# Batch app needs to call an API

1. Register the client and get client id & secret (assumes API already registered)
2. POST request to token ep with client & secret, returns an access token

# MT Web App serving html calling an API

1. Register app with STS, mark as MT
2. Get signing keys from STS .well-known
3. Receive a request from browser
4. Is there an authn cookie? If yes, convert to claims principal and goto 9; use /common or /organization
5. Redirect to auth ask id token, client id, code
6. Receive a POST (from browser) with id\_token & code
7. Validate:
   1. Signature
   2. Audience
   3. Validity period
   4. Nonce – did we ask for it?
   5. Validate issuer
8. Deserialize token claims into a programming object (ClaimsPrincipal)
9. Exchange code for access token to API, cache at and refresh token
10. Business logic, uses ClaimsPrincipal for authz, customization
11. If business logic needs to call API get at from cache, add it to Authz hdr and call API
12. Serialize claims into an authn cookie
13. Respond with data

# Web API

1. Register in AAD
2. Obtain signing keysReceive an http request
3. Receive http call
4. Obtain at from Authz header
5. Validate (see 7 above)
6. Deserialzie into a programming object
7. Business logic
8. Respond