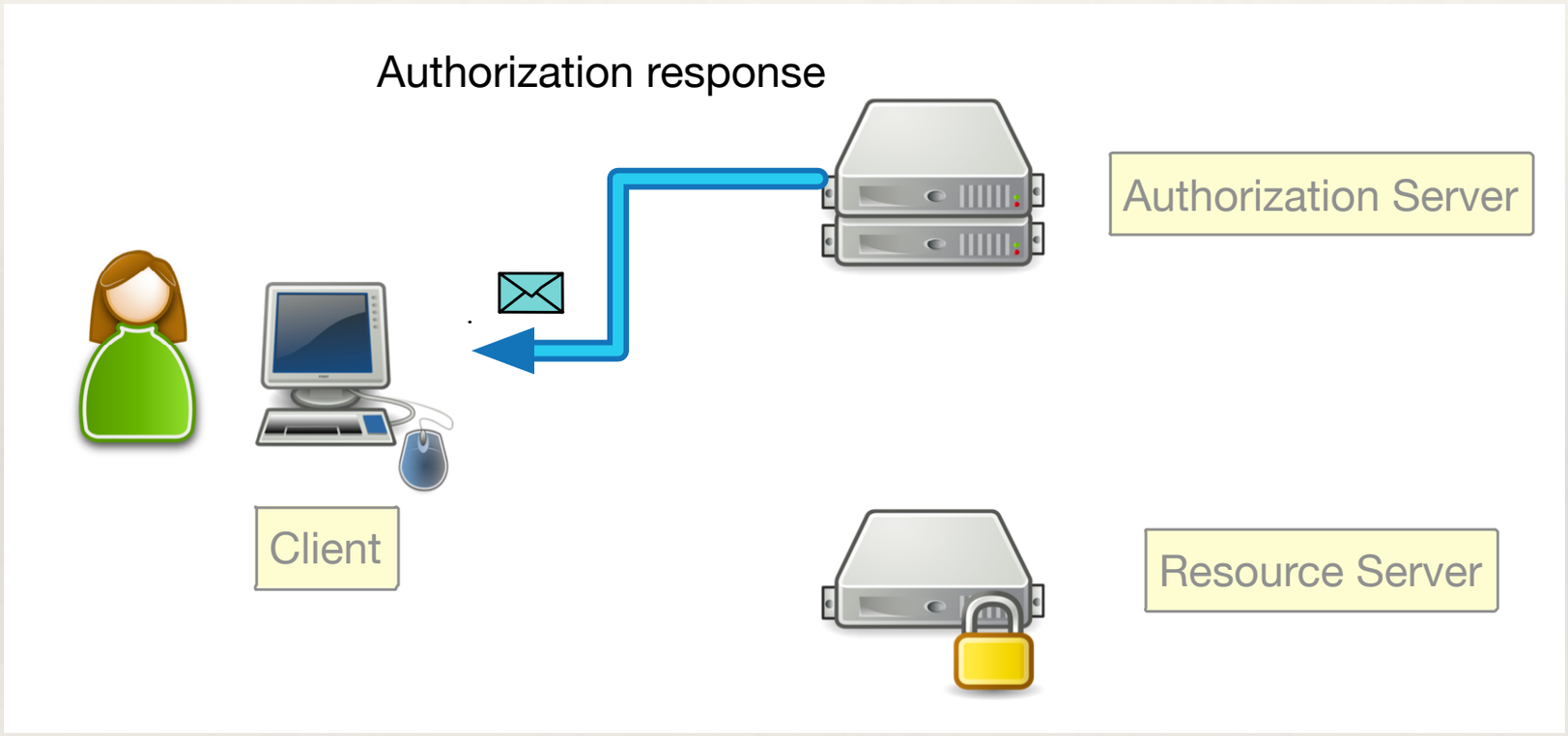
OpenID Connect	SAML2
User centric	Organisations centric
JSON	XML
JWT/JWS/JWE/JWK	XMLSEC
HTTPS GET/POST	HTTPS GET/POST, SOAP, POAS
Dynamic	’Static’
Minimalistic	Extensible

LIKHETER ?

Authorization Request



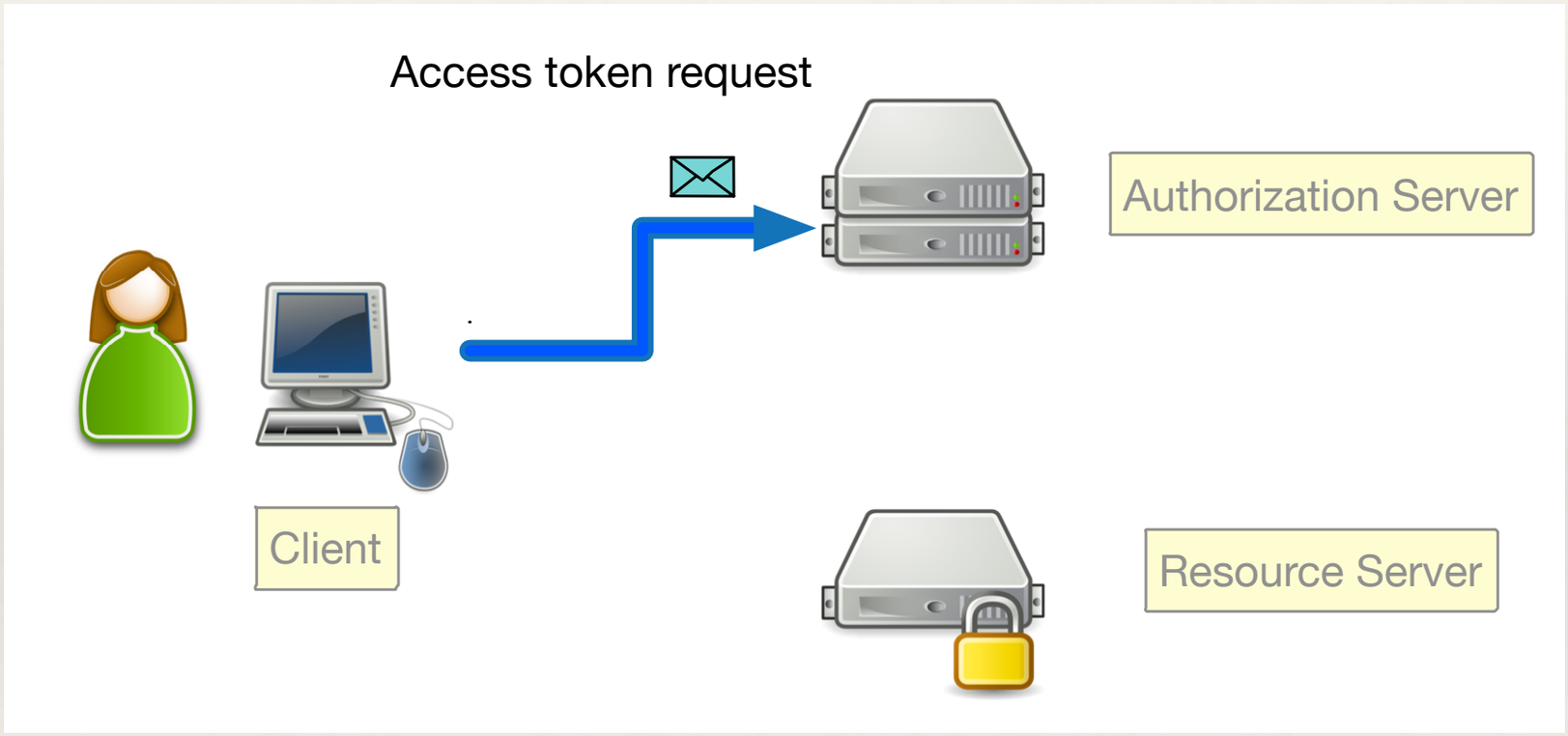
Authorization Response



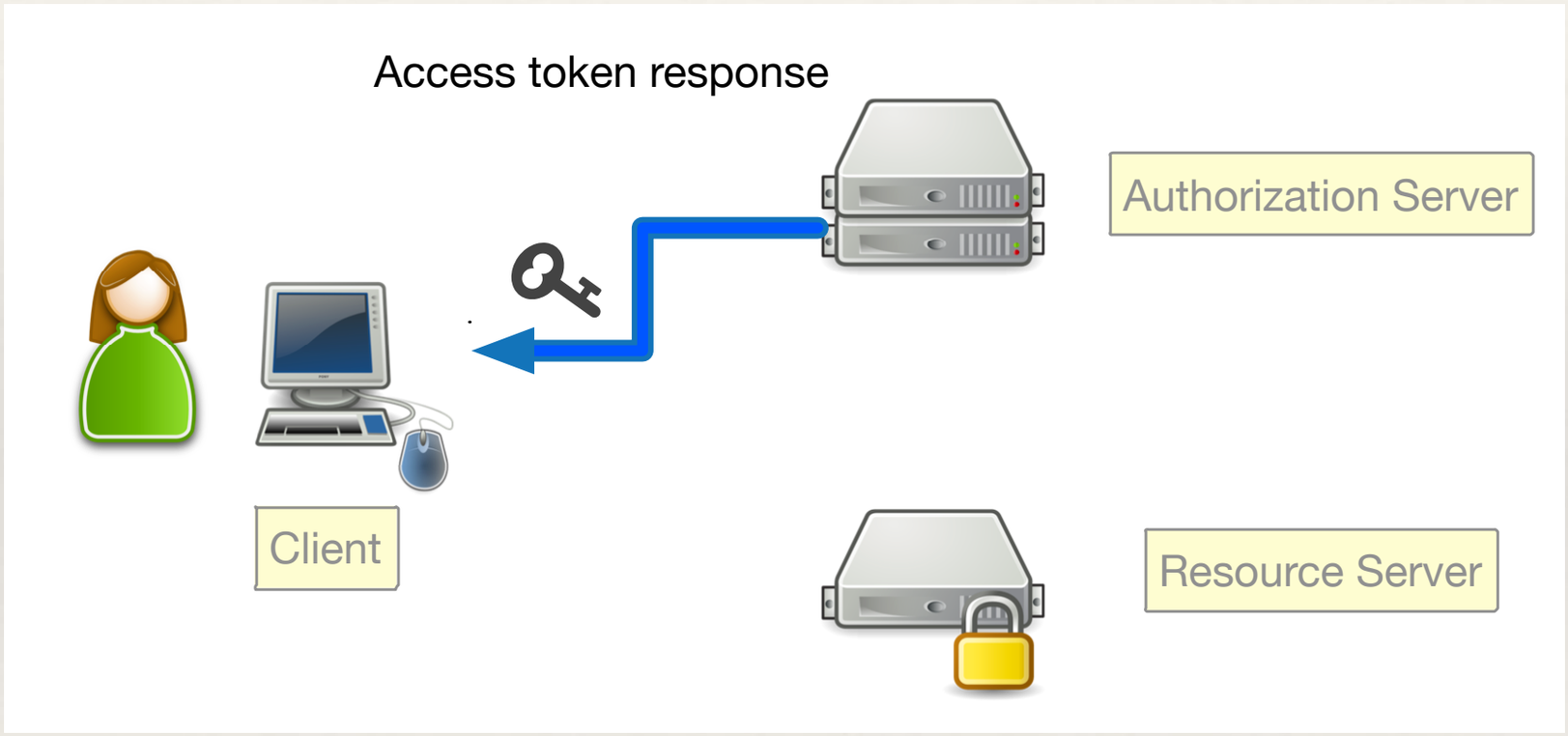
AUTHORIZATION RESPONSE

- SAML
  - Assertion
    - issuer, signature. subject, condition, statement, authnStatement, attributeStatement, ..
- OIDC
  - code (+ token) (+ id_token)

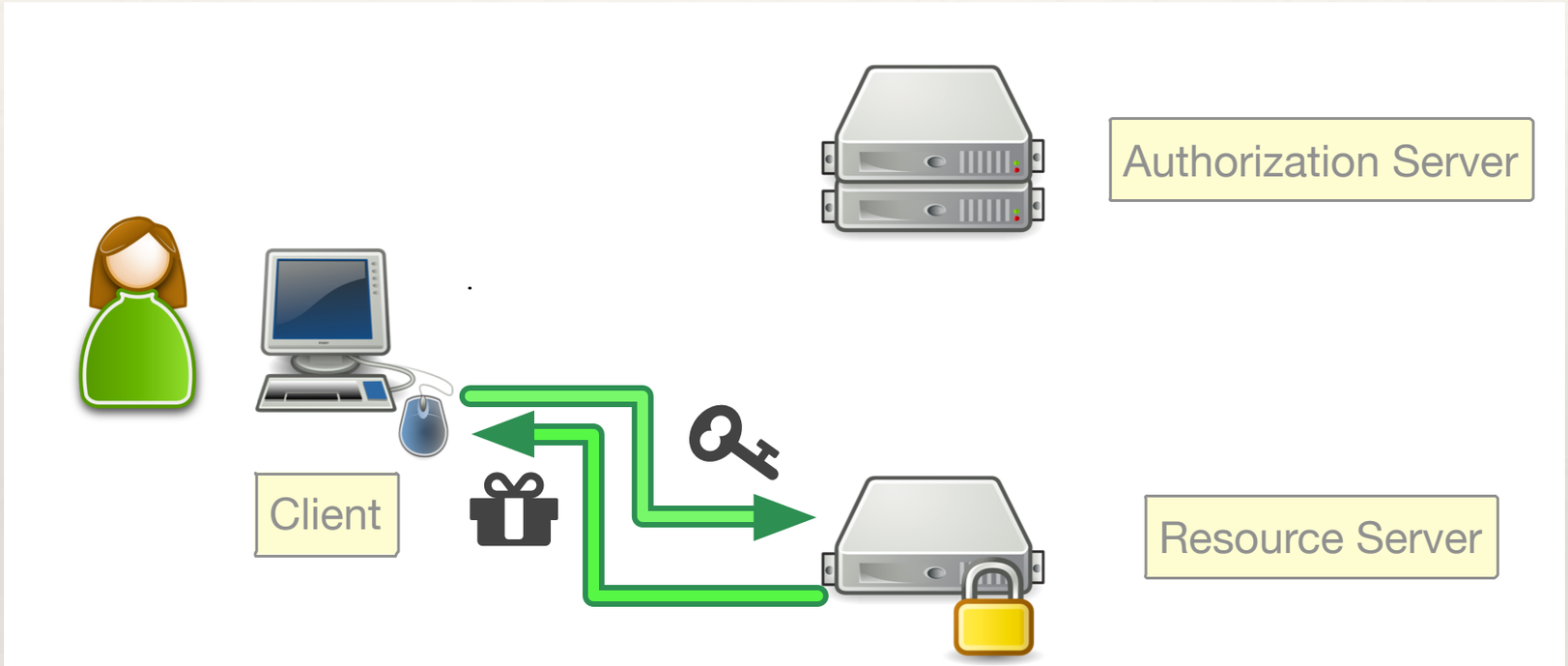
Access Token Request



Access Token Response



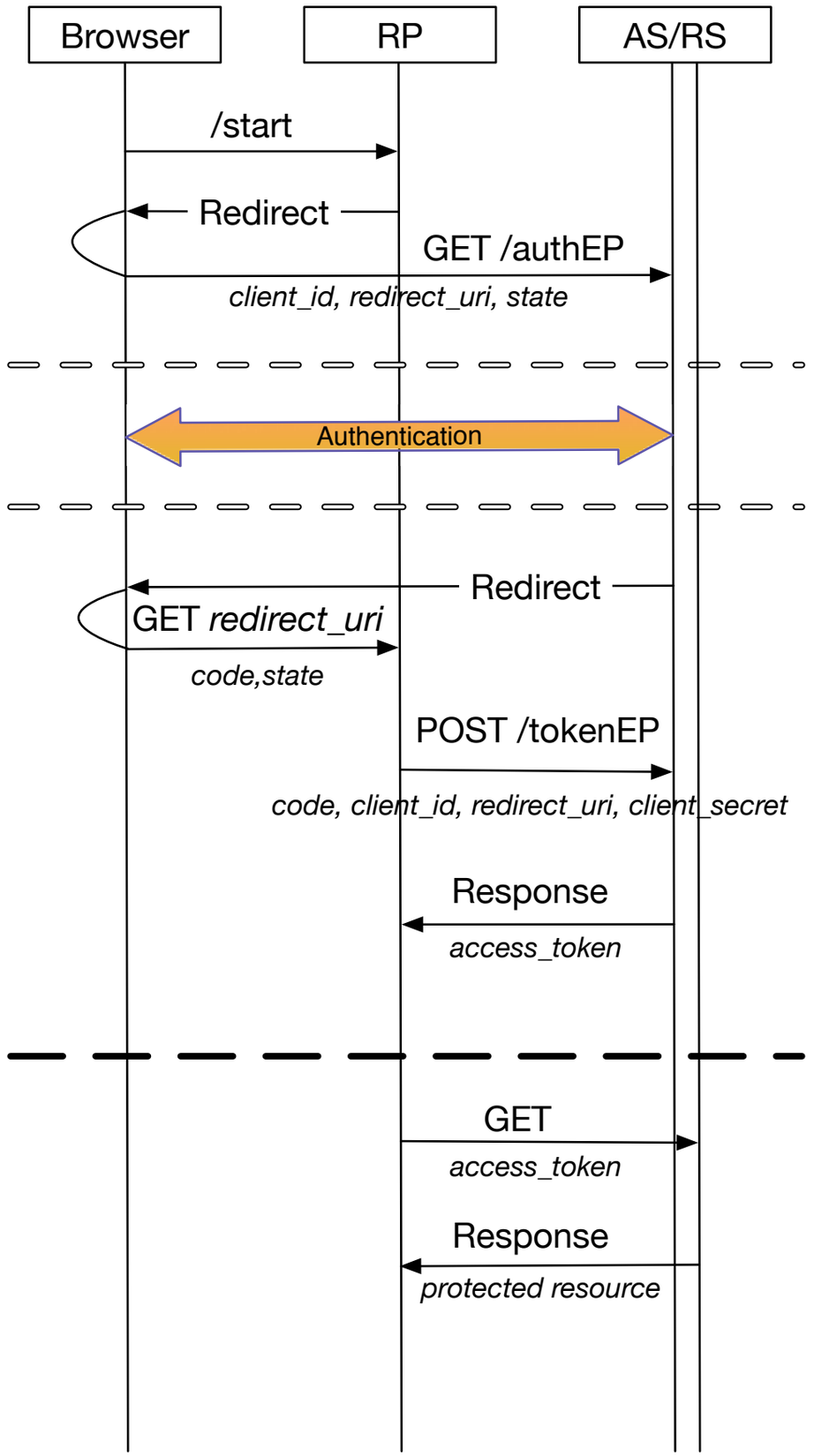
Resource Access



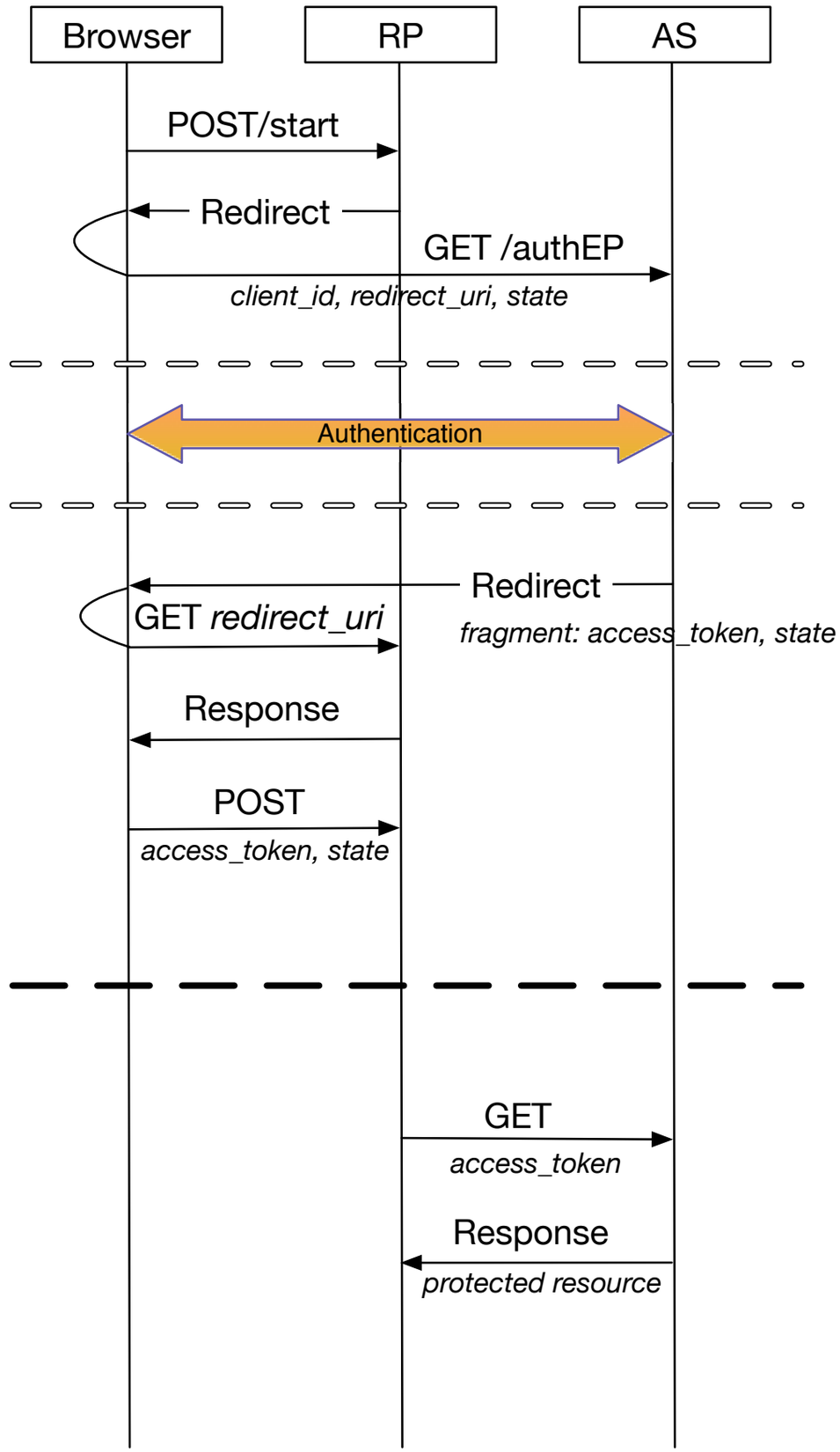
Resource request/response

ALLA ÄR INTE SKAPADE LIKA

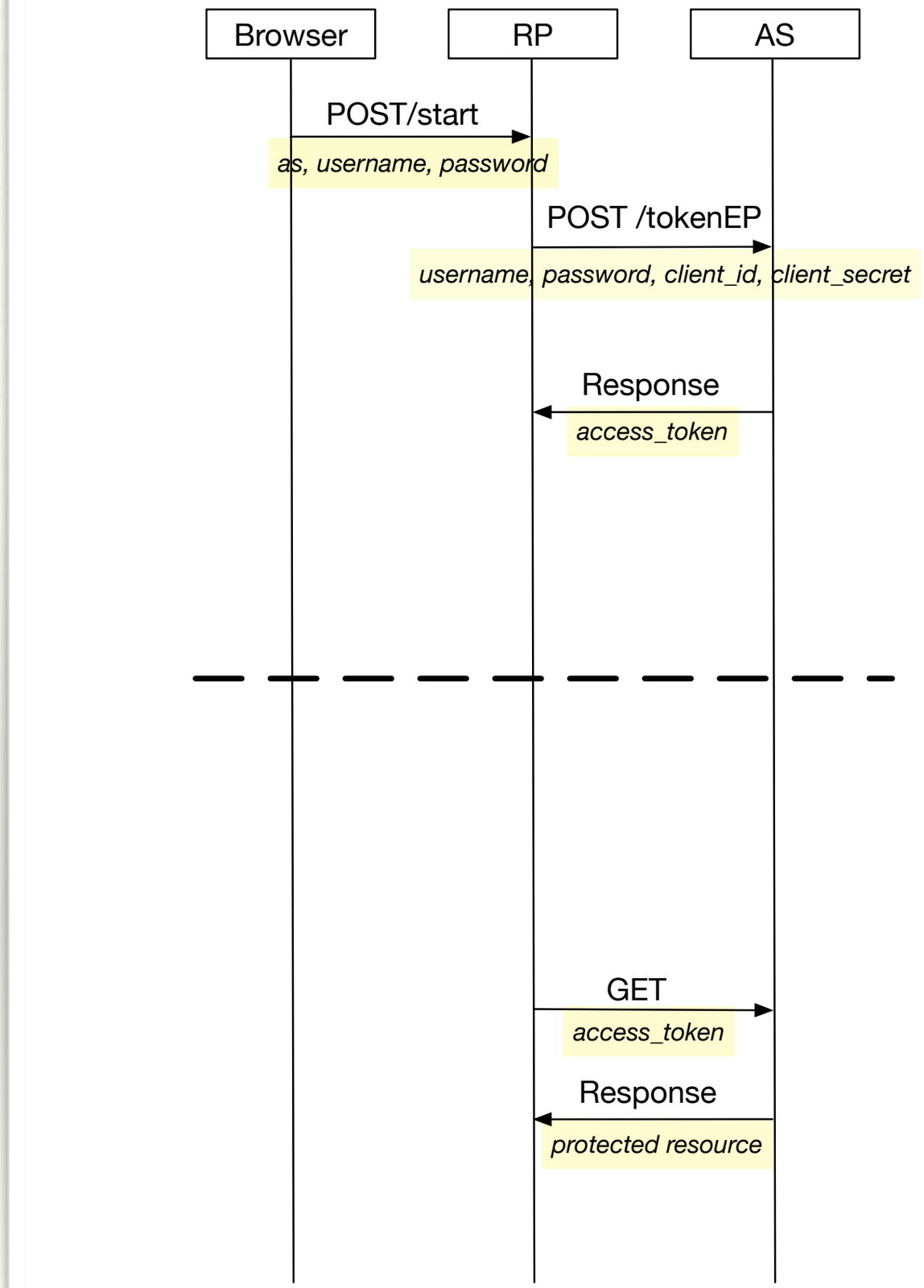
Code


Browser
RP
AS/RS
/start
Redirect
GET /authEP
client_id, redirect_uri, state
Authentication
Redirect
GET redirect_uri
code,state
POST /tokenEP
code, client_id, redirect_uri, client_secret
Response
access_token
GET
access_token
Response
protected resource

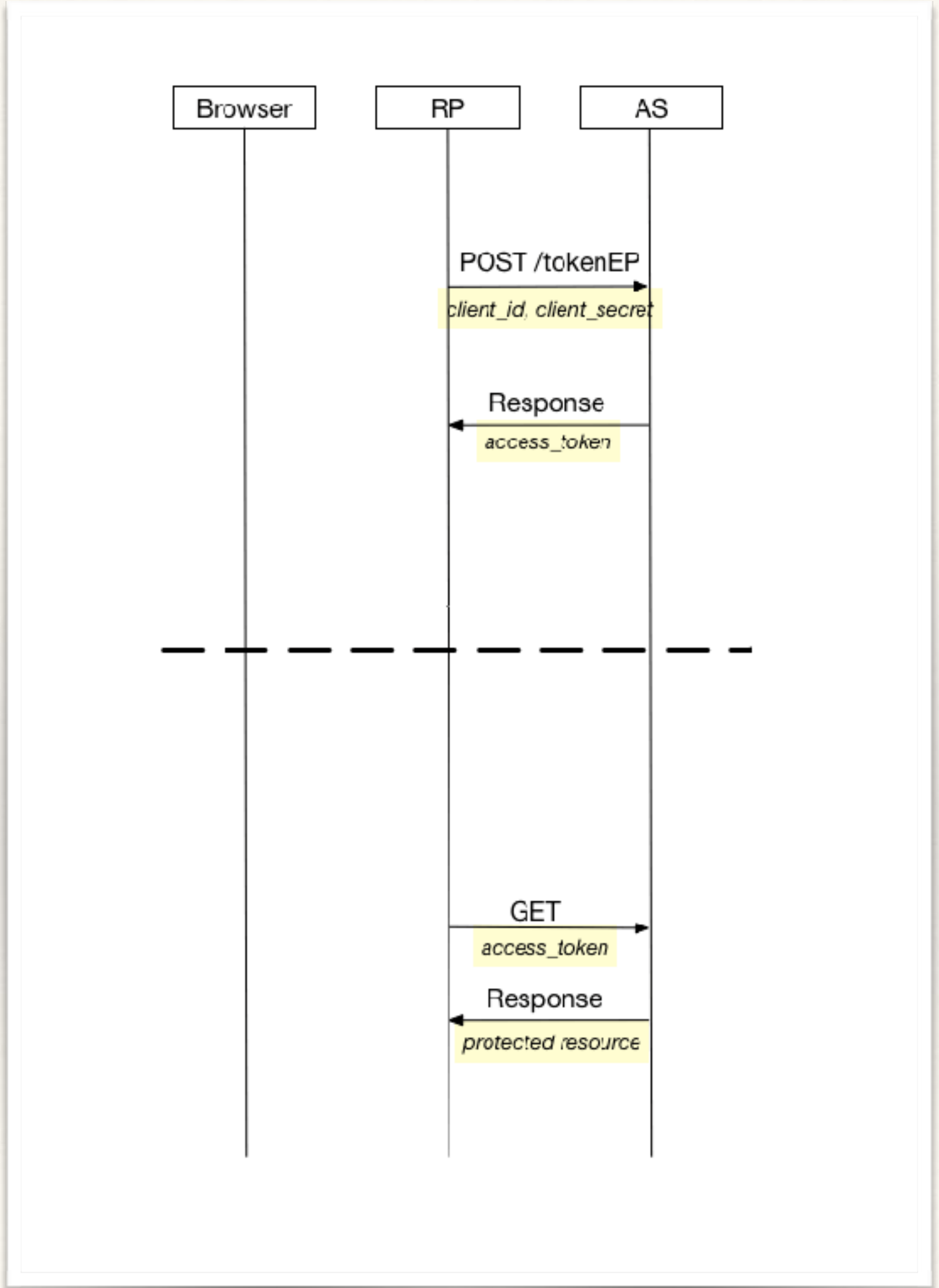
Token


Browser
RP
AS
POST/start
Redirect
GET /authEP
client_id, redirect_uri, state
Authentication
Redirect
GET redirect_uri
fragment: access_token, state
Response
POST
access_token, state
GET
access_token
Response
protected resource

Resource Owner Password Credentials



Client Credentials



OIDC TILLÄGG

Discover provider info - query

```
GET /.well-known/openid-configuration HTTP/1.1
Host: openid.example.com
```

Client registration

- uris
- application information
- support for signing/encrypting algorithms
- key material
- server behaviour
- client behaviour

ID Token

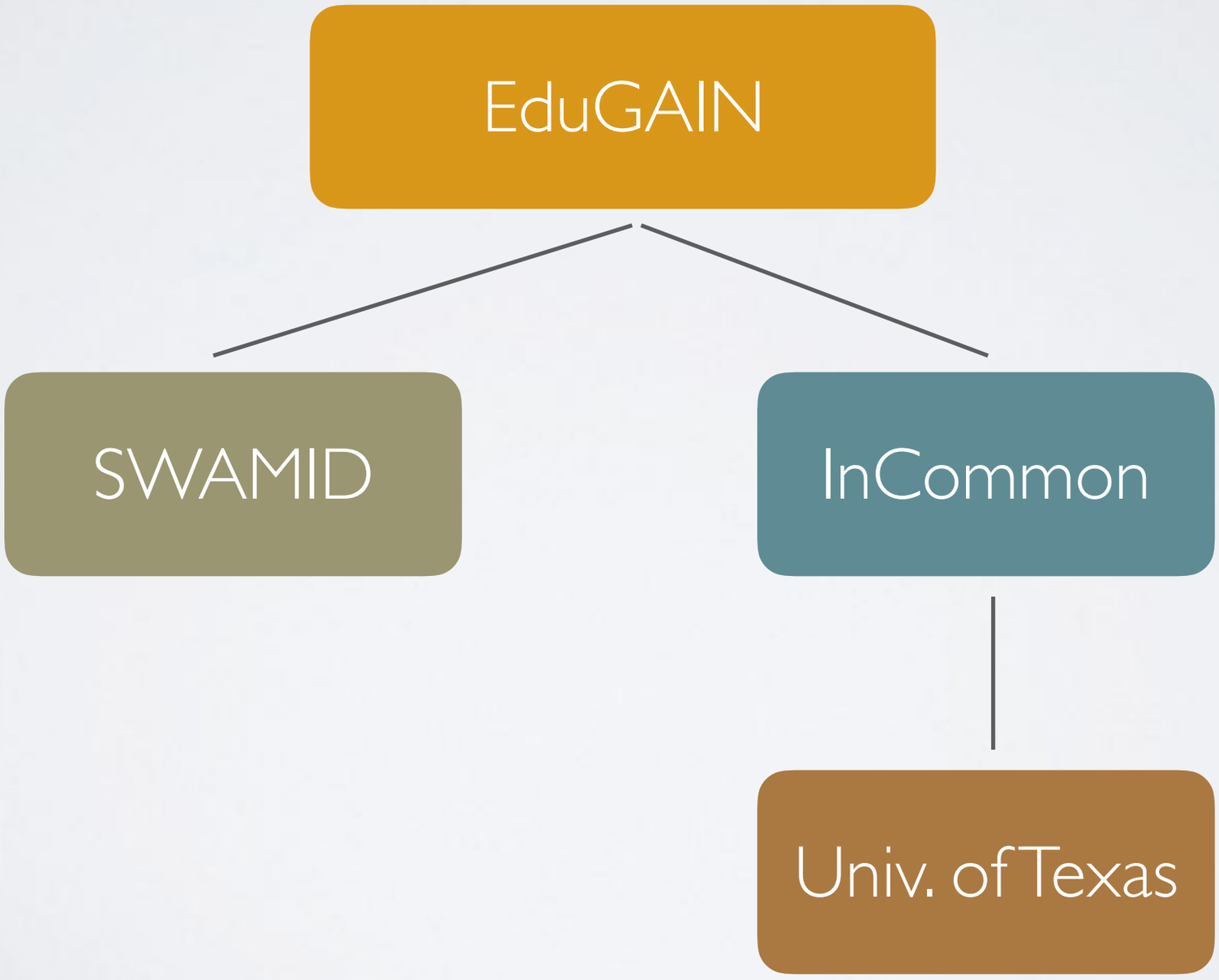
- a security token that contains Claims about the **Authentication** of an End-User by an Authorisation Server when using a Client, and potentially other requested Claims.
- is represented as a JSON Web Token (JWT)

OPENID FOUNDATION ARBETSGRUPPER

- Account chooser
- Enhanced Authentication Profile
- Financial API
- International Government Assurance Profile
- Mobile Operator Discovery, Registration & autheNticAtion (MODRNA)
- Risk and Incident Sharing and Coordination

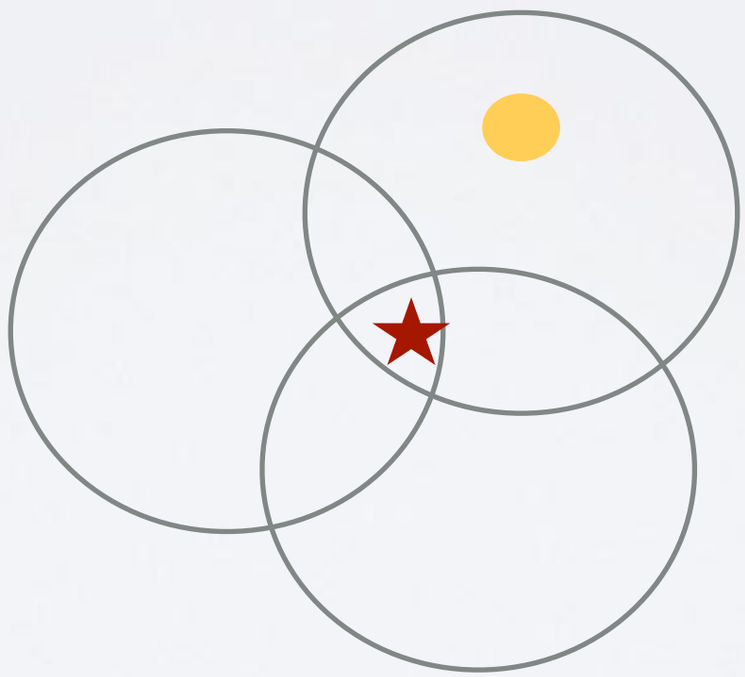
IDENTITETSFEDERATIONER

SAML2 FEDERATIONER



OIDC FEDERATION

- On demand !



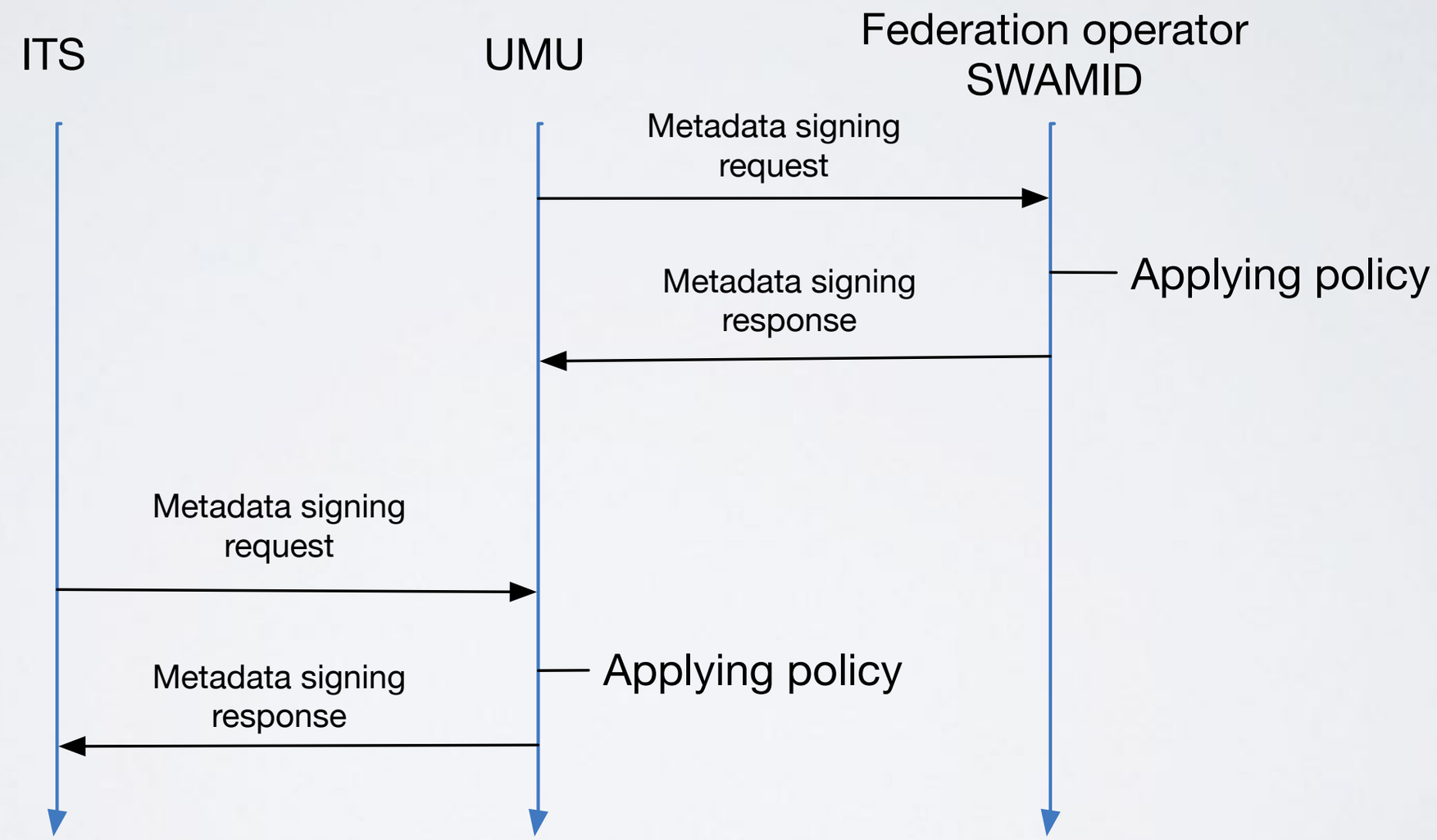
OIDC IDENTITY FEDERATION

- Allow dynamic discovery and registration without losing trust.
- Enforcement of federation and organisation policies
- Allow delegation of entity registration
- Metadata transport and origin independent
- Metadata Self-contained

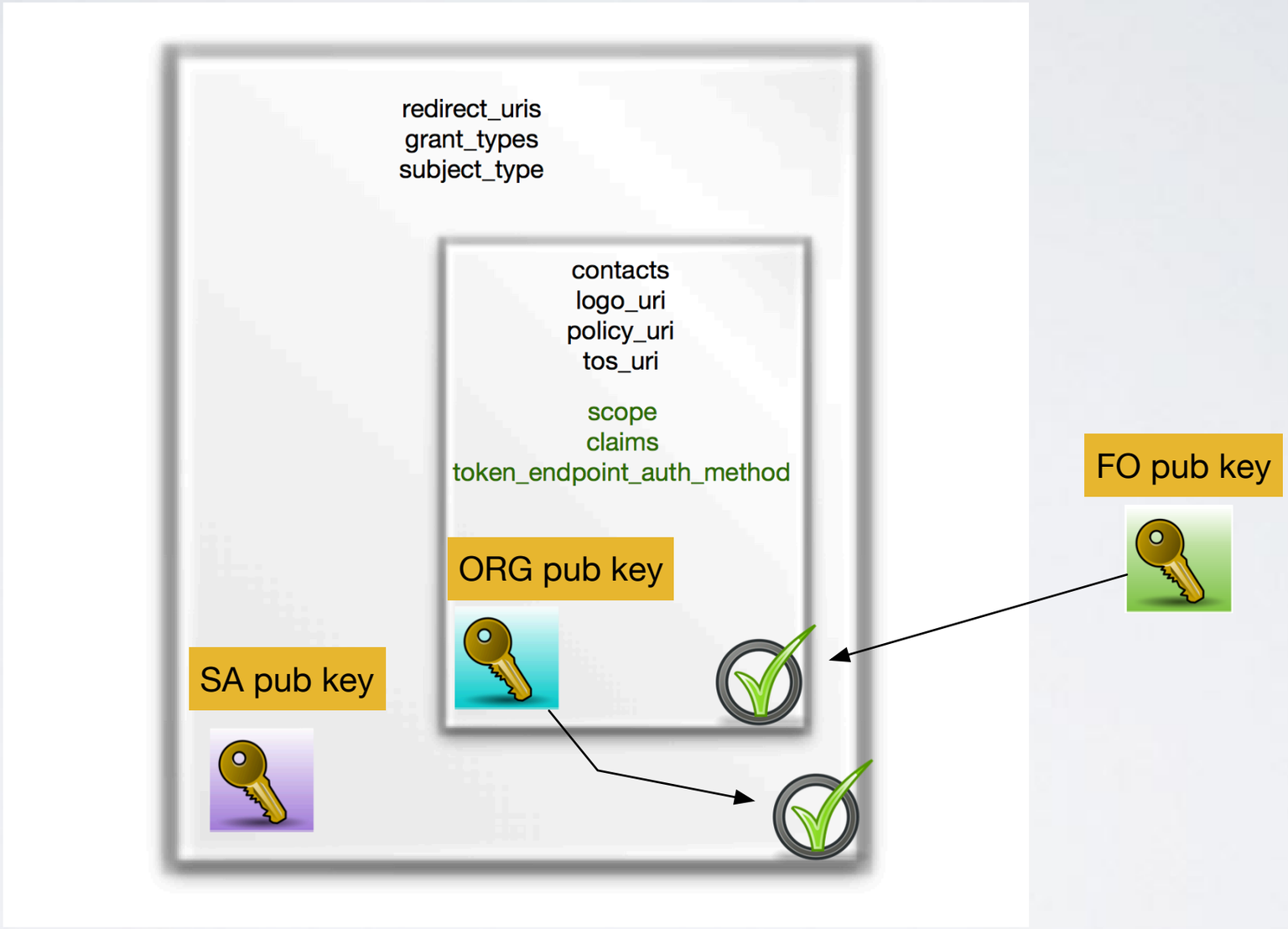
CHAIN OF TRUST

- Trusted 3rd party
- Chain of verifiable claims
- Metadata construction

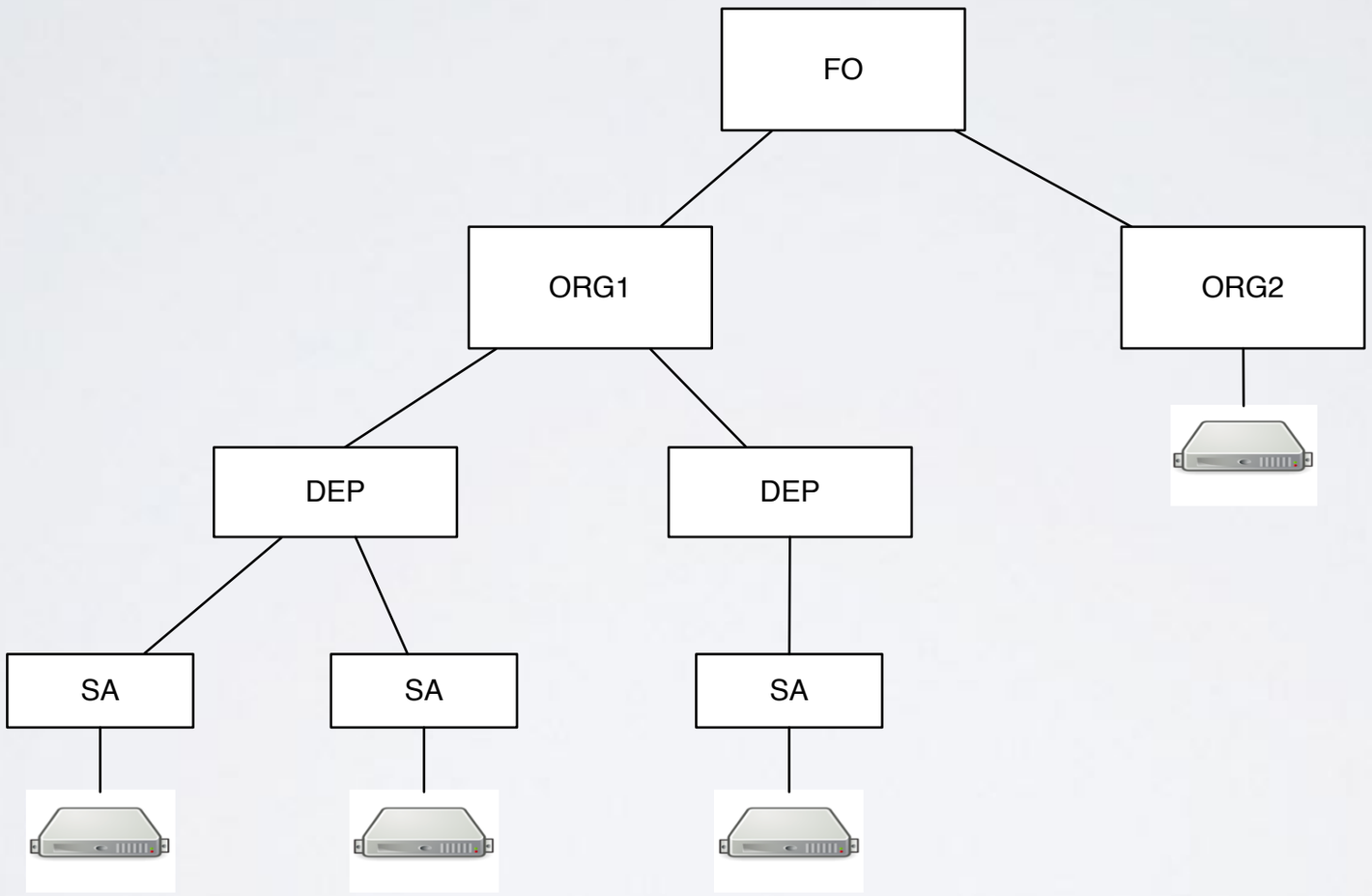
METADATA SIGNING SEQUENCE



METADATA STATEMENT



FEDERATION 'DEPTH'

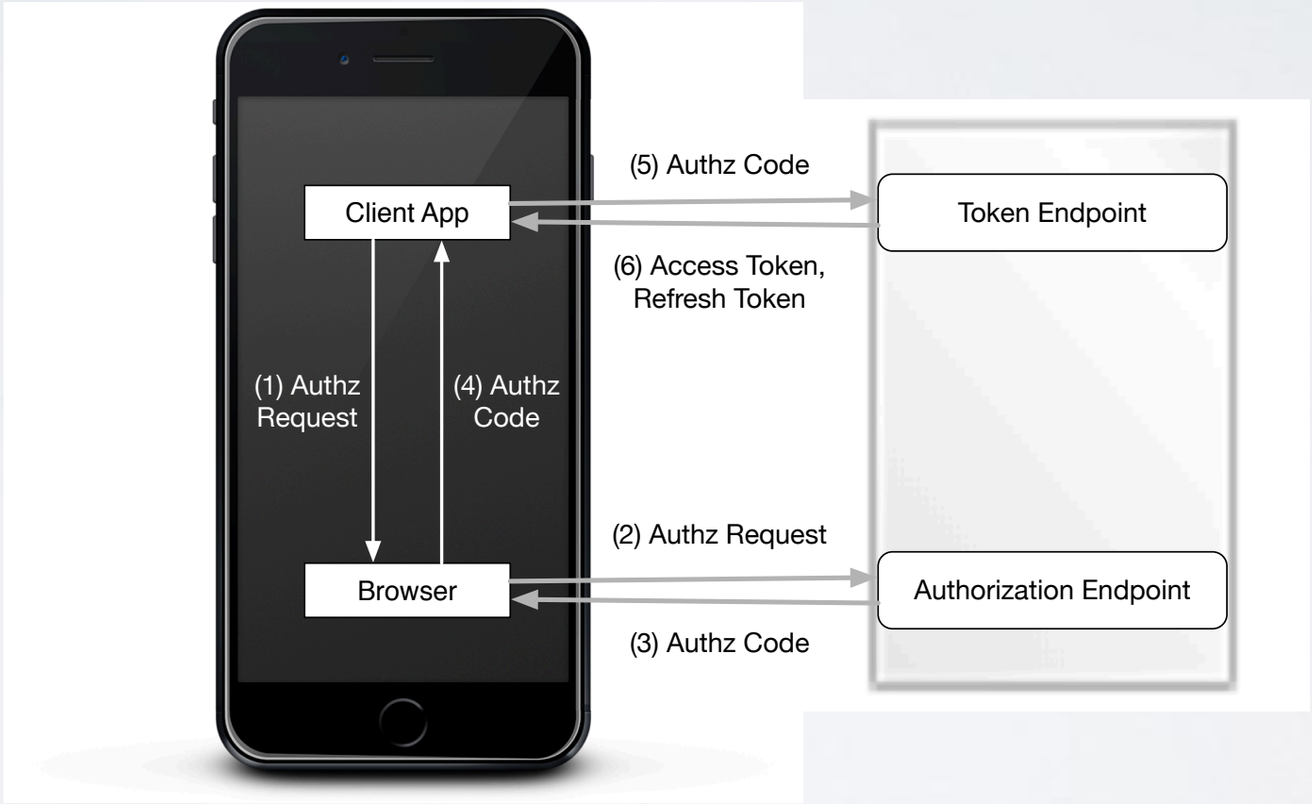


NATIVE APPS - APPAUTH

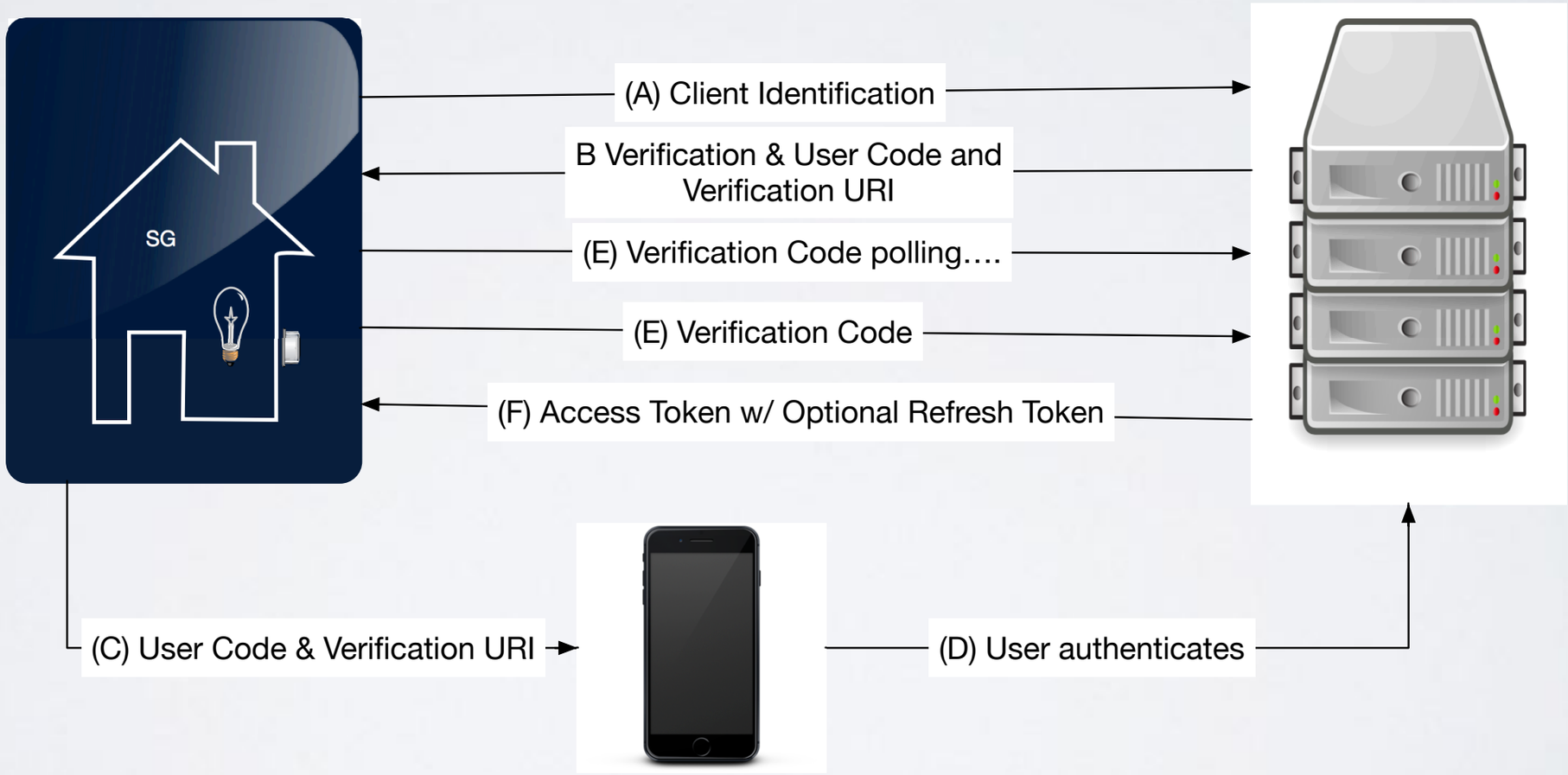
- An application that is installed by the user to their device, as distinct from a web app that runs in the browser context only.

- https://tools.ietf.org/id/draft-ietf-oauth-native-apps-09.html

AUTHORISATION FLOW
FOR NATIVE APPS USING THE BROWSER



DEVICE FLOW


SG
(A) Client Identification
B Verification & User Code and Verification URI
(E) Verification Code polling….
(E) Verification Code
(F) Access Token w/ Optional Refresh Token
(C) User Code & Verification URI
(D) User authenticates

CERTIFIERING

Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP
Auth0	Auth0	24-May-2016	15-Feb-2017	15-Feb-2017	24-May-2016	
Dominick Baier & Brock Allen	IdentityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015	
Dominick Baier & Brock Allen	IdentityServer4	12-Dec-2016	12-Dec-2016	12-Dec-2016	12-Dec-2016	
Clareity Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016	
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015	
Connect2id	Connect2id Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017
CZ.NIC	mojeID	7-Jul-2016		31-Jul-2016	7-Jul-2016	7-Jul-2016
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015	
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015	
Google	Google Federated Identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015	
Thierry Habart	SimpleIdentityServer V1.0.0	9-Dec-2015			11-Dec-2015	
Thierry Habart	SimpleIdentityServer V2.0.0	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
Roland Hedberg	pyoidc 0.7.7	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015
Cal Heldenbrand	Spark Platform	2-Oct-2015	2-Oct-2015	2-Oct-2015	5-Oct-2015	
KSIGN	KSign Access 4.0	17-Mar-2017				
Microsoft	ADFS on Windows Server 2016	13-Sep-2015	13-Sep-2015		7-Apr-2015	
Microsoft	Azure Active Directory				8-Apr-2015	
NEC	NC7000-3A-OC	7-Mar-2016				
Nomura Research Institute	phpOIDC	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015
Nomura Research Institute	Uni-ID	10-Apr-2015				
NTT Software Corporation	TrustBind/Federation Manager	26-Jan-2017	26-Jan-2017	26-Jan-2017		
PayPal	Login with PayPal				15-Apr-2015	
OGIS-RI	ThemiStruct Identity Platform v1.1.0	7-Oct-2016	7-Oct-2016		7-Oct-2016	
Okta	Okta OP	25-May-2016	26-May-2016	26-May-2016	26-May-2016	
Peercraft ApS	Peercraft	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
Ping Identity	PingFederate	10-Apr-2015	10-Apr-2015	10-Apr-2015	9-Apr-2015	
Privacy Vaults Online (PRIVO)	PRIVO-Lock	23-Oct-2015			25-Nov-2015	
Red Hat	Keycloak 2.3.0	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016
Justin Richer	MITREidConnect	13-May-2015			13-May-2015	13-May-2015
Salesforce	Summer 2015 Release				14-May-2015	
Michael Schwartz	Gluu Server 2.3	2-Jul-2015	2-Jul-2015	8-Jul-2015	2-Jul-2015	2-Jul-2015
SecureAuth	SecureAuth IdP 8.2	25-Feb-2016	25-Feb-2016	25-Feb-2016	7-Mar-2016	
Filip Skokan	node oidc-provider	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017
Symantec	NSL 2016.4.0.16	13-Oct-2016			13-Oct-2016	
University of Chicago	OIDC OP Overlay for Shibboleth IdP v3.2.1 version 1.0	25-Feb-2016			25-Feb-2016	
Verizon	VZConnect 1.9	21-Dec-2016				
ViewDS	Cobalt V1.0	28-Jan-2016	2-Feb-2016		28-Jan-2016	
Matias Woloski	Auth0	6-Feb-2016			8-Feb-2016	
Yahoo! Japan	Yahoo! ID Federation v2	7-Dec-2016	7-Dec-2016	7-Dec-2016	7-Dec-2016	

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic RP
Brock Allen	oidc-client-js 1.3		4-Feb-2017		7-Feb-2017	
Dominick Baier	IdentityModel.OidcClient 2.0	27-Jan-2017			6-Feb-2017	
Thierry Habart	SimpleIdentityServer V1.0.1	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017
Janrain	IDPD 2.6.0	7-Feb-2017				
Roland Hedberg	pyoidc 0.9.4	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016
Karlsruher Institut für Technologie, SCC	oidcc 1.0.1	2-Feb-2017			2-Feb-2017	
Nomura Research Institute	phpOIDC 2016 Winter	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017
Nov Matake	openid_connect rubygem v1.0.3	20-Jan-2017				
Ping Identity	PingAccess 4.2.2	26-Jan-2017				
Ping Identity	PingFederate 8.3.1	17-Jan-2017			31-Jan-2017	
Filip Skokan	node openid-client ^1.3.0	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016
Hans Zandbelt	mod_auth_openidc 2.1.2	13-Dec-2016			13-Dec-2016	13-Dec-2016

SAMMANFATTNING

- OIDC kan göra samma som SAML men också mycket, mycket mer

- Vi börjar få grepp om hur man bygger identitetsfederationer med OIDC.

- OAuth2 för mobila enheter finns ! (OIDC snart)

- Genom certifiering en bättre chans att det fungerar.


Frågor ?

Frågor ?