

[Desconflito][Autenticação]

Roteiro Etapa 1

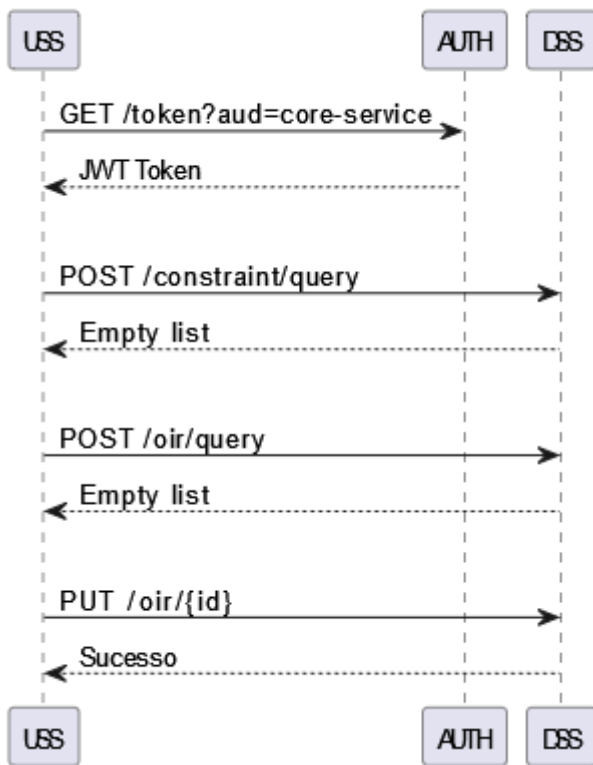
Criação de OIR

Uma *Operational Intent Reference(OIR)* é a representação 4D da intenção de operação de uma aeronave não tripulada. No ambiente UTM, a criação e edição de OIRs deve ser coordenada com os outros provedores presentes ou interessados na região da operação. Para possibilitar que essa coordenação seja feita programaticamente, o DECEA manterá um serviço de Descoberta, que é um local onde provedores podem declarar suas operações, assim como obter as operações de outros provedores numa área específica.

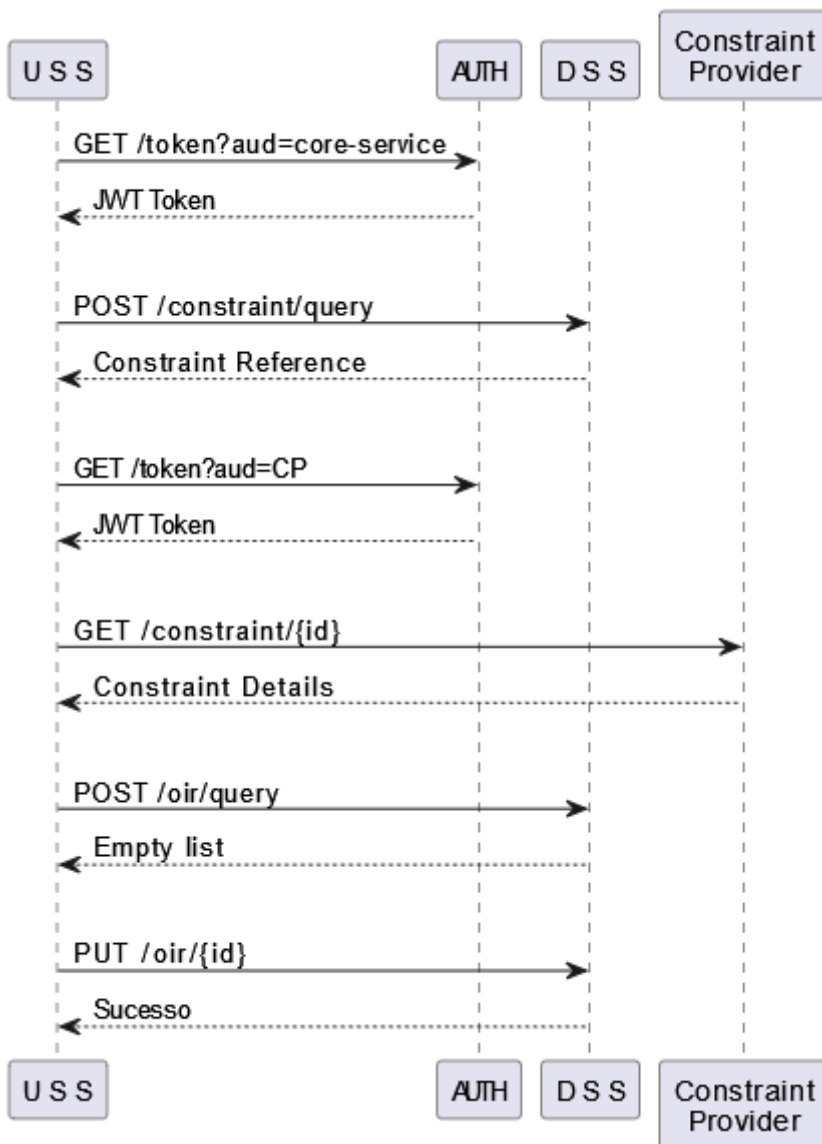
Nesse workshop, iremos aprender a interagir com esse serviço de descoberta, chamado DSS. O DSS provido pelo DECEA é derivado da implementação feita pelo projeto [InterUSS](#), que por sua vez é uma implementação dos padrões ASTM-3411 e ASTM-3548. A comunicação com o DSS é feita via HTTP e os contratos estão definidos em: <https://github.com/dp-icea/Protocols>

A complexidade na criação da OIR depende de quantas outras entidades (Constraints ou outras OIRs) estão presentes no mesmo volume 4D. Nesse workshop, iniciaremos com o cenário mais simples, evoluindo até o cenário mais complexo.

OIR isolada

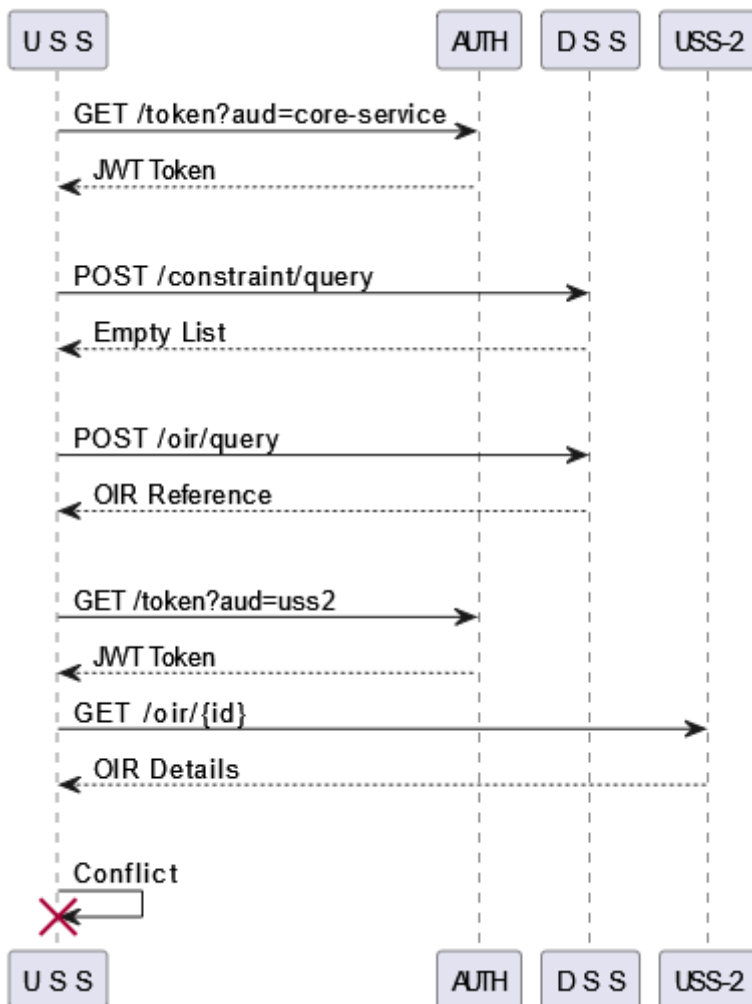


OIR próxima a Constraint

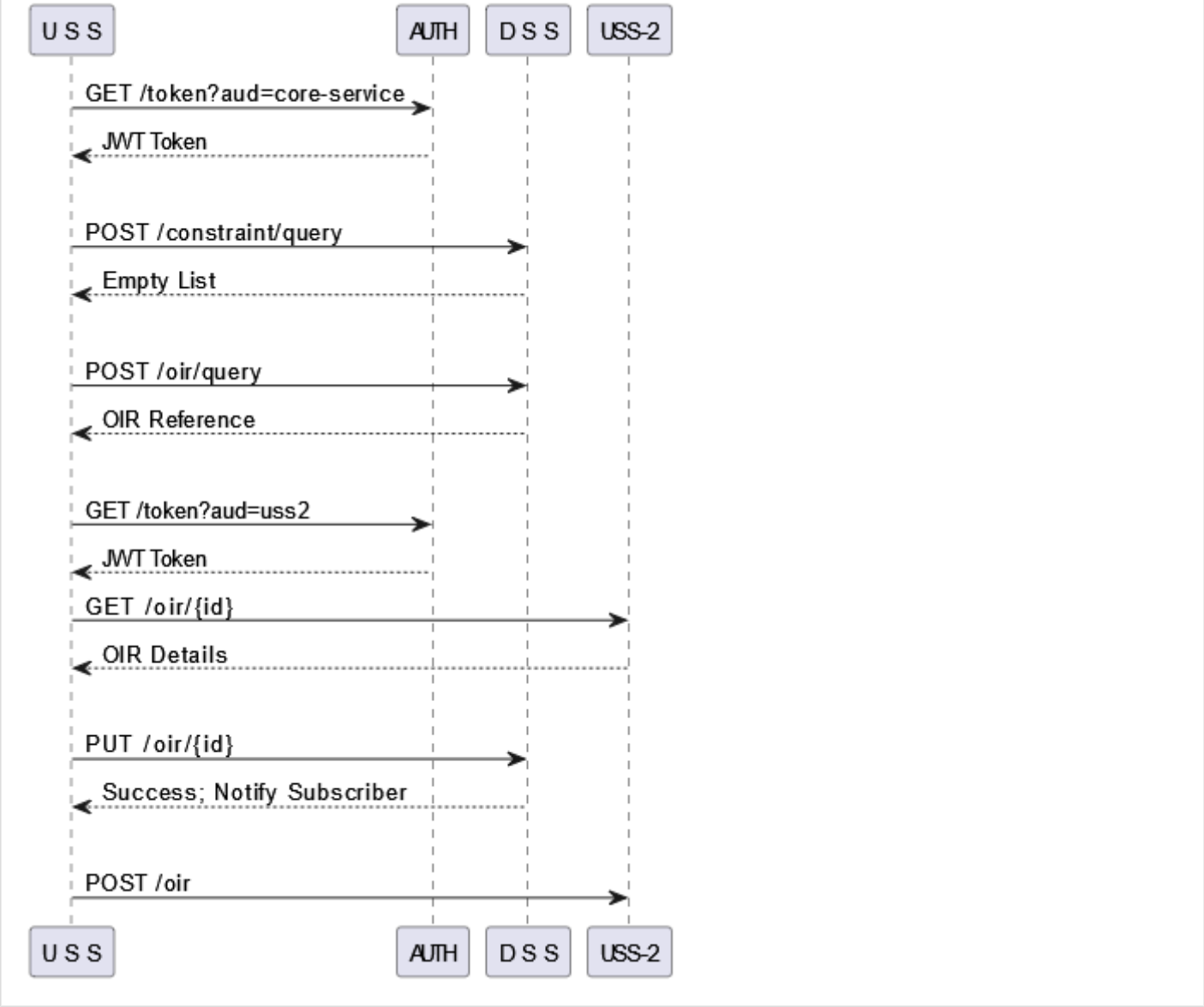


OIR com conflito

Maior ou igual prioridade



Menor prioridade



Endpoints de coordenação

Operational intent details			Endpoints exposed by USSs for interaction with details of operational intents.	^
GET	/uss/v1/operational_intents/{entityid}	Retrieve the specified operational intent details from a USS.	🔒	▼
GET	/uss/v1/operational_intents/{entityid}/telemetry	Query detailed information on the position of an off-nominal operational intent from a USS.	🔒	▼
POST	/uss/v1/operational_intents	Notify a peer USS of changed operational intent details.	🔒	▼

Ativação de OIR (Momentos antes do voo)

Atualizar a OIR no DSS e notificar os Subscribers

PUT**/dss/v1/operational_intent_references/{entityid}/{ovn}** Update the specified operational intent reference in the DSS.

Autenticação

Autenticar-se

A URL base é <http://montreal.icea.decea.mil.br:64235/token>

A requisição deve conter as seguintes *query_strings*

intended_audience	USS de destino da mensagem (Domínio do provedor) Ex. "utm.decea.mil.br"
scope	escopo da requisição. Ex.: utm.strategic_coordination. O scope esperado de cada endpoint está definido no OpenAPI
apikey	chave recebida do ICEA. Pode-se optar em enviar esse campo no Header da requisição

Validar autenticação de outro USS

Ao receber uma requisição de outro USS em seu servidor, é necessário validar o token de autenticação fornecido pelo outro USS. O payload do token contém as seguintes informações:

aud	Domínio do seu provedor.	"utm.provider1.com"
exp	Timestamp epoch do horário de expiração do token. O token não deve ser aceito a partir desse horário	1719777868
iss	Nome do provedor emissor do token	ICEA

scope	Scope autorizado pelo token. Cada endpoint deve aceitar apenas determinados scopes, conforme definido no OpenAPI	utm.strategic_coordination
sub	Nome do provedor origem da requisição. Não deve ser validado	"USS1"

Os passos para verificação são

- 1. Verificar assinatura do token
 - 1. Deve-se validar a assinatura do token utilizando a chave pública do ICEA, que será fornecida durante o workshop.
- 2. Verificar a validade do token
 - 1. Deve-se validar que o campo "exp" não seja menor do que o horário atual
- 3. Verificar audiência do token
 - 1. Deve-se validar que o campo "aud" seja o seu nome, ou seja, o nome do provedor que está recebendo a requisição
- 4. Verificar o scope
 - 1. Deve-se validar que o campo "scope" contenha o scope necessário para requisitar o endpoint. Um token pode possuir mais de um scope separados por espaço em branco.

Chave Publica Eco-UTM

-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgHkNtpy3GB0YTCI2VCCd22i0rJwI
GBSazD4QRKvH6rch0IP4igb+02r7t0X//tuj0VbwtJz3cEICP8OGSqrDTSCGj5Y0
3Oa2gPxx/0c0V8D0eSXS/CUC0qrYHnAGLqko7eW87HW0rh7nnl2bB4Lu+R8fOmQt
5frCJ5eTkzwK5YczAgMBAAE=
-----END PUBLIC KEY-----