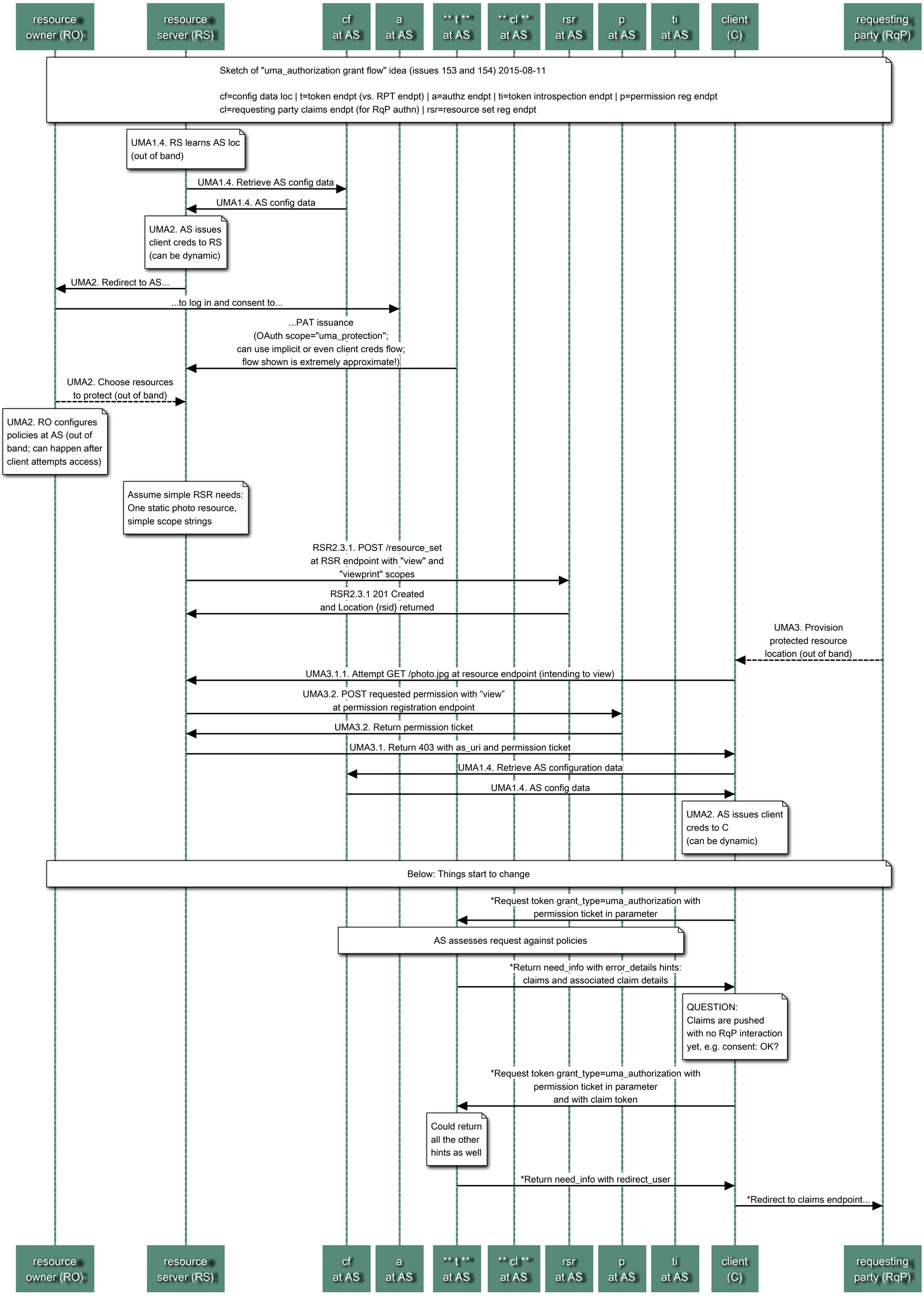
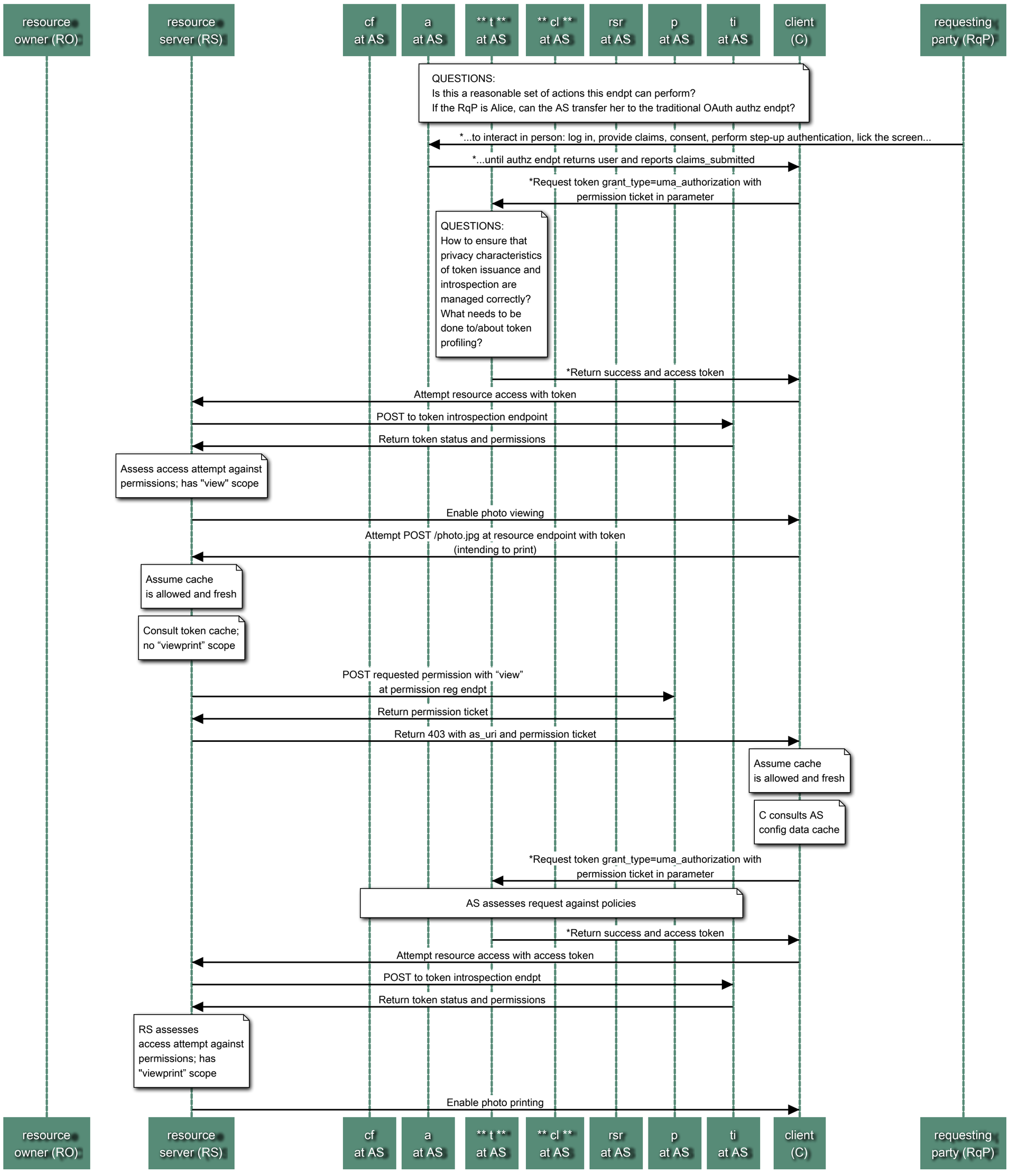

resource owner (RO)
resource server (RS)
cf at AS
a at AS
** t ** at AS
** cl ** at AS
rsr at AS
p at AS
ti at AS
client (C)
requesting party (RqP)
Sketch of "uma_authorization grant flow" idea (issues 153 and 154) 2015-08-11
cf=config data loc | t=token endpt (vs. RPT endpt) | a=authz endpt | ti=token introspection endpt | p=permission reg endpt
cl=requesting party claims endpt (for RqP authn) | rsr=resource set reg endpt
UMA1.4. RS learns AS loc (out of band)
UMA1.4. Retrieve AS config data
UMA1.4. AS config data
UMA2. AS issues client creds to RS (can be dynamic)
UMA2. Redirect to AS...
...to log in and consent to...
...PAT issuance (OAuth scope="uma_protection"; can use implicit or even client creds flow; flow shown is extremely approximate!)
UMA2. Choose resources to protect (out of band)
UMA2. RO configures policies at AS (out of band; can happen after client attempts access)
Assume simple RSR needs: One static photo resource, simple scope strings
RSR2.3.1. POST /resource_set at RSR endpoint with "view" and "viewprint" scopes
RSR2.3.1 201 Created and Location {rsid} returned
UMA3. Provision protected resource location (out of band)
UMA3.1.1. Attempt GET /photo.jpg at resource endpoint (intending to view)
UMA3.2. POST requested permission with “view” at permission registration endpoint
UMA3.2. Return permission ticket
UMA3.1. Return 403 with as_uri and permission ticket
UMA1.4. Retrieve AS configuration data
UMA1.4. AS config data
UMA2. AS issues client creds to C (can be dynamic)
Below: Things start to change
*Request token grant_type=uma_authorization with permission ticket in parameter
AS assesses request against policies
*Return need_info with error_details hints: claims and associated claim details
QUESTION: Claims are pushed with no RqP interaction yet, e.g. consent: OK?
*Request token grant_type=uma_authorization with permission ticket in parameter and with claim token
Could return all the other hints as well
*Return need_info with redirect_user
*Redirect to claims endpoint...


resource owner (RO)
resource server (RS)
cf at AS
a at AS
** t ** at AS
** cl ** at AS
rsr at AS
p at AS
ti at AS
client (C)
requesting party (RqP)
QUESTIONS:
Is this a reasonable set of actions this endpt can perform?
If the RqP is Alice, can the AS transfer her to the traditional OAuth authz endpt?
*...to interact in person: log in, provide claims, consent, perform step-up authentication, lick the screen...
*...until authz endpt returns user and reports claims_submitted
*Request token grant_type=uma_authorization with permission ticket in parameter
QUESTIONS:
How to ensure that privacy characteristics of token issuance and introspection are managed correctly?
What needs to be done to/about token profiling?
*Return success and access token
Attempt resource access with token
POST to token introspection endpoint
Return token status and permissions
Assess access attempt against permissions; has "view" scope
Enable photo viewing
Attempt POST /photo.jpg at resource endpoint with token (intending to print)
Assume cache is allowed and fresh
Consult token cache; no “viewprint” scope
POST requested permission with “view” at permission reg endpt
Return permission ticket
Return 403 with as_uri and permission ticket
Assume cache is allowed and fresh
C consults AS config data cache
*Request token grant_type=uma_authorization with permission ticket in parameter
AS assesses request against policies
*Return success and access token
Attempt resource access with access token
POST to token introspection endpt
Return token status and permissions
RS assesses access attempt against permissions; has "viewprint” scope
Enable photo printing