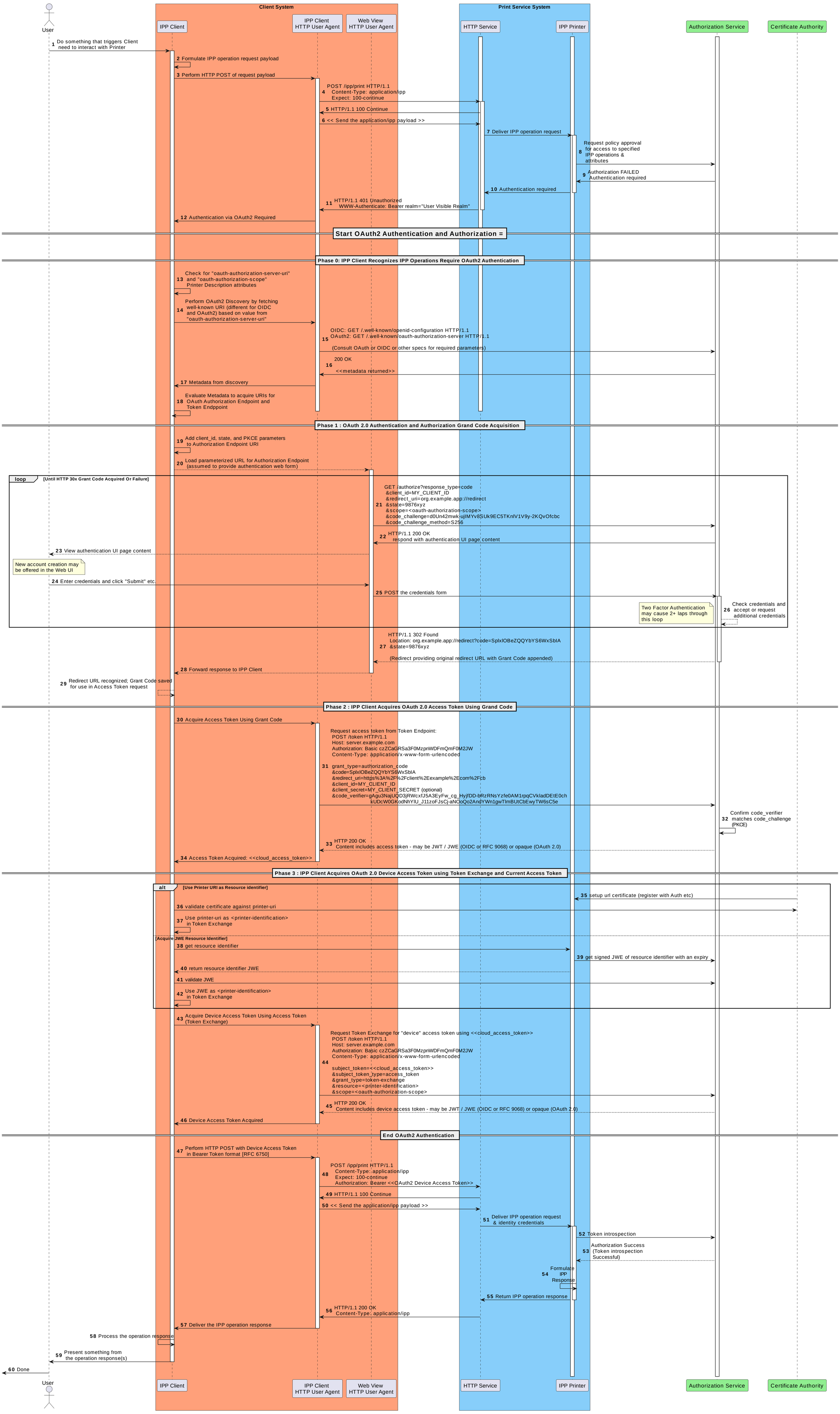
Client System
Print Service System
User
IPP Client
IPP Client HTTP User Agent
Web View HTTP User Agent
HTTP Service
IPP Printer
Authorization Service
Certificate Authority
1 Do something that triggers Client need to interact with Printer
2 Formulate IPP operation request payload
3 Perform HTTP POST of request payload
4 POST /ipp/print HTTP/1.1 Content-Type: application/ipp Expect: 100-continue
5 HTTP/1.1 100 Continue
6 << Send the application/ipp payload >>
7 Deliver IPP operation request
8 Request policy approval for access to specified IPP operations & attributes
9 Authorization FAILED Authentication required
10 Authentication required
11 HTTP/1.1 401 Unauthorized WWW-Authenticate: Bearer realm="User Visible Realm"
12 Authentication via OAuth2 Required
Start OAuth2 Authentication and Authorization =
Phase 0: IPP Client Recognizes IPP Operations Require OAuth2 Authentication
13 Check for "oauth-authorization-server-uri" and "oauth-authorization-scope" Printer Description attributes
14 Perform OAuth2 Discovery by fetching well-known URI (different for OIDC and OAuth2) based on value from "oauth-authorization-server-uri"
15 OIDC: GET /.well-known/openid-configuration HTTP/1.1 OAuth2: GET /.well-known/oauth-authorization-server HTTP/1.1 (Consult OAuth or OIDC or other specs for required parameters)
16 200 OK <<metadata returned>>
17 Metadata from discovery
18 Evaluate Metadata to acquire URIs for OAuth Authorization Endpoint and Token Endpoint
Phase 1 : OAuth 2.0 Authentication and Authorization Grand Code Acquisition
19 Add client_id, state, and PKCE parameters to Authorization Endpoint URI
20 Load parameterized URL for Authorization Endpoint (assumed to provide authentication web form)
loop [Until HTTP 30x Grant Code Acquired Or Failure]
21 GET /authorize?response_type=code &client_id=MY_CLIENT_ID &redirect_uri=org.example.app://redirect &state=9876xyz &scope=<oauth-authorization-scope> &code_challenge=d0Un42mwk-ujIMYv8SUk9EC5TKnlV1V9y-2KQvOfcbc &code_challenge_method=S256
22 HTTP/1.1 200 OK respond with authentication UI page content
23 View authentication UI page content
New account creation may be offered in the Web UI
24 Enter credentials and click "Submit" etc.
25 POST the credentials form
Two Factor Authentication may cause 2+ laps through this loop
26 Check credentials and accept or request additional credentials
27 HTTP/1.1 302 Found Location: org.example.app://redirect?code=SplxlOBeZQQYbYS6WxSbIA &state=9876xyz (Redirect providing original redirect URL with Grant Code appended)
28 Forward response to IPP Client
29 Redirect URL recognized; Grant Code saved for use in Access Token request
Phase 2 : IPP Client Acquires OAuth 2.0 Access Token Using Grand Code
30 Acquire Access Token Using Grant Code
31 Request access token from Token Endpoint: POST /token HTTP/1.1 Host: server.example.com Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW Content-Type: application/x-www-form-urlencoded grant_type=authorization_code &code=SplxlOBeZQQYbYS6WxSbIA &redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb &client_id=MY_CLIENT_ID &client_secret=MY_CLIENT_SECRET (optional) &code_verifier=gAgu3NajUQD3jRWcxfJ5A3EyFw_cg_HyjfDD-bRzRNsYzfe0AM1rpqCVkladDEtE0ch kUDcW0GKodNhYIU_J11zoFJsCj-aNOoQo2AndYWn1gwTlmBUtCbEwyTW6sC5e
32 Confirm code_verifier matches code_challenge (PKCE)
33 HTTP 200 OK Content includes access token - may be JWT / JWE (OIDC or RFC 9068) or opaque (OAuth 2.0)
34 Access Token Acquired: <<cloud_access_token>>
Phase 3 : IPP Client Acquires OAuth 2.0 Device Access Token using Token Exchange and Current Access Token
alt [Use Printer URI as Resource identifier]
35 setup url certificate (register with Auth etc)
36 validate certificate against printer-uri
37 Use printer-uri as <printer-identification> in Token Exchange
[Acquire JWE Resource Identifier]
38 get resource identifier
39 get signed JWE of resource identifier with an expiry
40 return resource identifier JWE
41 validate JWE
42 Use JWE as <printer-identification> in Token Exchange
43 Acquire Device Access Token Using Access Token (Token Exchange)
44 Request Token Exchange for "device" access token using <<cloud_access_token>> POST /token HTTP/1.1 Host: server.example.com Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW Content-Type: application/x-www-form-urlencoded subject_token=<<cloud_access_token>> &subject_token_type=access_token &grant_type=token-exchange &resource=<printer-identification> &scope=<oauth-authorization-scope>
45 HTTP 200 OK Content includes device access token - may be JWT / JWE (OIDC or RFC 9068) or opaque (OAuth 2.0)
46 Device Access Token Acquired
End OAuth2 Authentication
47 Perform HTTP POST with Device Access Token in Bearer Token format [RFC 6750]
48 POST /ipp/print HTTP/1.1 Content-Type: application/ipp Expect: 100-continue Authorization: Bearer <<OAuth2 Device Access Token>>
49 HTTP/1.1 100 Continue
50 << Send the application/ipp payload >>
51 Deliver IPP operation request & identity credentials
52 Token introspection
53 Authorization Success (Token introspection Successful)
54 Formulate IPP Response
55 Return IPP operation response
56 HTTP/1.1 200 OK Content-Type: application/ipp
57 Deliver the IPP operation response
58 Process the operation response
59 Present something from the operation response(s)
60 Done