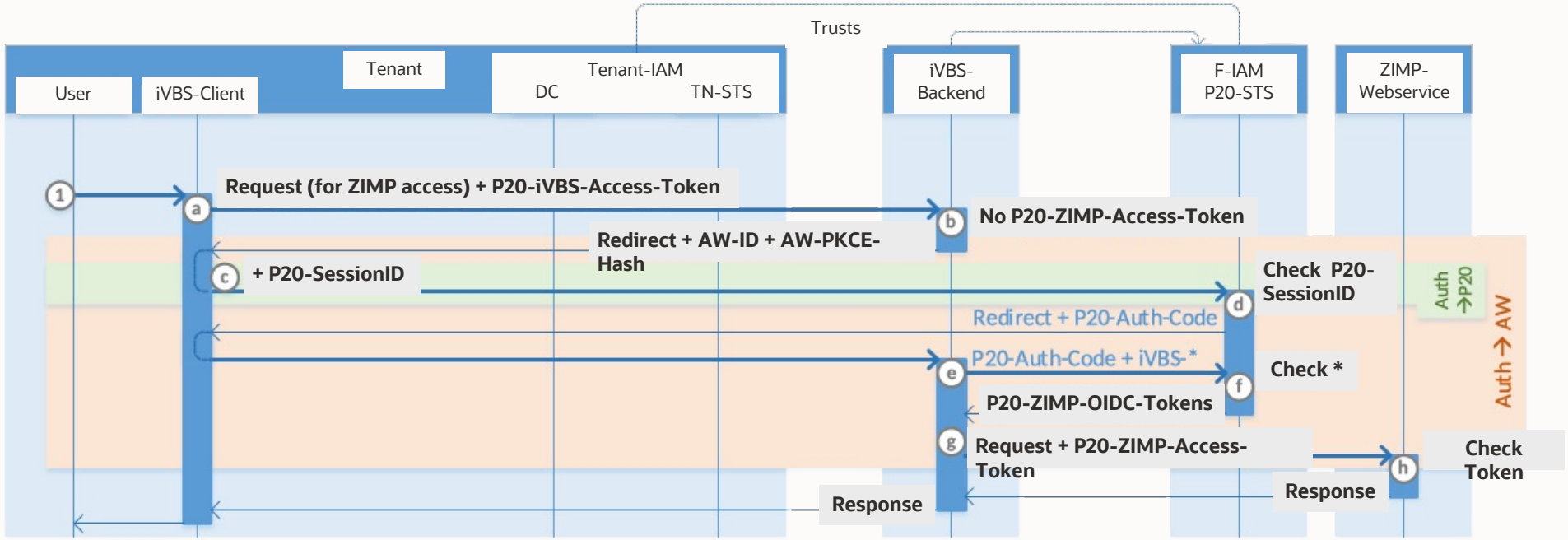
Specification & Justification for ER 32804378 @Federal Criminal Police Office (BKA) & Federal Office for Migration and Refugees (BAMF)

Oracle Germany
Joerg Leonardy, Uemit Aytekin, Melinda Nath-Richter

BKA / Sequence Diagram for “Token Exchange” Use Case



Please see next slide for detailed step description outlined from 1 a to h.

BKA / “Token Exchange” Use Case

When processing a case via the iVBS client (a native desktop application), the iVBS backend needs to call the ZIMP web service (integration module query). The authentication has to be done via a dedicated JWT (P20-ZIMP-Access-Token) so the JWT (P20-iVBS-Access-Token) used between the iVBS client and iVBS backend is not suitable. As long as the token exchange is not available in F-IAM, another way must be found.

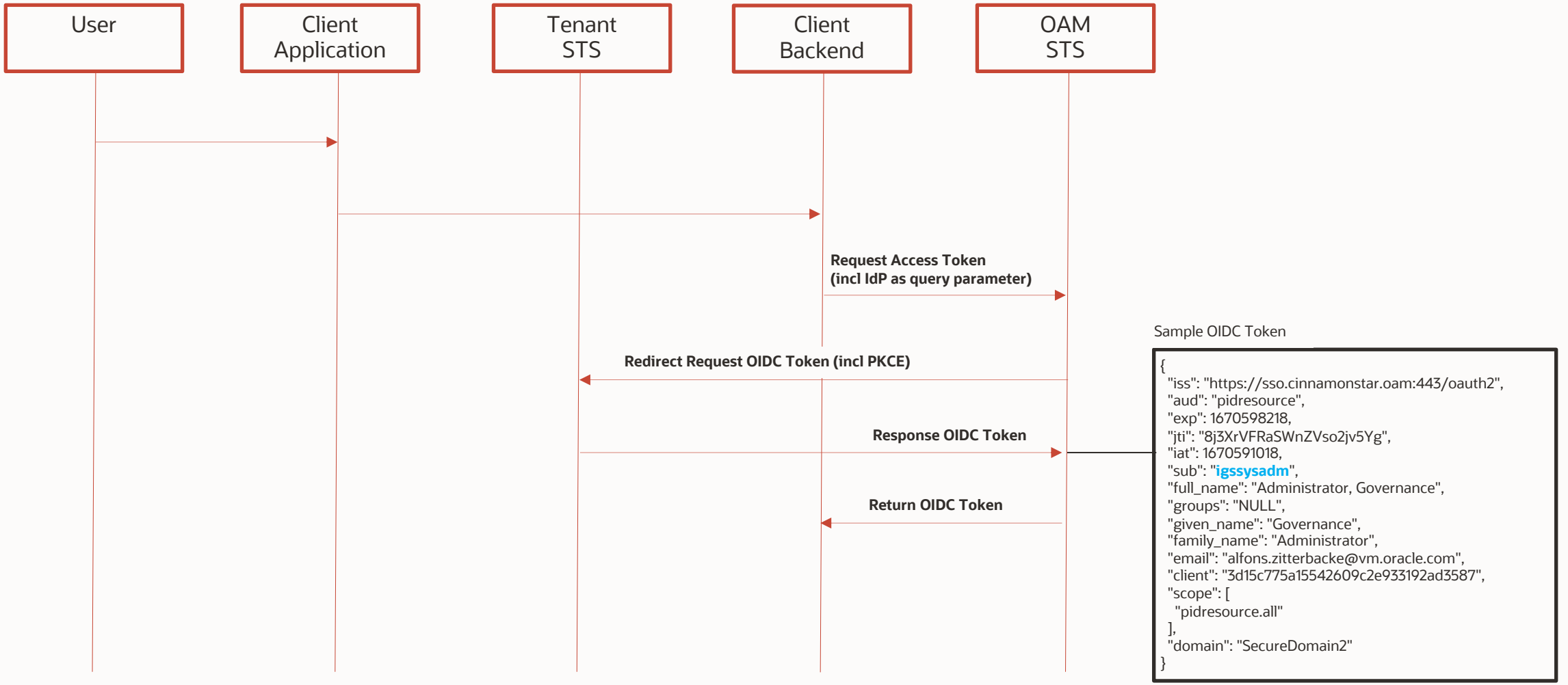
The user is already logged in, so the iVBS client has a JWT for authentication to the iVBS backend.

1. Transaction processing with ZIMP web service requirements

The user interacts with the iVBS client, thus creating the need to make a ZIMP web service request through the iVBS backend.

a. The iVBS client sends a request to the iVBS backend, with the existing access token being sent for authentication.
b. The iVBS backend identifies the need to invoke the ZIMP web service, but does not yet have a suitable token for authentication against ZIMP and therefore initiates an OIDC authorization code flow. To do this, it responds with a redirect to the F-IAM and transfers, among other things, its own application ID (OIDC client ID) and the hash of a self-generated PKCE as query parameters. Note: In this case, the iVBS backend is the OIDC client. From the point of view of the F-IAM, this is a different application than the login, where the iVBS client was the OIDC client and the iVBS backend took on the role of the service provider.
c. The rich client executes the redirect and adds the session ID received from the F-IAM as part of the login.
d. The F-IAM checks the received session ID, making renewed authentication via the TN-IAM unnecessary. In response, a redirect is sent to the iVBS backend along with a newly generated authorization code.
e. The iVBS backend uses the authorization code and sends an authentication request to the P20-STS together with its own application ID, the plaintext PKCE whose hash value was transmitted in 1.b, and its own application secret.
f. The P20-STS checks the transferred parameters. It then determines the P20 UID associated with the authorization code and the associated user attributes and authorizations. It finally responds with the requested tokens.
g. The iVBS backend stores the received access token for all further ZIMP requests. It now sends the request to the ZIMP web service, passing the dedicated access token for authentication.
h. The ZIMP web service checks the access token and sends the technical answer, which is then processed by the iVBS backend and enables the answer to the iVBS client.

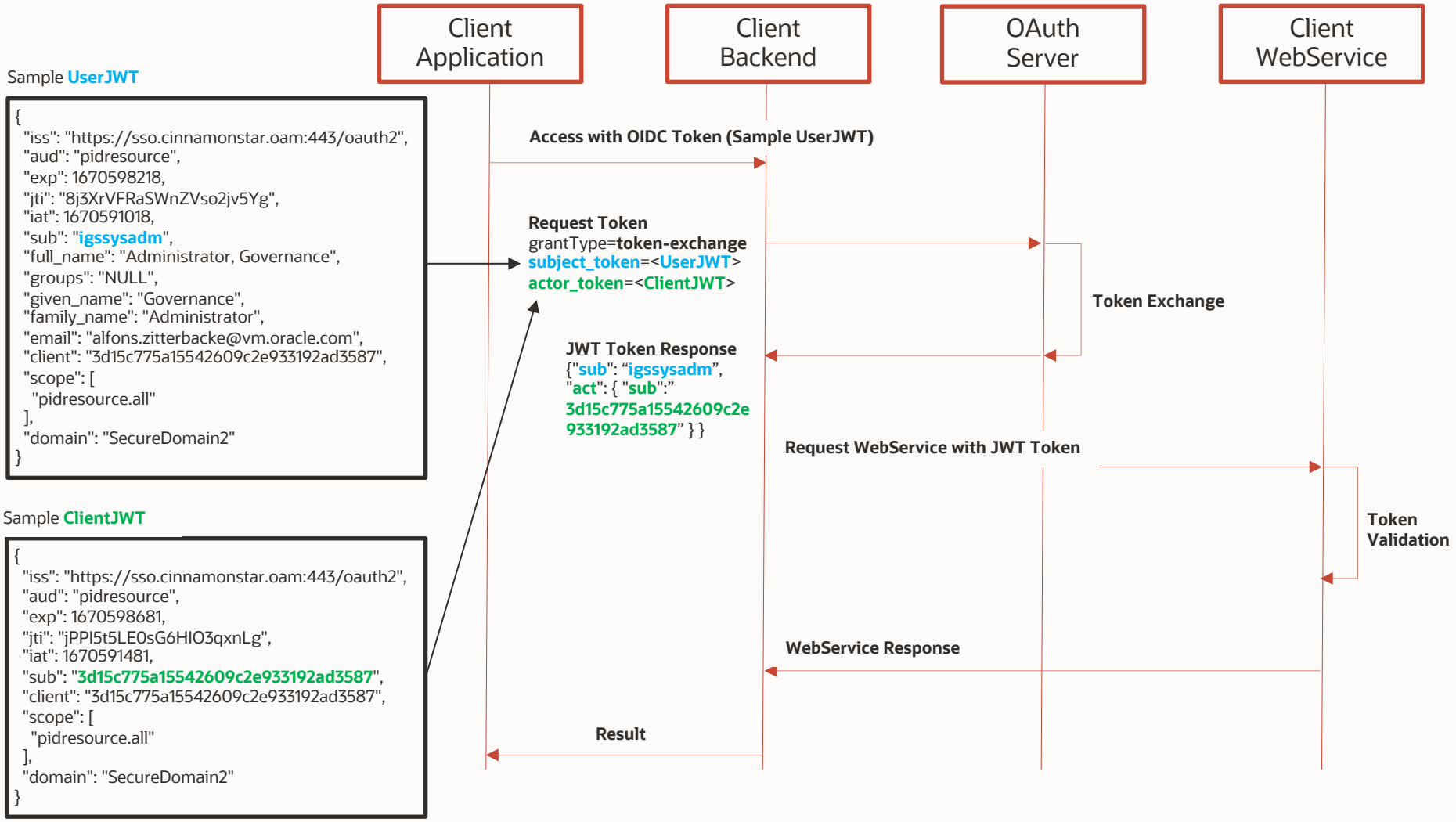
1. Get OIDC Token for Client Application



Sample OIDC Token


```
{
 "iss": "https://sso.cinnamonstar.oam:443/oauth2",
 "aud": "pidresource",
 "exp": 1670598218,
 "jti": "8j3XrVFRaSWnZVso2jv5Yg",
 "iat": 1670591018,
 "sub": "igssysadm",
 "full_name": "Administrator, Governance",
 "groups": "NULL",
 "given_name": "Governance",
 "family_name": "Administrator",
 "email": "alfons.zitterbacke@vm.oracle.com",
 "client": "3d15c775a15542609c2e933192ad3587",
 "scope": [
  "pidresource.all"
 ],
 "domain": "SecureDomain2"
}
```

2. Token Exchange (Delegation) based on OIDC Token for Client Application



BAMF / SR and ER for “Token Exchange” Use Case

SR “3-25728439331 : OAM / OAuth impersonation & delegation support (RFC8693)” created **Apr 20, 2021**
ER 32804378 - OAM / OAUTH IMPERSONATION & DELEGATION SUPPORT (RFC8693) created Apr 29, 2021
last updated **Jul 15, 2021**

1. Why is this technically desirable

As described in IETF's RFC8693 (https://tools.ietf.org/html/rfc8693)
one common use case for an STS is to allow a resource server A to make calls to a backend service C on behalf of the requesting user B. Depending on the local site policy and authorization infrastructure, it may be desirable for A to use its own credentials to access C along with an annotation of some form that A is acting on behalf of B ("delegation") or for A to be granted a limited access credential to C but that continues to identify B as the authorized entity ("impersonation"). Delegation and impersonation can be useful concepts in other scenarios involving multiple participants as well.

2. Describe the business problem that this request addresses

Missing standard in OAM to achieve delegation and impersonation use cases to implement customer's applications security characteristics