# OGC Testbed-14

## *Authorisation, Authentication, & Billing Engineering Report*

# Table of Contents

Publication Date: 2019-02-07

Approval Date: 2018-12-13

Submission Date: 2018-11-22

Reference number of this document: OGC 18-057

Reference URL for this document: http://www.opengis.net/doc/PER/t14-D010

Category: Public Engineering Report

Editor: Jérôme Gasperi

Title: OGC Testbed-14: Authorisation, Authentication, & Billing Engineering Report

---

**OGC Engineering Report**

**COPYRIGHT**



**WARNING**

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as a deliverable in an OGC Interoperability Initiative and is not an official position of the OGC membership. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, any OGC Engineering Report should not be referenced as required or mandatory technology in procurements. However, the discussions in this document could very well lead to the definition of an OGC Standard.

**LICENSE AGREEMENT**

Permission is hereby granted by the Open Geospatial Consortium, ("Licensor"), free of charge and subject to the terms set forth below, to any person obtaining a copy of this Intellectual Property and any associated documentation, to deal in the Intellectual Property without restriction (except as set forth below), including without limitation the rights to implement, use, copy, modify, merge, publish, distribute, and/or sublicense copies of the Intellectual Property, and to permit persons to whom the Intellectual Property is furnished to do so, provided that all copyright notices on the intellectual property are retained intact and that each person to whom the Intellectual Property is furnished agrees to the terms of this Agreement.

If you modify the Intellectual Property, all copies of the modified Intellectual Property must include, in addition to the above copyright notice, a notice that the Intellectual Property includes modifications that have not been approved or adopted by LICENSOR.

THIS LICENSE IS A COPYRIGHT LICENSE ONLY, AND DOES NOT CONVEY ANY RIGHTS UNDER ANY PATENTS THAT MAY BE IN FORCE ANYWHERE IN THE WORLD. THE INTELLECTUAL PROPERTY IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE INTELLECTUAL PROPERTY WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE INTELLECTUAL PROPERTY WILL BE UNINTERRUPTED OR ERROR FREE. ANY USE OF THE INTELLECTUAL PROPERTY SHALL BE MADE ENTIRELY AT THE USER’S OWN RISK. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR ANY CONTRIBUTOR OF INTELLECTUAL PROPERTY RIGHTS TO THE INTELLECTUAL PROPERTY BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM ANY ALLEGED INFRINGEMENT OR ANY LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR UNDER ANY OTHER LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH THE IMPLEMENTATION, USE, COMMERCIALIZATION OR PERFORMANCE OF THIS INTELLECTUAL PROPERTY.

This license is effective until terminated. You may terminate it at any time by destroying the Intellectual Property together with all copies in any form. The license will also terminate if you fail to comply with any term or condition of this Agreement. Except as provided in the following sentence, no such termination of this license shall require the termination of any third party end-user sublicense to the Intellectual Property which is in force as of the date of notice of such termination. In addition, should the Intellectual Property, or the operation of the Intellectual Property, infringe, or in LICENSOR’s sole opinion be likely to infringe, any patent, copyright, trademark or other right of a third party, you agree that LICENSOR, in its sole discretion, may terminate this license without any compensation or liability to you, your licensees or any other party. You agree upon termination of any kind to destroy or cause to be destroyed the Intellectual Property together with all copies in any form, whether held by you or by any third party.

Except as contained in this notice, the name of LICENSOR or of any other holder of a copyright in all or part of the Intellectual Property shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Intellectual Property without prior written authorization of LICENSOR or such copyright holder. LICENSOR is and shall at all times be the sole entity that may authorize you or any third party to use certification marks, trademarks or other special designations to

indicate compliance with any LICENSOR standards or specifications.

This Agreement is governed by the laws of the Commonwealth of Massachusetts. The application to this Agreement of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded. In the event any provision of this Agreement shall be deemed unenforceable, void or invalid, such provision shall be modified so as to make it valid and enforceable, and as so modified the entire Agreement shall remain in full force and effect. No decision, action or inaction by LICENSOR shall be construed to be a waiver of any rights or remedies available to it.

None of the Intellectual Property or underlying information or technology may be downloaded or otherwise exported or reexported in violation of U.S. export laws and regulations. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use the Intellectual Property, and you represent that you have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

# Chapter 1. Summary

In the context of a generic Earth Observation Exploitation Platform ecosystem, populated by Thematic Exploitation Platforms (TEPs) and Mission Exploitation Platforms (MEPs), which make use of cloud computing resources for Earth Observation data processing, the European Space Agency (ESA) has established two fundamental building blocks within a TEP, with different functions, the Application Deployment and Execution Service (ADES) and the Execution Management Service (EMS). Users interact with a TEP using a Web Client and the TEP contains an EMS and an ADES. The EMS includes most of the control logic, required for deploying and executing applications in different MEPs and TEPs while the ADES instead is responsible for the single application deployment and execution on a specific platform (i.e. TEP and/or MEP).

The D009 - ADES and EMS Results and Best Practices Engineering Report [https://github.com/opengeospatial/D009-ADES_and_EMS_Results_and_Best_Practices_Engineering_Report] describes how the two services should be engineered in the Exploitation Platform context.

This Engineering Report (ER) describes the work performed by the Participants in the Exploitation Platforms Earth Observation Clouds (EOC) Thread of OGC Testbed-14 concerning the interfaces proposed for the Authentication, Authorization, Billing and Quoting topics associated to the EMS and the ADES components.

## 1.1. Requirements & Research Motivation

The primary motivation behind this ER is to tackle user's authentication and subsequent authorization concerns in terms of process deployment and execution within a pool of Thematics Exploitation Platforms (TEP) and Mission Exploitation Platforms (MEP).

Additionally, this ER addresses quotation mechanism and associated billing aspects of existing processes exposed through a secured OGC Web Processing Service 2.0 endpoint.

## 1.2. Prior-After Comparison

In Testbed-13, the Security Engineering Report (ER) covered topics related to the implementation of authentication and authorization plugins for the QGIS open source desktop GIS client and the implementation of a secured workflow. The present ER covers more specifically the authentication and authorization mechanism applied to EMS and ADES.

Billing and Quotation have been introduced within Testbed14 and are currently not addressed by OGC standards.

## 1.3. Recommendations for Future Work

The OGC WPS 2.0 standard was already a key part of the work done in Testbed-13 and continued to be so in Testbed-14. Indeed, given that one of the core aspects of Earth Observation Exploitation Platforms is the data processing, WPS is a natural fit. At the same time, not only in Testbed-13 but in general, variations and possibilities related to WPS, such as the Transactional extension (WPS-T) and the reliance on REST bindings and JSON encoding, are of increasing interest and popularity as

they bring the OGC and WPS in particular closer to the mainstream web and technological realms.

Given that a significant amount of effort in the EOC thread of Testbed 14 has been dedicated to experimenting with these WPS variations and possibilities, this work is expected to be of high interest to the WPS 2.0 Standards Working Group (SWG). In coordination with the WPS 2.0 SWG, several smaller (or one or two larger) Change Requests can be prepared so as to start the standardization path for WPS-T and the WPS REST/JSON work.

For OGC, the work described in this Engineering Report, which makes the case for how OGC standards are helpful in such a densely populated ecosystem of very heterogeneous entities, technologies and implementations such as the Exploitation Platforms one, is deemed extremely relevant in satisfying the needs of the ESA as one of its Strategic Partners.

## 1.4. Document contributor contact points

All questions regarding this document should be directed to the editor or the contributors:

**Contacts**

| Name | Organization |
|---|---|
| Jérôme Gasperi | Geomatys |
| Guilhem Legal | Geomatys |
| Patrick Jacques | Spacebel |
| Tom Landry | CRIM |
| Paulo Sacramento | Solenix |
| Peter Vretanos | CubeWerx |

## 1.5. Foreword

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

# Chapter 2. References

The following normative documents are referenced in this document.

*NOTE: Only normative standards are referenced here, e.g. OGC, ISO or other SDO standards. All other references are listed in the bibliography. Example:*

- OGC: OGC 06-121r9 - OGC® Web Services Common Standard, April 2010 [https://portal.opengeospatial.org/files/?artifact_id=38867&version=2]
- OGC: OGC 14-065 - OGC® WPS 2.0 Interface Standard, March 2015 [http://docs.opengeospatial.org/is/14-065/14-065.html]
- IETF: RFC 6749 - The OAuth 2.0 Authorization Framework [https://tools.ietf.org/html/rfc6749]
- IETF: RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage [https://tools.ietf.org/html/rfc6750]
- IETF: RFC 7235 - Hypertext Transfer Protocol (HTTP/1.1): Authentication [https://tools.ietf.org/html/rfc7235]
- IETF: RFC 7519 - JSON Web Token (JWT) [https://tools.ietf.org/html/rfc7519]

# Chapter 3. Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Standard OGC 06-121r9 [https://portal.opengeospatial.org/files/?artifact_id=38867&version=2] shall apply. In addition,

The following terms and definitions apply:

## 3.1. Definitions

**Access Control List**

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.[1] Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Alice: read,write; Bob: read), this would give Alice permission to read and write the file and Bob to only read it (source Wikipedia [https://en.wikipedia.org/wiki/Access_control_list])

**Access Token**

Access tokens are credentials used to access protected resources.[RFC 6749]

**Authentication**

Process used to achieve sufficient confidence in the binding between the Entity and the presented Identity.

**Authentication Request**

OAuth 2.0 Authorization Request using extension parameters and scopes defined by OpenID Connect to request that the End-User be authenticated by the Authorization Server, which is an OpenID Connect Provider, to the Client, which is an OpenID Connect Relying Party.

**Authorization Server** The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.[RFC 6749]

**Bearer Token**

A security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can. Using a bearer token does not require a bearer to prove possession of cryptographic key material (proof-of-possession).

**Claim**

Piece of information asserted about an Entity.

**Claims Provider**

Server that can return Claims about an Entity.

**End-User**

Human participant.

**Entity**

Something that has a separate and distinct existence and that can be identified in a context. An End-User is one example of an Entity.

**Identifier**

Value that uniquely characterizes an Entity in a specific context.

**Issuer**

Entity that issues a set of Claims.

**Issuer Identifier**

Verifiable Identifier for an Issuer. An Issuer Identifier is a case-sensitive URL using the https scheme that contains scheme, host, and optionally, port number and path components and no query or fragment components.

**OpenAPI definition | OpenAPI document**

A document (or set of documents) that defines or describes an API and conforms to the OpenAPI Specification [https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md].

**OpenID Provider (OP)**

OAuth 2.0 Authorization Server that is capable of Authenticating the End-User and providing Claims to a Relying Party about the Authentication event and the End-User.

**Personally Identifiable Information (PII)**

Information that (a) can be used to identify the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person to whom such information relates.

**Relying Party (RP)**

OAuth 2.0 Client application requiring End-User Authentication and Claims from an OpenID Provider.

**Resource Server**

The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.[RFC 6749]

**UserInfo Endpoint**

Protected Resource that, when presented with an Access Token by the Client, returns authorized information about the End-User represented by the corresponding Authorization Grant.

## 3.2. Abbreviated terms

- **ACL** Access Control List
- **ADES** Application Deployment and Execution Service
- **API** Application Programming Interface
- **CWL** Common Workflow Language

- **EMS** Execution Management Service
- **EO** Earth Observation
- **EP** Exploitation Platform
- **ER** Engineering Report
- **ESA** European Space Agency
- **IdP** Identity Provider
- **JSON** JavaScript Object Notation
- **MEP** Mission Exploitation Platform
- **OP** OpenID Provider
- **OWC** OWS Context
- **OWS** OGC Web Services
- **RP** Relying Party
- **TEP** Thematic Exploitation Platform
- **WPS** Web Processing Service

# Chapter 4. Overview

Section 5 presents the architecture and concern of Authentication and Authorization and how it is tackled within Testbed-14.

Section 6 deals with the quotation aspect.

Section 7 deals with the billing aspect.

# Chapter 5. Authentication and Authorization

## 5.1. Overview

The sequence diagram below presents an overview of the authentication/authorization sequence between the different components involved in Testbed 14 in the case of a call to an execute service.

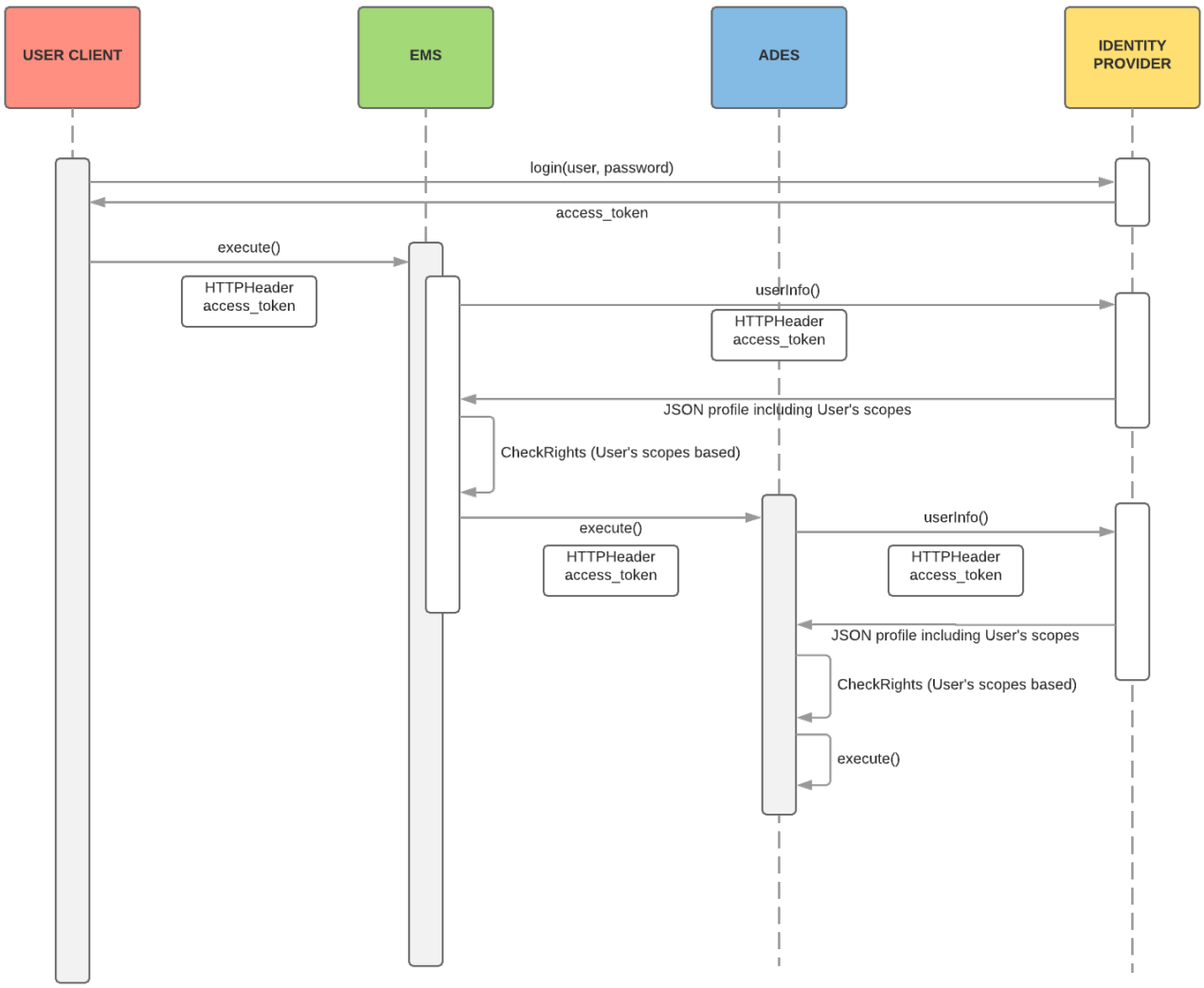



*Figure 1. General Sequence Diagram of authorization process*

## 5.2. Authentication

Usually, the authentication of users is delegated to an Identity Provider (IdP) while the authorizations occur at the resources/services providers level (i.e. EMS and ADES).

In Testbed-14, users authenticate through the Web client using the OpenID Connect protocol 1.0. Other protocols can be used for authentication (e.g. shibboleth, EduGain, etc.). However whatever the implementation and the authentication method chosen, the IdP should provide to the Client an access_token that can be used to request End User claims through a UserInfo Endpoint.

In summary, in Testbed-14 the following assumptions are made:

- There is only one Identity Provider (IdP).
- The IdP supports the OpenID Connect protocol 1.0. and provides an acces_token for subsequent claims requests
- The IdP stores user's role as part of the user's profile
- EMS and ADES components authorization is based on OAuth2

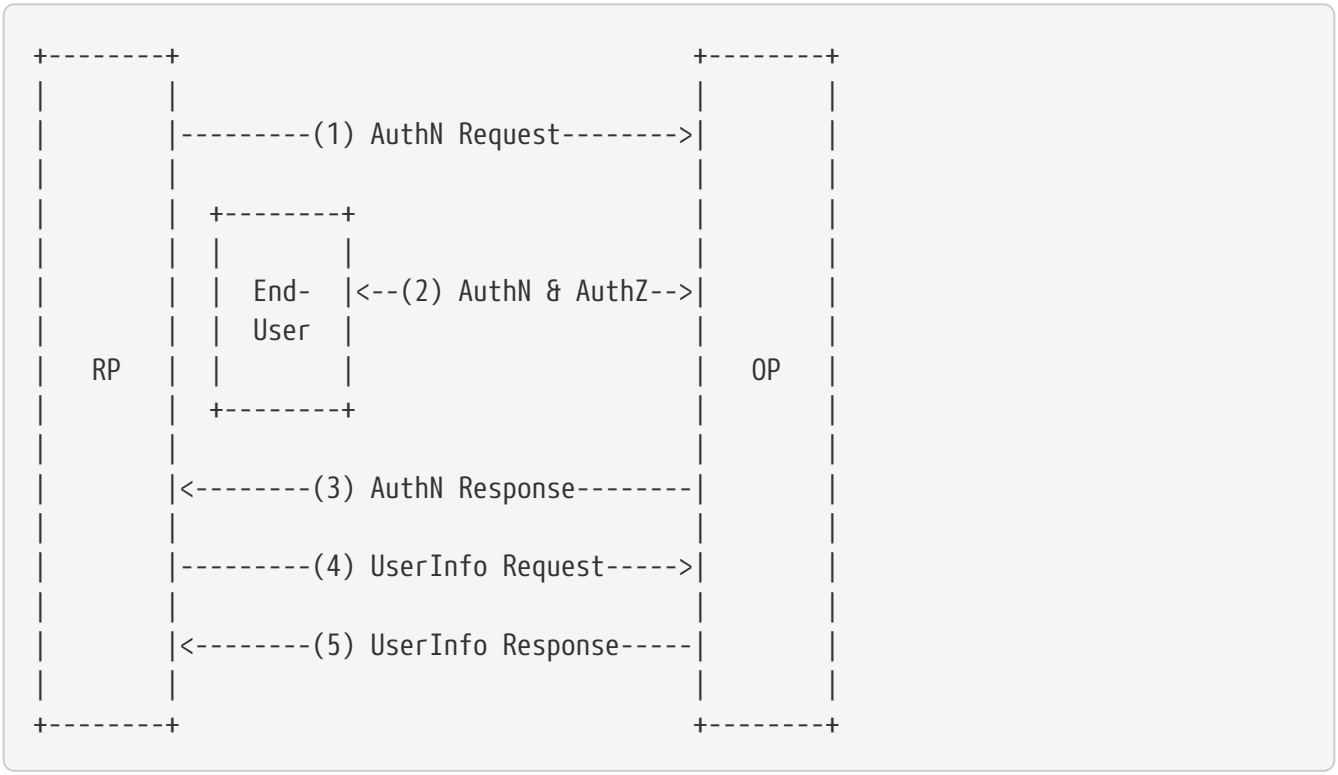
### 5.2.1. OpenID overview

**Note: The following chapter contains material from the OpenID Connect Basic Client Implementer's Guide 1.0 [https://openid.net/specs/openid-connect-basic-1_0.html].**

The OpenID Connect protocol, in abstract, follows the following steps.

- The RP (Client) sends a request to the OpenID Provider (OP).
- The OP authenticates the End-User and obtains authorization.
- The OP responds with an ID Token and usually an Access Token.
- The RP can send a request with the Access Token to the UserInfo Endpoint.
- The UserInfo Endpoint returns Claims about the End-User.

These steps are illustrated in the following diagram:




The way this authentication loop is implemented is described below.

### 5.2.2. Implementation in Testbed-14

The IdP is a WSO2 Identity Server provided by ATOS CVC and hosted on eocloud.eu [https://eodata-iam.user.eocloud.eu:8080/carbon/admin/login.jsp]

Two users are defined within the IdP specifically for OGC Testbed-14:

- Alice (username: "alice@ogctestbed14.com [mailto:alice@ogctestbed14.com]") is an "Application Developer"
- Bob (username: "bob@ogctestbed14.com [mailto:bob@ogctestbed14.com]") is an "Application Consumer"

The Web Client is developed by Solenix. It uses angular-oauth2-oidc module [https://github.com/manfredsteyer/angular-oauth2-oidc] configured for OIDC Implicit Flow. Essentially the user is redirected to a login page on the ATOS server and then back to Solenix's server after logging in - the redirect back includes the "access_token" which we can then use as required (eg. as a header in subsequent requests).

The "access_token" retrieval can be mimicked through curl

```
curl -k -d
"grant_type=password&username=alice%40ogctestbed14.com&password=YYYYYYYYYY&scope=openi
d" \
     -H "Authorization: Basic XXXXXXXXXX" \
     -H "Content-Type: application/x-www-form-urlencoded" \
     https://eodata-iam.user.eocloud.eu:8080/oauth2/token
```

Where :

- YYYYYYYYYY is Alice's password
- XXXXXXXXXX is the base64 encoding of the concatenation of the *clientId:clientSecret* Web Client identifiers provided by the IdP during Web Client application registration.

```
{
    "access_token":"The4cc3ssTok3nForAlice",
    "refresh_token":"b865eec5-6b07-326d-8dc6-ffc828116f52",
    "scope":"openid",

"id_token":"eyJ4NXQiOiJaV013WVdOa09URmlaREE1TXpNNFpETm1aREV5TlRRMU1ETXlZakV4WVRneE9EY3
lOemRoTlEiLCJraWQiOiJaV013WVdOa09URmlaREE1TXpNNFpETm1aREV5TlRRMU1ETXlZakV4WVRneE9EY3lO
emRoTlEiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiJScE56ODNzbl9OZW9zM2FxekE0N1pyQk00YUFhIiwic3ViI
joiYWxpY2VAb2djdGVzdGJlZDE0LmNvbSIsImF6cCI6IlJwTno4M3NuX05lb3MzYXF6QTQ3WnJCTTRhQWEiLCJ
hbXIiOlsicGFzc3dvcmQiXSwiaXNzIjoiaHR0cHM6XC9cL2VvZGF0YS1pYW0udXNlci5lb2Nsb3VkLmV1OjgwO
DBcL29hdXRoMlwvdG9rZW4iLCJleHAiOjE1NDI2NzI5ODcsImlhdCI6MTUzOTA3Mjk4N30.hfvlulTVyVZXXFK
MxvVpGhK8qHv_ojim06dXXSH9WWC5K261aVDtGDu8OeMXkWwYe1cXOt6-kqOq1ESaVl_8NiRxFJqIAF-
lMu5uv99rXb3mEeIs-
iCcePn1b71CL81fgl54cAqE5dl0kwm4uEJu6e051cfsIATUEGWMfYD3XmFn6TbFLmMopOQqQx0PwEP97WX9t_L
xh73wv3oxFCsJaXlEw6L-HdT2u4IN9epIRY9pRowZJHy-
rsK1PgCo_TZpEO41XN9s38RHo0ffD5ARQj7kFXhHsioO_BO5q5HN_vgXo1SNomVoqjZ4Tf4BLiw72OFiIsWDmM
VvS-LUrQZckw",
    "token_type":"Bearer",
    "expires_in":3600
}
```


### 5.2.3. Note on access token expiration

You will have noted from the token retrieval response that the *access_token* has a limited validity in time. The *expires_in* property indicates the number of seconds from the *access_token* issuing until it becomes invalid. In the previous example, the *access_token* validity duration is set to 1 hour (3600 seconds).

Hence a fresh *access_token* with an identical scope can be obtained from a valid and non-expired *access_token* using the *refresh_token* provided within the token retrieval response.

However, in Testbed-14, the EMS/ADES only receive an *access_token* from the Web Client requests. These components have no way to refresh the *access_token* if it appears to expire during the lifetime of a workflow for instance.

Thus, the Web Client should update the *access_token* on a regular basis to ensure that request sent to the EMS/ADES does not provide an *access_token* close to the expiration date.

This is clearly a concern if the *access_token* expires during a workflow execution. We consider that this concern should be addressed in future work.

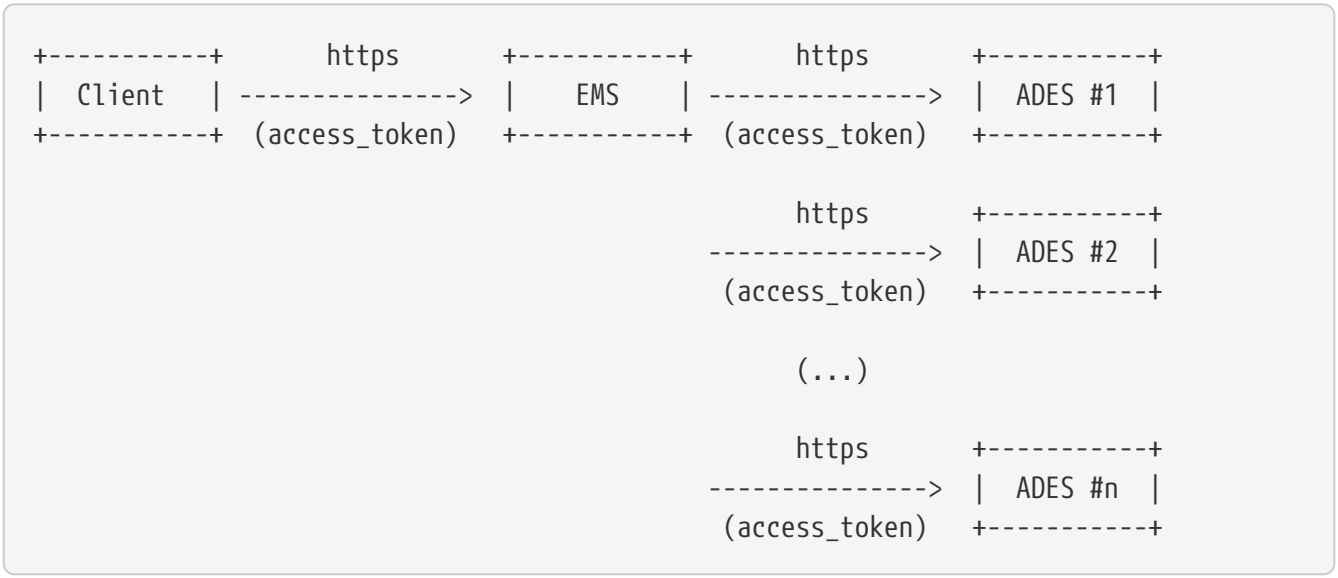
## 5.3. Authorization

On successful End User authentication, the Web Client stores the access_token. The access_token that is provided for each request is issued from the Client to the resource server (i.e. EMS) and propagated in a subsequent request (i.e. from EMS to ADES).

From a security point of view, the access_token credentials must be kept confidential in transit and storage, and only shared among the Web Client, the IdP and the EMS/ADES. Indeed, anyone in

possession of a valid access_token can get the corresponding user's profile without any verification.

As a consequence, to minimize the risk of exposing the access_token, all exchange between the Web Client, the IdP and the EMS/ADES must use the **https** protocol.




### 5.3.1. From Client to resource server

Client should make authenticated requests by providing the access_token using the "Authorization" request header field defined by HTTP/1.1 [RFC2617] with the "Bearer" HTTP authorization scheme. The resource servers (i.e. EMS, ADES) must support this method.

The following is an example of an authenticated request from the Client to the Resource server using curl:

```
    curl -X GET -i "http://tbd14.geomatys.com/examind/WS/wps/default" -H
"Authorization: Bearer The4cc3ssTok3nForAlice"
```

**Note:** The resource server should return a 401 (Unauthorized) status code when receiving a request with missing "Authorization" request header.

### 5.3.2. From resource server to IdP

Upon reception of an authenticated request, the Resource server sends a request to the UserInfo Endpoint of the IdP to obtain Claims about the End-User using the access_token obtained through the Client incoming request. The UserInfo Endpoint is an OAuth 2.0 [RFC 6749] Protected Resource that complies with the OAuth 2.0 Bearer Token Usage [RFC 6750] specification. The request must use the HTTP GET method and the access_token must be sent using the "Authorization" header field.

The following is an example of a userInfo Request sent by EMS/ADES to the IdP using curl:

```
curl -H "Authorization: Bearer The4cc3ssTok3nForAlice" \
        "https://eodata-iam.user.eocloud.eu:8080/oauth2/userinfo?schema=openid"
```

The response returns the user profile. The "sub" property contains the user's unique identifier (in Testbed14 the user's identifier is an email address):

```
{
    "sub":"alice@ogctestbed14.com",
    "eduPersonAffiliation":"member,staff",
    "name":"alice@ogctestbed14.com",
    "given_name":"Alice",
    "family_name":"OGCTestbed",
    "email":"alice@ogctestbed14.com"
}
```

### 5.3.3. Check user rights

The user's rights to access resources on EMS/ADES is based on the user's roles set within the *eduPersonAffiliation* attribute.

The *eduPersonAffiliation* contains a comma separated list of roles. Each role corresponds to a specific right on EMS/ADES:

- "member" role can execute processes on EMS/ADES and deploy process on ADES
- "staff" role can deploy processes on EMS/ADES

Upon reception of the user's profile, the EMS/ADES infers user's rights from *eduPersonAffiliation* attribute. If the user has rights to execute the request, then normal processing continue. Otherwise, the resource server should return an HTTP response with 403 (Forbidden) status error.

In the previous example, Alice's roles are "member,staff" which means that Alice can both deploy and execute processes on EMS/ADS.

## 5.4. Discussion on process deployment on ADES

In the initial scenario, Alice can deploy a process and Bob can only execute the process. Once Alice deploys her process, the process is effectively deployed on EMS and is made available for Bob.

When Bob launches a job to execute the process, the EMS decides on which MEP(s) the process should be executed deploys an ADES accordingly. This raises an authorization issue: to deploys ADES on MEPs, EMS must provide a user's access_token that give rights to deploy process on ADES. Since the execute request is sent by Bob, the EMS has access to the access_token from Bob and not from Alice.

To solve this issue, we are considering two solutions:

- We give Bob the right to deploy process on ADES
- We introduce an "ems user" associated to EMS. This user can deploy process on ADES. Each requests from EMS to ADES uses the credentials of this user instead of the real user (i.e. Alice or Bob)

In the previous example, we choose the first solution i.e. as "member", Bob can deploy on ADES. However, this discussion is not closed and could be adressed in future work.

# Chapter 6. Quotation

## 6.1. Context

Usually processing platforms provide pay-per-use services where customers are charged when they use the service. Thus, in the case of processing services, it may be interesting to have an estimate of the cost of processing before it is launched.

The quotation model has been discussed for that reason. Prior to executing a process, a user asks the resource server (e.g. EMS) for a quotation. The quotation service takes the same input as the corresponding execute service – basically it's like executing the process without actually executing it.

Upon reception of a quotation request, the EMS analyzes the request and subsequently propagates it to all ADES that would be involved in the final processing request. Finally, the EMS aggregates the quotation results from all ADES and provides to the user a consolidated quotation result based on the sum of ADES quotations results (including eventually an overhead from EMS itself).

Optionally, the quotation results can contain alternative quotations to the default quotation. For instance, these quotations can propose different prices based on different Quality-of-Service (lower or higher processing time, etc.).

### 6.1.1. Disclaimer

Although cost estimate computation is out of the scope of this testbed, it is important to note that such computation is not straightforward. Roughly the cost is based on the number of pixels processed and on the complexity to process each pixel.

For the NDVIMultiSensor process, the number of pixels can be easily estimated from the number, the footprint (i.e. area), the resolution and the format (compressed or not) of input images. However for the NDVIStacker it is more difficult to estimate the number of pixels involved to produce the mosaic unless you compute the various intersections between the input images and decide which pixels are best suited to produce the overall result. Moreover, in the context of a workflow, it is virtually impossible to make a quotation request to the involved ADES for downstream processes since their inputs are unknown without first executing the upstream process. To get a quote from the downstream processes we would need a quote request that is not based on the inputs like an approximation from previous executions.

The relevance of the cost estimate should be addressed in future work

## 6.2. Overview

The sequence diagram below presents an overview of the quotation process call.

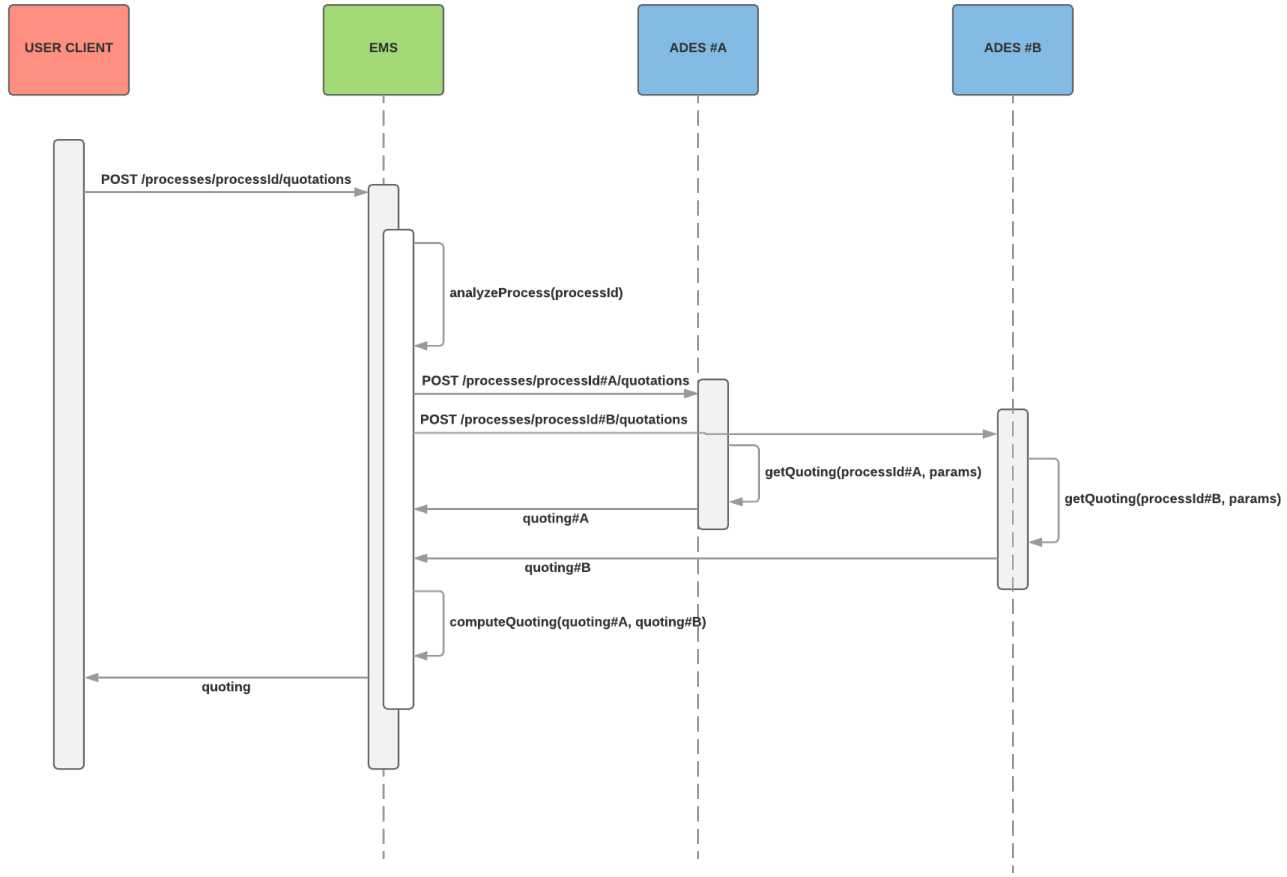



*Figure 2. General Sequence Diagram of quotation process*

## 6.3. List of services

Each resource server (EMS and ADES) that conforms to the quotation service should provide the endpoints described in this chapter.

A full description of these endpoints is available within the ADES WPS-T OpenAPI description [https://github.com/opengeospatial/D009-ADES_and_EMS_Results_and_Best_Practices_Engineering_Report/blob/master/code/ades_wpst.json].

### 6.3.1. Request a quotation

The quotation request is per process. The body is the same as the execute request.

```
POST /processes/{id}/quotations
```

On success, this request should return an HTTP 201 response including the url to the quotation resource

### 6.3.2. Execute a quoted process

A previously quoted process can be executed directly from the *quotationID*. The two endpoints are equivalents. The first endpoint follows the convention of the other WPS-T endpoints (e.g. /processes/{id}/jobs/{jobId}). However from the *quotationID* alone this URL cannot be built. That is

why the second endpoint is specified, allowing a client to request quotation information through the *quotationID* only.

```
POST /processes/{id}/quotations/{quotationID}
POST /quotations/{quotationID}
```

### 6.3.3. Retrieve quotation information

The two endpoints are equivalents for the same reasons expressed above.

```
GET /processes/{id}/quotations/{quotationID}
GET /quotations/{id}
```

On success, this request should return an HTTP 200 response including the quotation. The quotation model is described in the following tables.

**quotation**

| Name | Description | Schema |
|---|---|---|
| **alternativeQuotations** *optional* | | < alternateQuotation > array |
| **created** *required* | The date and time (ISO 8601 format) when the quotation was created | string (date-time) |
| **currency** *required* | Currency code in ISO 4217 format | string |
| **description** *optional* | A description of what the quotation is related | string |
| **details** *optional* | | string |
| **estimatedTime** *optional* | The estimated duration for the process to be performed (in ISO 8601 duration format) | string |
| **expire** *required* | The date and time (ISO 8601 format) when the quotation will expire | string (date-time) |
| **id** *required* | The id of the quotation | string |

| Name | Description | Schema |
| --- | --- | --- |
| **price**<br>*required* | | number (double) |
| **processId**<br>*required* | The id of the parent process | string |
| **processParameters**<br>*required* | | Execute parameters (see ADES WPS-T OpenAPI description [https://github.com/opengeospatial/D009-ADES_and_EMS_Results_and_Best_Practices_Engineering_Report/blob/master/code/ades_wpst.json]) |
| **status**<br>*required* | | enum (running, completed, failed) |
| **title**<br>*optional* | A name of the quotation | string |
| **userId**<br>*required* | User id that requested this quotation | string |

**alternateQuotation**

| Name | Description | Schema |
| --- | --- | --- |
| **created**<br>*required* | The date and time (ISO 8601 format) when the quotation was created | string (date-time) |
| **currency**<br>*required* | Currency code in ISO 4217 format | string |
| **description**<br>*optional* | The description of what the quotation is related to | string |
| **details**<br>*optional* | | string |

| Name | Description | Schema |
|---|---|---|
| **estimatedTime**<br>*optional* | The estimated duration for the process to be performed (in ISO 8601 duration format) | string |
| **expire**<br>*required* | The date and time (ISO 8601 format) when the quotation will expire | string (date-time) |
| **id**<br>*required* | The id of the quotation | string |
| **price**<br>*required* | | number (double) |
| **title**<br>*optional* | The name of the quotation | string |

### 6.3.4. Retrieve the list of all quotation ids

This endpoint returns all of the user's quotations as a list.

```
GET /quotations
```

### 6.3.5. quotationList

| Name | Schema |
|---|---|
| **quotations**<br>*optional* | < string > array |

## 6.4. Step by step example

In the following, we suppose that Bob is authenticated and get a valid Access Token aka *Th34cc3ssTok3nForBob*.

- Bob performs a Getcapabilities on the EMS

```
curl -X GET \
     -i "http://tbd14.geomatys.com/examind/WS/wps/ems/processes" \
     -H "Authorization: Bearer Th34cc3ssTok3nForBob"
```

- Bob receives the list of available processes

*Listing listProcessResponse (JSON)*


```
{
  "processes": [
    {
      "id": "NDVIMultiSensor",
      "title": "Multi Sensor NDVI",
      "abstract": "NDVI is calculated after the two bands values Near Infrared and
red. It is calculated by this formula : NDVI = (NIR-Red)/(NIR+Red)",
      "version": "1.0.0",
      "jobControlOptions": [
        "async-execute"
      ],
      "processDescriptionURL":
"http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor"
    }
  ]
}
```


- Bob chooses *NDVIMultiSensor* and performs a DescribeProcess

```
curl -X GET \
     -i "http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor" \
     -H "Authorization: Bearer Th34cc3ssTok3nForBob"
```

- Bob gets the process description

*Listing describeProcessResponse (JSON)*


```
{
  "process": {
    "id": "NDVIMultiSensor",
    "title": "NDVIMultiSensor",
    "keywords": [
      "NDVI"
    ],
    "owsContext": {
      "offering": {
        "code": "http://www.opengis.net/eoc/applicationContext/cwl",
        "content": {
          "href":
"https://raw.githubusercontent.com/Geomatys/Testbed14/master/application-
packages/NDVIMultiSensor/NDVIMultiSensor.cwl"
        }
      }
    },
    "inputs": [
      {
        "id": "StartDate",
```

```
      "title": "Time of Interest",
      "formats": [
        {
          "mimeType": "text/plain",
          "default": true
        }
      ],
      "minOccurs": "1",
      "maxOccurs": "1",
      "additionalParameters": [
        {
          "parameters": [
            {
              "name": "CatalogSearchField",
              "values": ["startDate"]
            }
          ]
        }
      ],
      "abstract": "Time of Interest (defined as Start date - End date)",
      "LiteralDataDomain": {
        "dataType": {
          "name": "String"
        }
      }
    },
    {
      "id": "EndDate",
      "title": "Time of Interest",
      "formats": [
        {
          "mimeType": "text/plain",
          "default": true
        }
      ],
      "minOccurs": "1",
      "maxOccurs": "1",
      "additionalParameters": [
        {
          "parameters": [
            {
              "name": "CatalogSearchField",
              "values": ["endDate"]
            }
          ]
        }
      ],
      "abstract": "Time of Interest (defined as Start date - End date)",
      "LiteralDataDomain": {
        "dataType": {
          "name": "String"
```

```
        }
      }
    },
    {
      "id": "aoi",
      "title": "Area of Interest",
      "formats": [
        {
          "mimeType": "OGC-WKT",
          "default": true
        }
      ],
      "minOccurs": "1",
      "maxOccurs": "1",
      "additionalParameters": [
        {
          "parameters": [
            {
              "name": "CatalogSearchField",
              "values": ["bbox"]
            }
          ]
        }
      ],
      "abstract": "Area of Interest (Bounding Box)"
    },
    {
      "id": "collection",
      "title": "Collection of the data.",
      "formats": [
        {
          "mimeType": "text/plain",
          "default": true
        }
      ],
      "minOccurs": "1",
      "maxOccurs": "1",
      "additionalParameters": [
        {
          "parameters": [
            {
              "name": "CatalogSearchField",
              "values": ["parentIdentifier"]
            }
          ]
        }
      ],
      "abstract": "Collection",
      "LiteralDataDomain": {
        "dataType": {
          "name": "String"
```

```
          }
        }
      }
    ],
    "outputs": [
      {
        "id": "output",
        "title": "NDVI Images",
        "formats": [
          {
            "mimeType": "application/octet-stream",
            "default": true
          }
        ]
      }
    ],
    "executeEndpoint":
"http://tbd14.geomatys.com/WS/wps/default/processes/NDVIMultiSensor/jobs",
    "abstract": "Normalized Difference Vegetation Index (NDVI) from an input list of
satellite images."
  },
  "processVersion": "1.0.0",
  "jobControlOptions": [
    "async-execute"
  ],
  "outputTransmission": [
    "reference"
  ]
}
```

- Bob sends a quotation request - this request is **asynchronous**

```
  curl -X POST \
       -i
"http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor/quotations" \
       -H "Authorization: Bearer Th34cc3ssTok3nForBob"
       -d "@3-quoteProcessRequest.json"
```

With the following POST data

*Listing quoteProcessRequest (JSON)*

```
{
  "inputs": [
    {
      "id": "StartDate",
      "data": "2016-05-05T04:11:00Z"
    },
    {
      "id": "aoi",
      "data": "POLYGON((120 -10,155 -10,155 -30,120 -30))"
    },
    {
      "id": "collection",
      "data": "EOP:VITO:PDF:urn:ogc:def:EOP:VITO:PROBAV_P_V001"
    },
    {
      "id": "EndDate",
      "data": "2016-05-06T00:00:00Z"
    }
  ],
  "outputs": [
    {
      "id": "output",
      "transmissionMode": "reference"
    }
  ]
}
```

The response is an HTTP 201 "Created" with a *Location* property containing the url to the getQuotation endpoint

```
HTTP/1.1 201
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Origin, access_token, X-Requested-With, Content-Type,
Accept
Access-Control-Allow-Credentials: true
Location:
http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor/quotations/6c6a
dacb-dd42-4816-8e89-787d1e095fec
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Content-Length: 0
Date: Wed, 26 Sep 2018 08:44:12 GMT
```

- Bob get the quotation result from *Location* url

```
  curl -X GET \
       -i
"http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor/quotations/6c6
adacb-dd42-4816-8e89-787d1e095fec"
```

The quotation is considered as completed when the *status* property is set to "complete". Otherwise the quotation process is not finished and the request must be sent again (i.e. polling strategy)

*Listing quoteProcessResponse (JSON)*


```
{
  "id": "6c6adacb-dd42-4816-8e89-787d1e095fec",
  "title": "NDVIMultiSensor",
  "description": "Normalized Difference Vegetation Index (NDVI) from an input list of
satellite images.",
  "processId": "NDVIMultiSensor",
  "status": "completed",
  "price": 10.72,
  "currency": "EUR",
  "expire": "2018-10-18T02:42:355Z",
  "created": "2018-10-11T02:42:355Z",
  "details": "Basic price 10 euros. - input file 66mo : 0.07euros. - input file 651mo
: 0.65euros. Total: 10.72 euros.",
  "estimatedTime": "PT1M7.17S",
  "processParameters": {
    "inputs": [
      {
        "id": "StartDate",
        "data": "2016-05-05T04:11:00Z"
      },
      {
        "id": "aoi",
        "data": "POLYGON((120 -10,155 -10,155 -30,120 -30))"
      },
      {
        "id": "collection",
        "data": "EOP:VITO:PDF:urn:ogc:def:EOP:VITO:PROBAV_P_V001"
      },
      {
        "id": "EndDate",
        "data": "2016-05-06T00:00:00Z"
      }
    ],
    "outputs": [
      {
        "id": "output",
        "transmissionMode": "reference"
      }
    ]
  }
}
```

# Chapter 7. Billing

## 7.1. Context

Billing is very specific to each platform. Therefore the scope of this chapter is limited to the association of a bill identifier to a processing result and considers the relationship between billing and quotation.

On the latter, it would seem legitimate that the price displayed on the bill would be the same as the price provided during the quotation process. From the discussion on the cost estimate in the previous chapter, the billing should not be based on the real use of each platform but on the estimated use of each platform computed during the quotation task.

## 7.2. List of services

Each resource server (EMS and ADES) that conforms to the billing service should provide the endpoints described in this chapter.

A full description of these services is available within the ADES WPS-T OpenAPI description [https://github.com/opengeospatial/D009-ADES_and_EMS_Results_and_Best_Practices_Engineering_Report/blob/master/code/ades_wpst.json].

### 7.2.1. Retrieve bill information

The billID should be returned within the getResult response as an **hypermedia link** to the following service.

```
GET /bills/{billID}
```

On success, this request should return an HTTP 200 response including the bill. The bill model is described in the following table.

### 7.2.2. bill

| Name | Description | Schema |
|---|---|---|
| **created** *required* | The date and time (ISO 8601 format) when the bill was created | string (date-time) |
| **currency** *required* | Currency code in ISO 4217 format | string |
| **description** *optional* | A description of what is charged | string |

| Name | Description | Schema |
|---|---|---|
| **id** *required* | The id of the bill | string |
| **price** *required* | | number (double) |
| **quotationId** *optional* | Reference to the quotation id corresponding to this bill | string |
| **title** *required* | The name of the bill | string |
| **userId** *required* | User id that is charged for this bill | string |

### 7.2.3. Retrieve the list of all bills ids

This endpoint returns all of the user's bills as a list.

```
GET /bills
```

### 7.2.4. billList

| Name | Schema |
|---|---|
| **bills** *optional* | < string > array |

## 7.3. Step by step example

- Following the quotation request, Bob decides to execute the process based on the quotationID

```
curl -X POST \
     -i
"http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor/quotations/6c6
adacb-dd42-4816-8e89-787d1e095fec" \
      -H "Authorization: Bearer Th34cc3ssTok3nForBob"
```

The response is an empty HTTP 201 "Created" with a *Location* property containing the url to the getStatus endpoint

```
HTTP/1.1 201
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Origin, access_token, X-Requested-With, Content-Type,
Accept
Access-Control-Allow-Credentials: true
Location:
http://tbd14.geomatys.com/WS/wps/default/processes/NDVIMultiSensor/jobs/5135fbdb-b668-
441b-afed-d8d5cd57e9bc
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Content-Length: 0
Date: Wed, 26 Sep 2018 08:44:12 GMT
```

- Once the job is finished, Bob retrieves the result using the *Location* url

```
  curl -X POST \
       -i
"http://tbd14.geomatys.com/examind/WS/wps/ems/processes/NDVIMultiSensor/jobs/5135fbdb-
b668-441b-afed-d8d5cd57e9bc/result" \
       -H "Authorization: Bearer Th34cc3ssTok3nForBob"
```

With the following result .Listing executeProcessResponse (JSON)

```
{
  "outputs": [
    {
      "id": "output",
      "value": "http://tbd14.geomatys.com/examind/WS/wps/webdav/f57d319c-b0d1-481a-
a2b4-b30c2d957518-results/7b440d6c-3dd2-41fe-a2fa-c72d808b0ce1.tif"
    },
    {
      "id": "output",
      "value": "http://tbd14.geomatys.com/examind/WS/wps/webdav/f57d319c-b0d1-481a-
a2b4-b30c2d957518-results/e754c998-a83b-47f0-8234-bef598dfffd4.tif"
    }
  ],
  "links": [
    {
      "href": "http://tbd14.geomatys.com/examind/WS/wps/ems/bills/ed7a944b-9b8c-4664-
baf0-b8a0e175c2ce",
      "rel": "bill",
      "type": "application/json",
      "title": "Associated Bill"
    }
  ]
}
```


The url to the bill for this job is provided as an hypermedia link with rel="bill"

- Bob get the bill from the hypermedia link retrieved within the result

```
  curl -X GET \
       -i "http://tbd14.geomatys.com/examind/WS/wps/ems/bills/ed7a944b-9b8c-4664-baf0-
b8a0e175c2ce" \
       -H "Authorization: Bearer Th34cc3ssTok3nForBob"
```

with the following result

*Listing getBillResponse (JSON)*


```
{
  "id": "ed7a944b-9b8c-4664-baf0-b8a0e175c2ce",
  "title": "NDVIMultiSensor",
  "description": "Normalized Difference Vegetation Index (NDVI) from an input list of
satellite images.",
  "price": 10.72,
  "currency": "EUR",
  "created": "2018-10-12T08:12:965Z"
}
```

# Chapter 8. Identity Provider EndPoints

Below is a list of useful OpenID/oauth2 endpoints provided by the IdP

- Authorization Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/authorize]
- Token Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/token]
- Token Revocation Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/revoke]
- Token Introspection Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/introspect]
- User Info Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/userinfo]
- Session IFrame Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oidc/checksession]
- Logout Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oidc/logout]
- JWKS Endpoint URL [https://eodata-iam.user.eocloud.eu:8080/oauth2/jwks]

# Appendix A: Revision History

*Table 1. Revision History*

| Date | Editor | Release | Primary clauses modified | Descriptions |
|---|---|---|---|---|
| October 25, 2018 | J. Gasperi | 1.0 rc1 | all | Include feedbacks |
| October 11, 2018 | J. Gasperi | 0.9 | all | First public draft |
| July 2, 2018 | J. Gasperi | 0.1 | all | Initial version |

# Appendix B: Bibliography