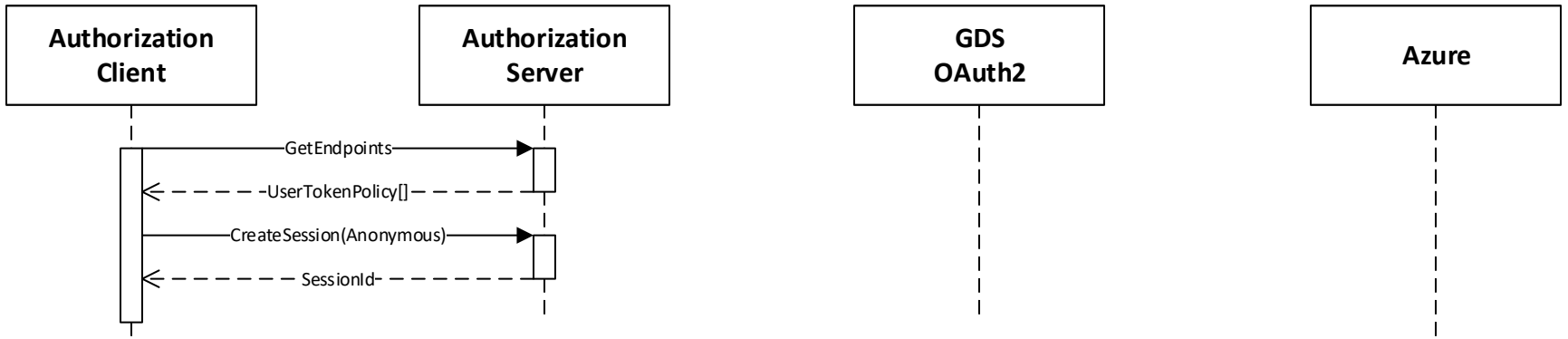
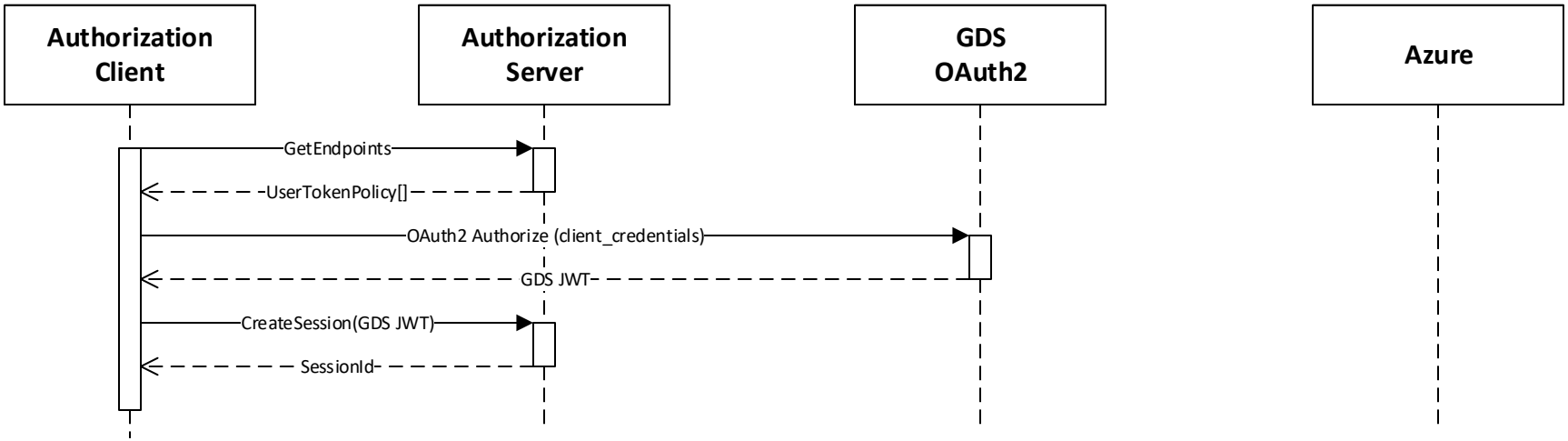
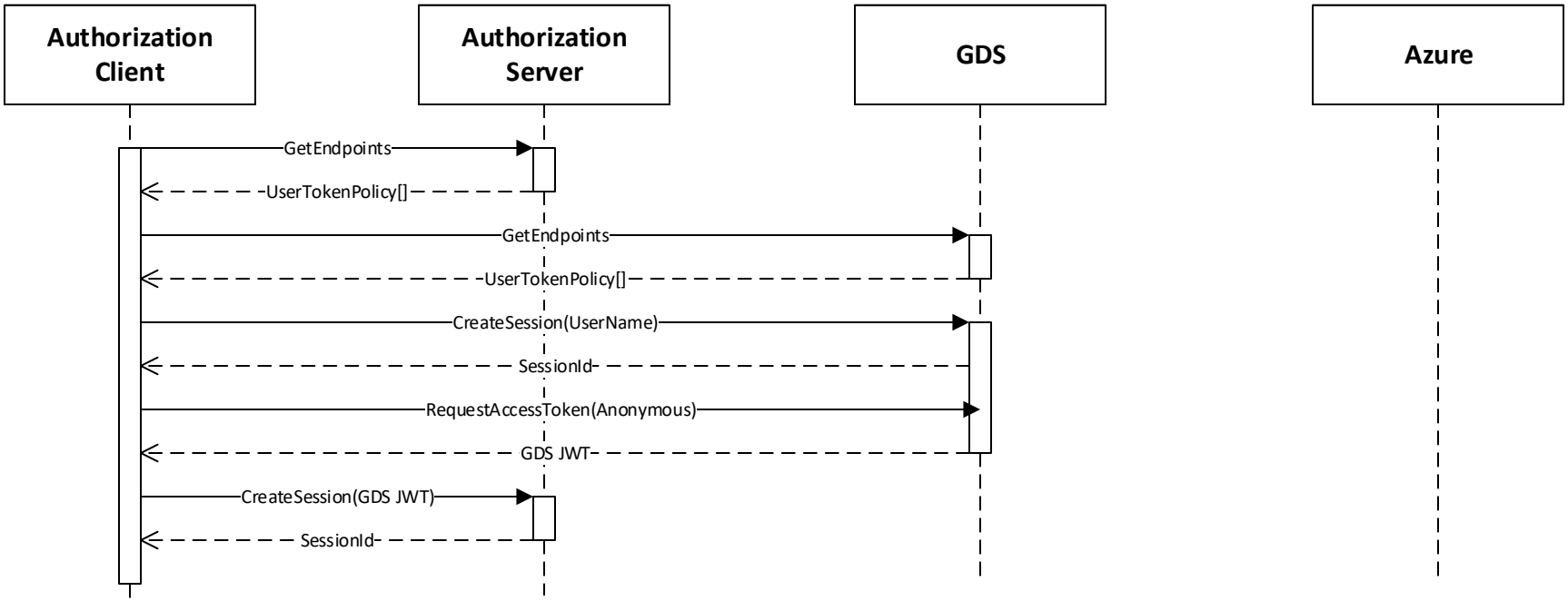


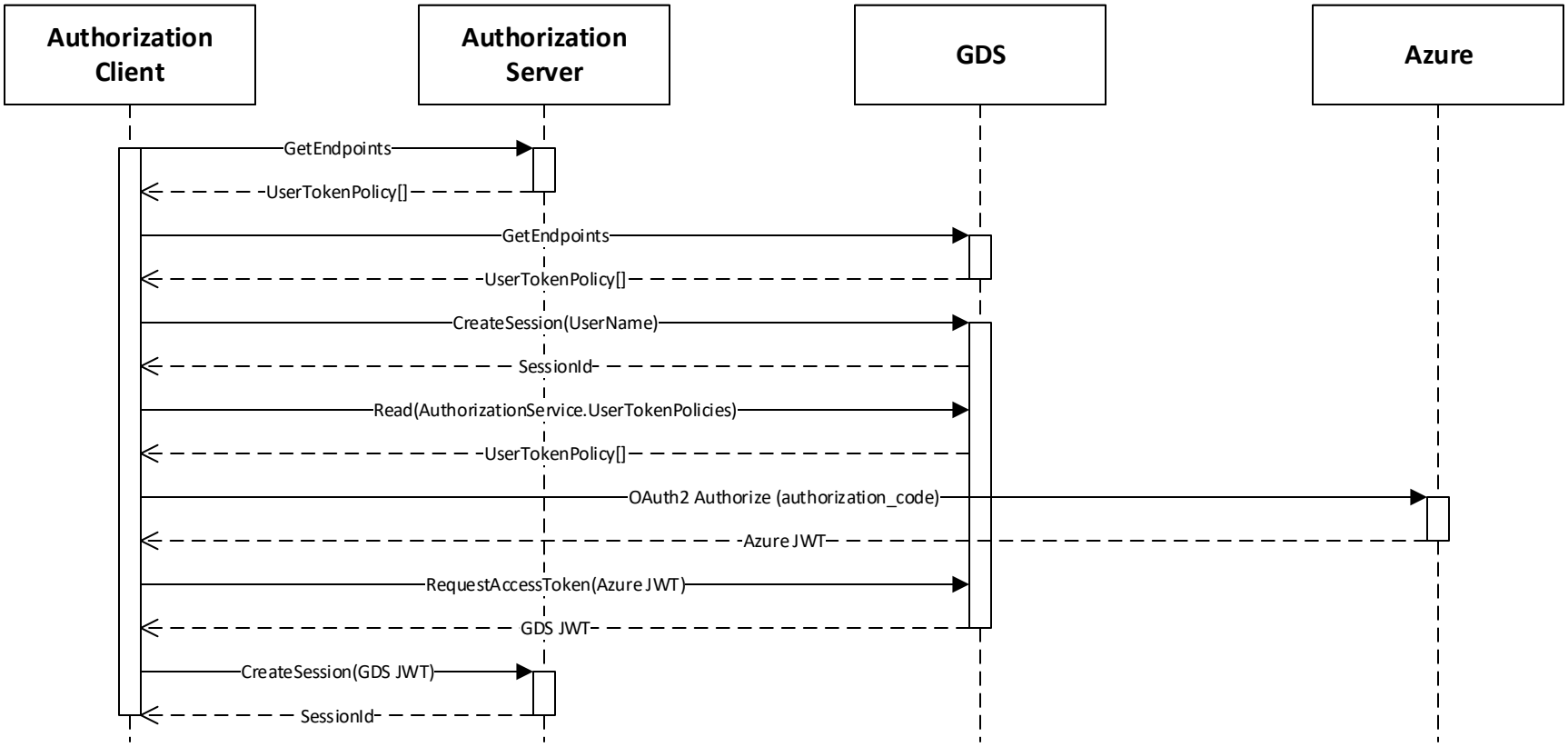
Simple Authentication: Client selects a policy (anonymous) that allows it to connect directly to the Server.



GDS OAuth2: Client selects a policy requires a JWT issued by the GDS OAuth2 endpoint.
Client connects to the GDS OAuth2 endpoint and provides credentials supplied out-of-band (in config file).
Client connects to the Server with the GDS JWT.



GDS JWT: Client selects a policy requires a JWT issued by the GDS OPC-UA endpoint.
Client connects to the GDS OPC-UA endpoint and provides credentials supplied out-of-band (in config file).
Client requests an JWT from the GDS using the default credentials (anonymous).
Server validates the default credentials and creates a new JWT which is returned to the Client.
Client connects to the Server with the GDS JWT.



GDS JWT: Client selects a policy requires a JWT issued by the GDS OPC-UA endpoint.
Client connects to the GDS OPC-UA endpoint and provides credentials supplied out-of-band (in config file).
Client reads the policies supported by the GDS when requesting JWTs.
Client selects a policy that requires an Azure JWT.
Client requests a JWT from Azure using credentials supplied out-of-band (in config file) and information provided by user.
Client requests an JWT from GDS using the Azure JWT.
Server validates the Azure JWT and creates a new JWT which is returned to the Client.
Client connects to the Server with the GDS JWT.