



# ZCREQUEST - IBM z/OS Connect

## An introduction to API Requesters

API Requester Code and Security Considerations

Mitch Johnson

[mitchj@us.ibm.com](mailto:mitchj@us.ibm.com)

Washington System Center



# Notes and Disclaimers



- The information in this presentation was derived from various product documentation web sites.
- Additional information included in this presentation was distilled from years of experience implementing security using RACF with z/OS products like CICS, IMS, Db2, MQ, etc. as well as Java runtimes environments like WebSphere Application Server and WebSphere Application Server Liberty which is commonly called Liberty.
- There will be additional information on slides that will be designated as Tech/Tips. These contain information that at perhaps at least interesting and hopefully, useful to the reader.
- The examples, tips, etc. present in this material are based on firsthand experiences and are not necessarily sanctioned by Liberty or z/OS Connect product areas.

# **z/OS Connect Wildfire Github Site** <https://ibm.biz/zCEEWorkshopMaterial>



The image displays three GitHub repository pages related to z/OS Connect Wildfire workshops:

- ibm-wsc / zCONNEE-Wildfire-Workshop (Public)**: This page shows a list of files uploaded by user emitchj. A red oval highlights the "ZCREQUEST - Introduction to zOS Co..." file.
- ibm-wsc / zCONNEE-Wildfire-Workshop (Public)**: This page shows a list of files uploaded by user emitchj under the "OpenAPI2" directory. A red oval highlights the "Developing CICS API Requester Applications.pdf", "Developing IMS API Requester Applications.pdf", and "Developing MVS Batch API Requester Applications.pdf" files.
- ibm-wsc / zCONNEE-Wildfire-Workshop (Public)**: This page shows a list of files uploaded by user emitchj under the "APIRequesters" directory. A red oval highlights the same three PDF files: "Developing CICS API Requester Applications.pdf", "Developing IMS API Requester Applications.pdf", and "Developing MVS Batch API Requester Applications.pdf".

**ibm-wsc / zCONNEE-Wildfire-Workshop (Public)**

**Code** Issues Pull requests Actions Projects Wiki Security Insights Settings

master zCONNEE-Wildfire-Workshop / OpenAPI2 /

emitchj Delete Developing d880029 on Apr 23 History

..

Developing CICS API Requester Applications.pdf Add files via upload 2 months ago

Developing IMS API Requester Applications.pdf Add files via upload 2 months ago

Developing MVS Batch API Requester Applications.pdf Add files via upload 2 months ago

3 months ago 15 watching

**ibm-wsc / zCONNEE-Wildfire-Workshop (Public)**

**Code** Issues Pull requests Actions Projects Wiki Security Insights

master zCONNEE-Wildfire-Workshop / APIRequesters /

emitchj Add files via upload 428fc6c 5 days ago History

..

Developing CICS API Requester Applications.pdf Add files via upload 5 days ago

Developing IMS API Requester Applications.pdf Add files via upload 5 days ago

Developing MVS Batch API Requester Applications.pdf Add files via upload 5 days ago

5 days ago

This repository contains material from the z/OS Connect EE Wildfire workshops run by the IBM Center. It is should be referenced frequently for updates to the presentations, exercises, samples, and other materials.

- Contact your IBM representative to schedule access to these exercises

# **/first, what\_is\_a\_REST\_API?**



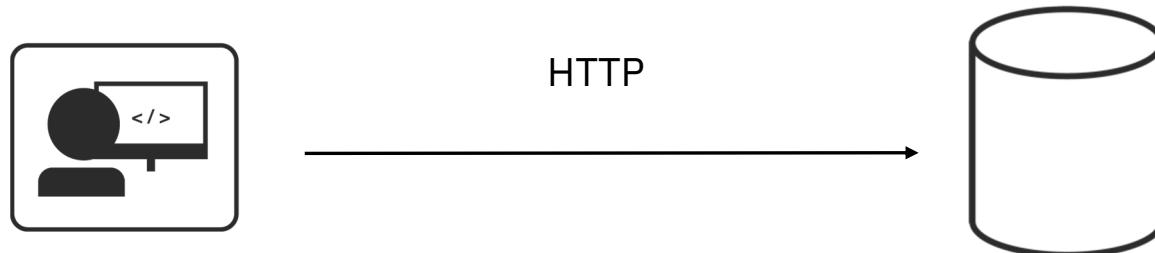
# REST is architectural programming style

**REST** stands for **R**epresentational **S**tate **T**ransfer.

An architectural programming style for **accessing** and **updating** data over the internet.

Typically using HTTP... but not all HTTP interfaces are “RESTful”.

Simple and intuitive for the end consumer (**the developer**).



Roy Fielding defined REST in his 2000 PhD dissertation "Architectural Styles and the Design of Network-based Software Architectures" at UC Irvine. He developed the REST architectural style in parallel with HTTP 1.1 of 1996-1999, based on the existing design of HTTP 1.0 of 1996.



# Key Principles of REST

Use HTTP verbs for Create, Read, Update, Delete (CRUD) operations

POST  
GET  
PUT  
DELETE

`http://<host>:<port>/path/parameter?name=value&name=value`

Use Path and Query parameters to refine the request

URI path identifies a resource (or lists of resources)

URL identifies the protocol, host and port and includes the URI Path

Request/Response Body is used to represent the data object

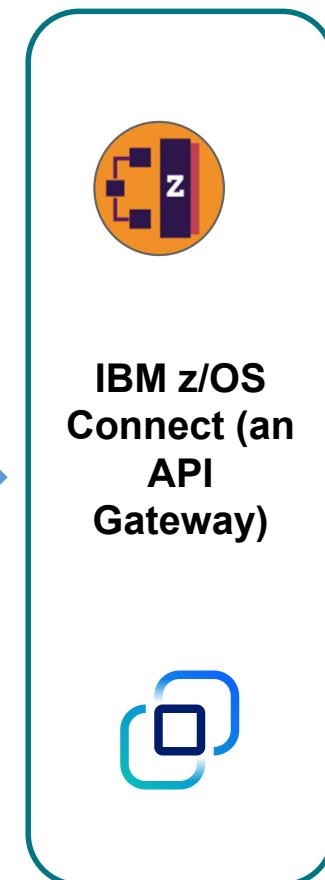
```
GET http://www.acme.com/customers/12345?personalDetails=true
RESPONSE: HTTP 200 OK
BODY { "id" : 12345
      "name" : "Joe Bloggs",
      "address" : "10 Old Street",
      "tel" : "01234 123456",
      "dateOfBirth" : "01/01/1980",
      "maritalStatus" : "married",
      "partner" : "http://www.acme.com/customers/12346" }
```



# Why is REST popular?

<b>Ubiquitous Foundation</b>	It's based on HTTP, which operates on TCP/IP, which is a ubiquitous networking topology.
<b>Relatively Lightweight</b>	Compared to other technologies (for example, SOAP/WSDL), the REST/JSON pattern is relatively light protocol and data model, which maps well to resource-limited devices.
<b>Relatively Easy Development</b>	Since the REST interface is so simple, developing the client involves very few things: an understanding of the URI requirements (path, parameters) and any JSON data schema.
<b>Increasingly Common</b>	REST/JSON is becoming more and more a de facto "standard" for exposing APIs and Microservices. As more adopt the integration pattern, the more others become interested.
<b>Stateless</b>	REST is by definition a stateless protocol, which implies greater simplicity in topology design. There's no need to maintain, replicate or route based on state.

# **z/OS Connect EE exposes z/OS resources to applications in the “cloud” via RESTful APIs**

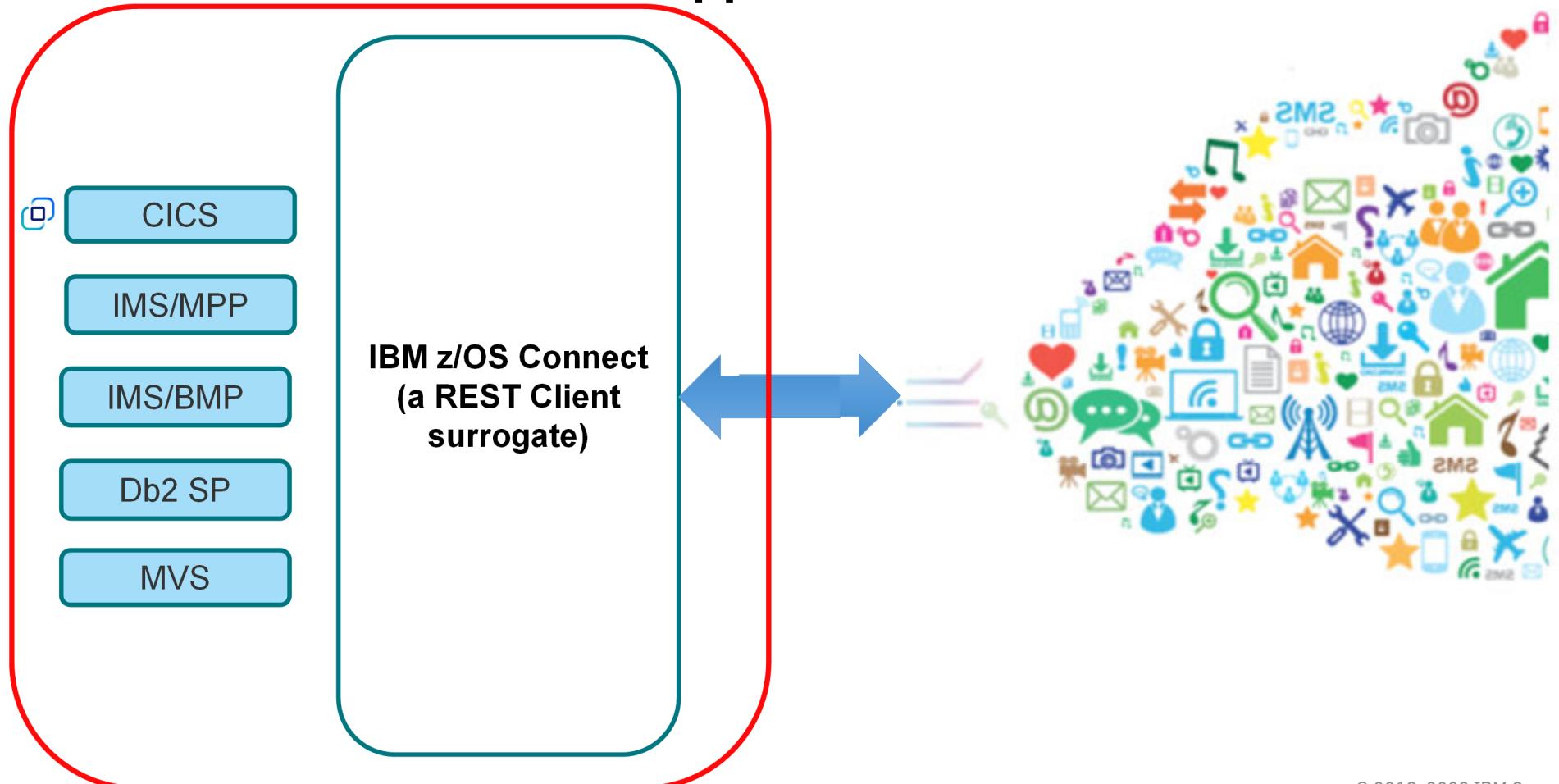


+ HCL and Rocket Software

\*Other Vendors or your own implementation



## **z/OS Connect EE exposes external REST APIs in the “cloud” to z/OS COBOL applications**



# How do we describe a REST API?



## /oai/open\_api\_initiative

The industry standard framework for describing REST APIs

The OpenAPI Initiative (OAI) was created by a consortium of forward-looking industry experts who recognize the immense value of standardizing on how APIs are described. As an open governance structure under the Linux Foundation, the OAI is focused on creating, evolving and promoting a vendor neutral description format. The OpenAPI Specification was originally based on the Swagger Specification, donated by SmartBear Software.



# Why use OpenAPI?

- It is more than just an API framework



There are a number of tools available to aid consumption:

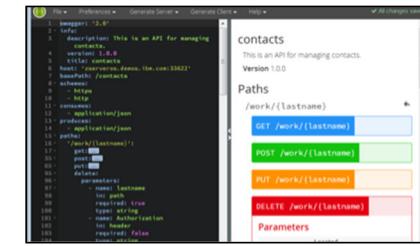
**Code Generation\*** - create stub code to consume APIs from various languages



**Test UIs** - allows API consumers to easily browse and try APIs based on an OpenAPI document.



**Editors** - allows API developers to design their OpenAPI documents.



\* z/OS Connect API Requester

+z/OS Connect, MQ REST support, Zowe

**Important** - You may have used or heard of the term Swagger with the use of APIs. As the use of APIs has grown this term has become in some respects misleading. To be more precise, OpenAPI refers to the API specifications (OpenAPI 2 and OpenAPI3) where Swagger refers to the tooling used to implement the specifications.



# Tech-Tip: Swagger (OpenAPI 2) Specification Example

The image displays two side-by-side browser windows showing the Swagger (OpenAPI 2) specification for a Miniloan API.

**Left Window (Request Message):**

- Base URI Path:** Circled in red, showing `basePath: "/miniloan"`.
- URI Path extension/method:** Circled in red, showing the path `/loan/post`.
- Request message:** Circled in red, showing the parameters and schema for the `post` method.

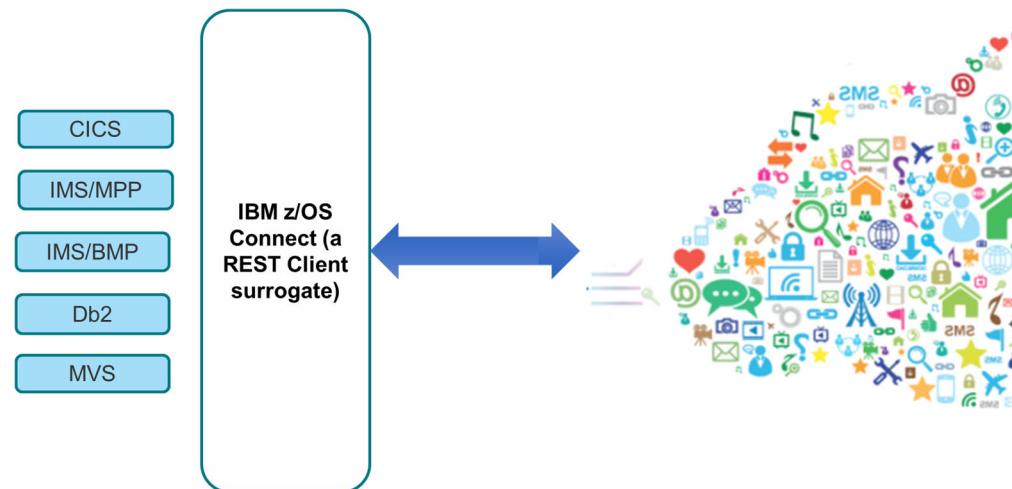
**Right Window (Response Message Layout):**

- Response message layout:** Circled in red, showing the schema for the `postMiniloanService\_response\_200` response.
- Response message fields:** A large red circle encompasses the properties of the `MINILOAN\_COMMAREA` schema, including `name`, `creditscore`, `yearlyIncome`, `age`, `amount`, `effectiveDate`, and `yearlyRepayment`.



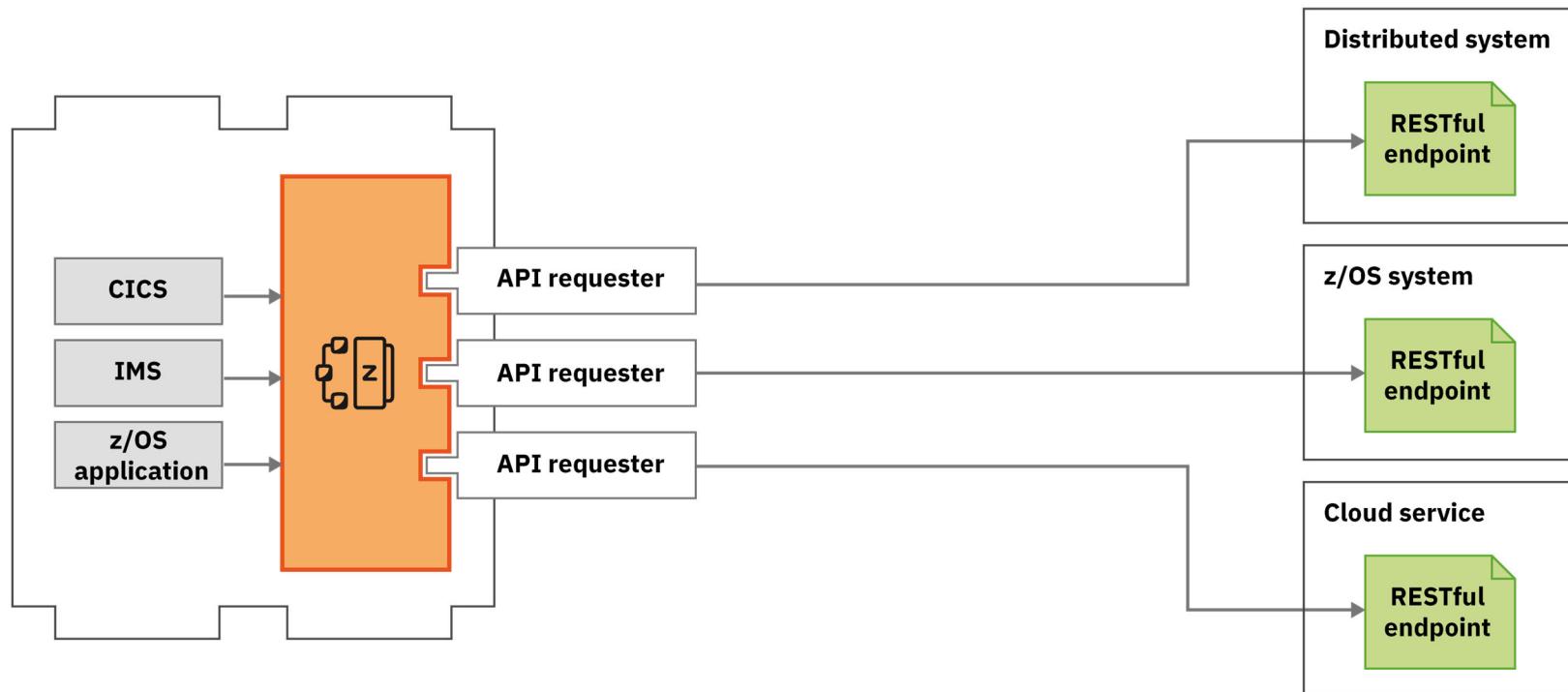
## /api\_toolkit/apiRequesters

Quick and easy API mapping.





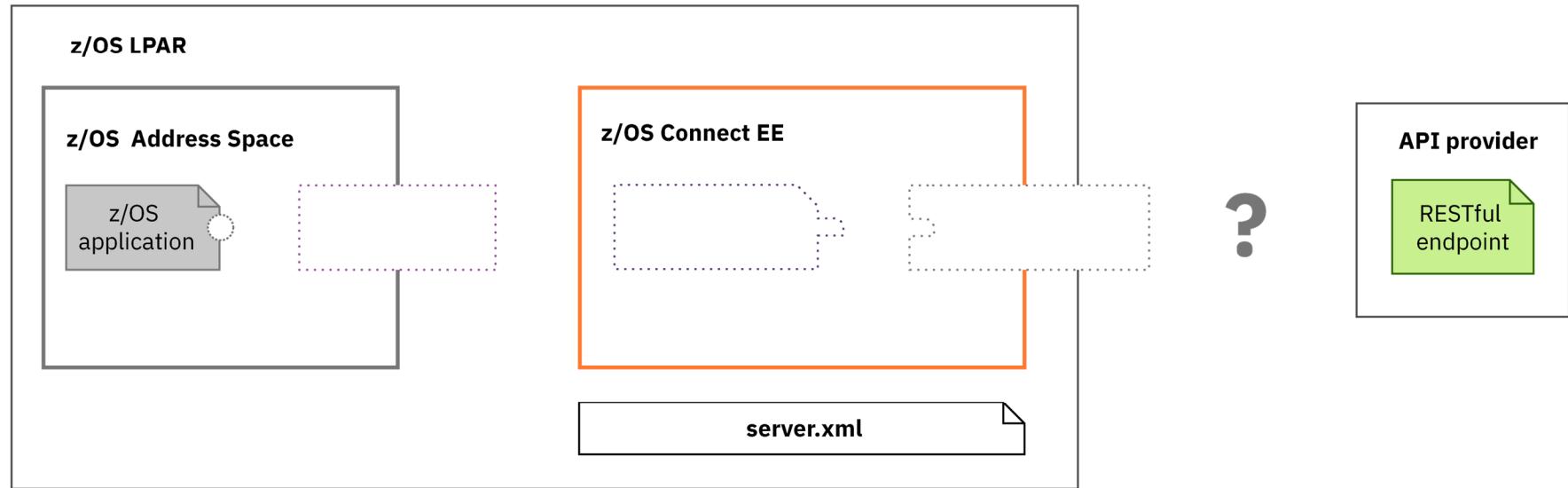
# Use API requester to call external APIs from z/OS assets





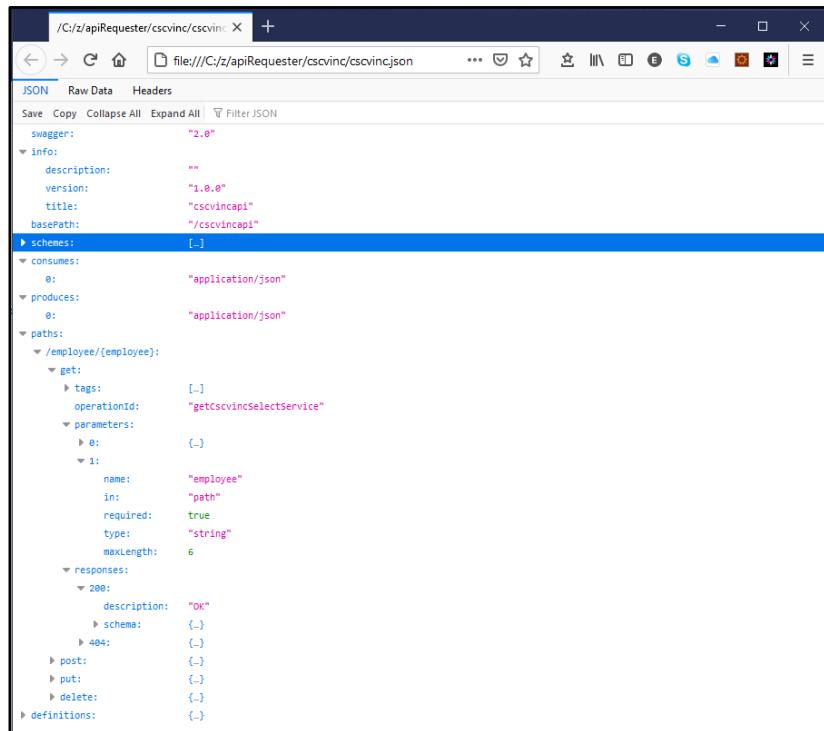
# Steps to calling an external API

Starting point



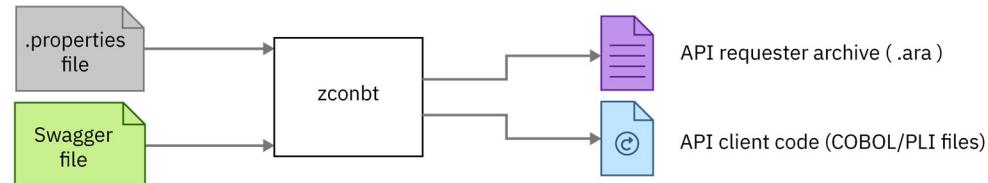
# Calling an external API requires the API's specification document

Start with the API's specification and generate the API requester archive file and API client code



The screenshot shows a JSON editor window displaying a Swagger JSON file. The file defines an API endpoint for employees, including parameters, responses, and definitions. Key sections include:

- swagger:** "2.0"
- info:** description: "", version: "1.0.0", title: "cscvincapi", basePath: "/cscvincapi"
- schemes:** []
- consumes:** @: "application/json"
- produces:** @: "application/json"
- paths:**
  - /employee/{employee}:**
    - get:**
      - tags:** []
      - operationId:** "getCscvincSelectService"
      - parameters:**
        - @:** {..}
        - 1:**
          - name:** "employee"
          - in:** "path"
          - required:** true
          - type:** "string"
          - maxLength:** 6
      - responses:**
        - 200:**
          - description:** "OK"
          - schema:** {..}
        - 404:**
          - schema:** {..}
      - post:**
        - schema:** {..}
      - put:**
        - schema:** {..}
      - delete:**
        - schema:** {..}



## properties file#

```
apiDescriptionFile=./cscvinc.json
dataStructuresLocation=./syslib
apiInfoFileLocation=./syslib
logFileDirectory=./logs
language=COBOL
connectionRef=cscvincAPI
requesterPrefix=csc
```

#Additional property file attributes, e.g., *defaultCharacterMaxLength*, *defaultArrayMaxItems*, etc. are described at **The build toolkit properties file** article at URL <https://www.ibm.com/docs/en/zosconnect/3.0?topic=toolkit-build-properties-file>



# But there COBOL working storage implications

Specification properties are usually not constrained, this can lead to excessive COBOL working storage consumption

A screenshot of a JSON editor window titled "/C:/z/apiRequester/ATS/ATSContact:X". The URL in the address bar is "file:///C:/z/apiRequester/ATS/ATSContactPreferences". The JSON schema is displayed with various fields and their descriptions. Several fields are circled in red, including:

- "communicationPreferences": A field under "memberCodeableConcept" with a \$ref of "#/definitions/member-communication-preferences" and type "array".
- "firstName": A field under "name" with a \$ref of "#/definitions/member-name" and type "string".
- "lastName": A field under "name" with a \$ref of "#/definitions/member-name" and type "string".
- "birthDate": A field under "dateOfBirth" with a \$ref of "#/definitions/date-of-birth" and type "string".

mitchj@us.ibm.com

A screenshot of a Windows Notepad window titled "ATS01P01 - Notepad". The file contains a large amount of COBOL code. Several fields are circled in red, including:

- 09 memberContactsResponse OCCURS 255.
- 12 umi-num PIC S9(9) COMP-5 SYNC.
- 12 umi. 15 umi2-length 15 umi2 PIC S9999 COMP-5 PIC X(255).
- 12 pin-num PIC S9(9) COMP-5 SYNC.
- 12 pin. 15 pin2-length 15 pin2 PIC S9999 COMP-5 PIC X(255).
- 12 firstName-num PIC S9(9) COMP-5 SYNC.
- 12 firstName. 15 firstName2-length 15 firstName2 PIC S9999 COMP-5 PIC X(255).
- 12 middleName-num PIC S9(9) COMP-5 SYNC.
- 12 middleName. 15 middleName2-length 15 middleName2 PIC S9999 COMP-5 PIC X(255).
- 12 lastName-num PIC S9(9) COMP-5 SYNC.
- 12 lastName. 15 lastName2-length 15 lastName2 PIC S9999 COMP-5 PIC X(255).

© 2018, 2023 IBM Corporation

Page 23



# There are API Requester generation properties are available to help

Use these generation properties to set default array size and string field sizes

**defaultArrayMaxItems** - Specify the maximum array boundary to apply when no maximum occurrence information (maxItems) is implied in the Swagger. The value of this parameter can be a positive integer in the range 1 - 32767. By default, **defaultArrayMaxItems** is set to **255**.

**defaultCharacterMaxLength** - Specify the default array length of character data in characters for mappings where no length is implied in the JSON schema document. When **characterVarying** is set to YES, the value of this parameter can be a positive integer in the range of 1 to 32767. When **characterVarying** is set to NO or NULL the value of this parameter can be a positive integer in the range of 1 to 16777214. By default, **defaultCharacterMaxLength** is set to **255**.

**characterVarying** - Specifies how variable-length character data is mapped to the language structure.

- NO - Variable-length character data is mapped as fixed-length strings.
- NULL - Variable-length character data is mapped to null-terminated strings (**defaultCharacterMaxLength** + 1)
- YES - Variable-length character data is mapped to a CHAR VARYING data type in PL/I. In COBOL variable-length character data is mapped to an equivalent representation that consists of two related elements: the **data-length** and the **data**. By default, **characterVarying** is set to YES.

12 firstName-num	PIC S9(9) COMP-5	SYNC.
12 firstName.		
15 firstName2-length	PIC S9999 COMP-5	SYNC.

12 firstName-num	PIC S9(9) COMP-5	SYNC.
12 firstName	PIC X(31).	

```
MOVE 0 to ws-length
MOVE LENGTH OF firstName2 to firstName2-length.
INSPECT FUNCTION REVERSE (firstName2)
      TALLYING ws-length FOR ALL SPACES.
SUBTRACT ws-length FROM firstName2-length.
```

```
*-----*
 * Add null termination character to strings
 *-----*
 STRING firstName delimited by size
       X'00' delimited by size into _firstName.
 STRING ws-length delimited by size into _wsLength.
```



# Alternatively, consider adding constraints to the properties

Use the *maxItems* and *maxLength* attributes to set realistic maximum array and field sizes

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
  type: "array"
    communicationPreferences:
      items:
        $ref: "#/definitions/member-communication-preferences"
        type: "array"
        maxItems: 10
        memberCodeableConcept:
          description: "Multiple member codes"
        items:
          $ref: "#/definitions/member-codeable-concept"
          type: "object"
        type: "object"
      member-contacts-request:
        title: "Member Contacts Request"
        description: "Read-only request data to search for member contact information."
        properties:
          umi:
            description: "Unique Member Id. This value is at a contract level. All members under one contract have the same UMI."
            example: "112222444001"
            type: "string"
            maxLength: 12
          firstName:
            description: "Member first name or given name."
            example: "Arthur"
            type: "string"
            maxLength: 30
          lastName:
            description: "Member last name or family name."
            example: "Smith"
            type: "string"
            maxLength: 30
```

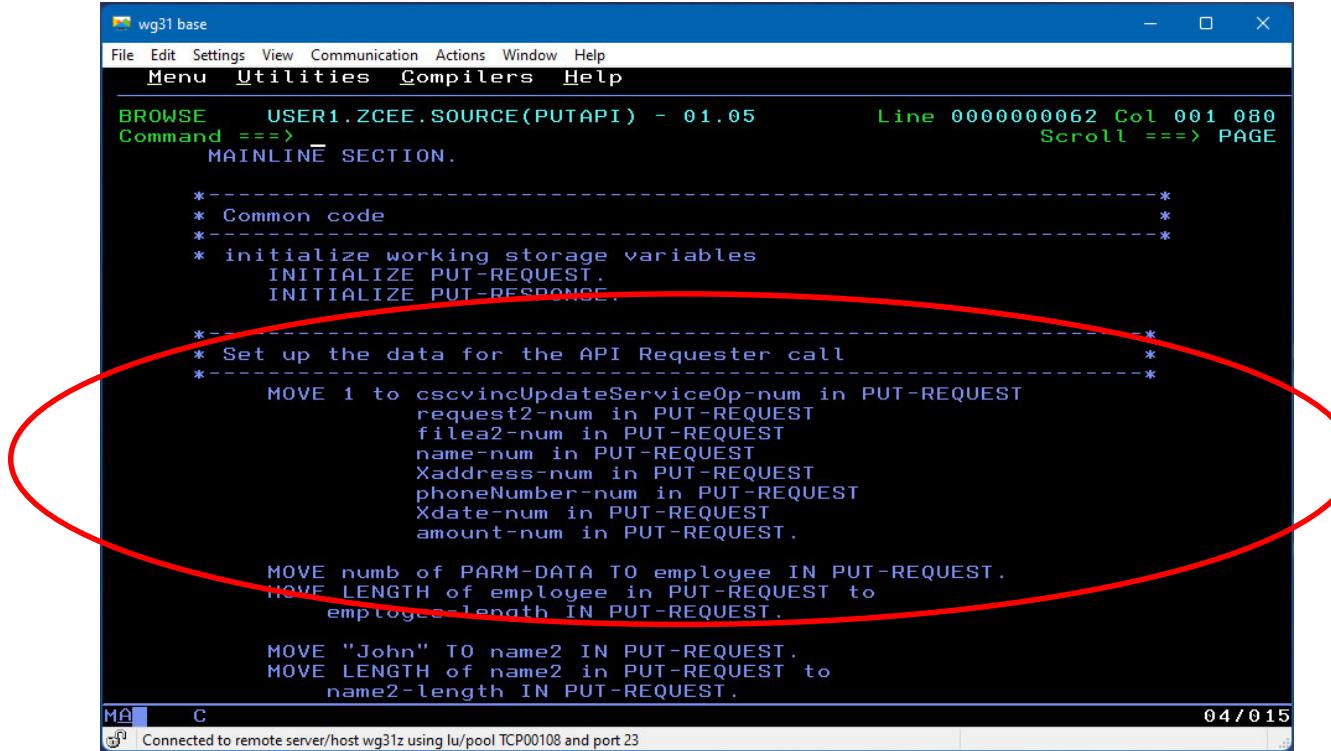
```
* Comments for field 'filler':
* This is a filler entry to ensure the correct padding for a
* structure. These slack bytes do not contain any application
* data.
*      15 filler          PIC X(3).
*
*
* ++++++
06 RespBody.

09 memberContactsResponse-num  PIC S9(9) COMP-5 SYNC.
09 memberContactsResponse OCCURS 10.
12 umi-num                    PIC S9(9) COMP-5 SYNC.
12 umi.
15 umi2-length
15 umi2
12 pin-num                    PIC S9(9) COMP-5 SYNC.
12 pin.
15 pin2-length
15 pin2
12 firstName-num               PIC S9(9) COMP-5 SYNC.
12 firstName.
15 firstName2-length
15 firstName2
12 middleName-num              PIC S9(9) COMP-5 SYNC.
12 middleName.
15 middleName2-length
15 middleName2
```



# The number of specific entries can be ambiguous

The COBOL copy book will include a counter variable (*variable-num*) for each variable whose number of occurrences is ambiguously defined in the specification document. The number of occurrences of these variables must be provided.



```
wg31 base
File Edit Settings View Communication Actions Window Help
Menu Utilities Compilers Help
BROWSE    USER1.ZCEE.SOURCE(PUTAPI) - 01.05      Line 0000000062 Col 001 080
Command ==>                               Scroll ==> PAGE
MAINLINE SECTION.

*-----
* Common code
*-----
* initialize working storage variables
  INITIALIZE PUT-REQUEST.
  INITIALIZE PUT-RESPONSE.

*-
* Set up the data for the API Requester call
*-
  MOVE 1 to cscvincUpdateServiceOp-num in PUT-REQUEST
    request2-num in PUT-REQUEST
    filea2-num in PUT-REQUEST
    name-num in PUT-REQUEST
    Xaddress-num in PUT-REQUEST
    phoneNumber-num in PUT-REQUEST
    Xdate-num in PUT-REQUEST
    amount-num in PUT-REQUEST.

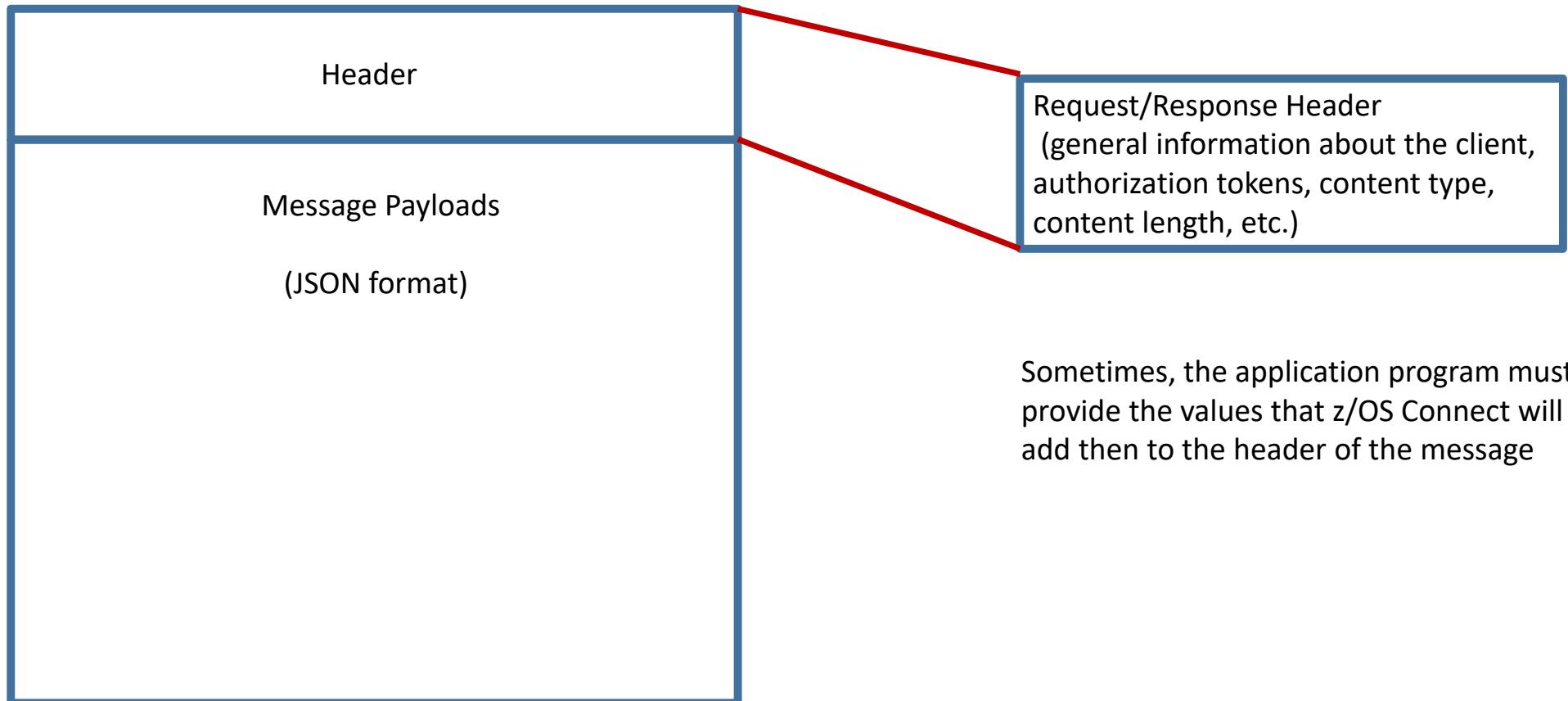
  MOVE num of PARM-DATA TO employee IN PUT-REQUEST.
  MOVE LENGTH of employee in PUT-REQUEST to
    employee-length IN PUT-REQUEST.

  MOVE "John" TO name2 IN PUT-REQUEST.
  MOVE LENGTH of name2 in PUT-REQUEST to
    name2-length IN PUT-REQUEST.

04 / 015
MA C
Connected to remote server/host wg31z using lu/pool TCP00108 and port 23
```



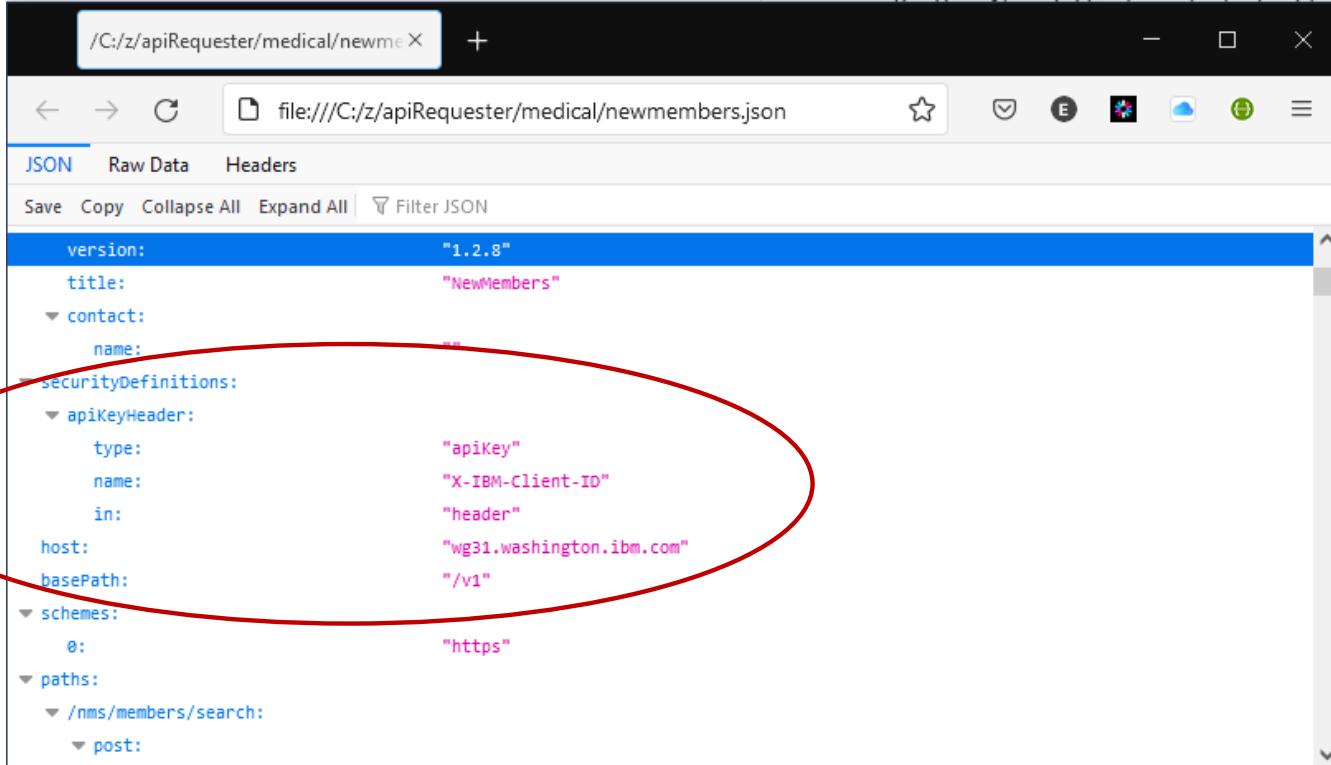
# Request and Response Message Layout





# For security, an API key(aka password) may be required

The details can be provided in the specification document as shown below or . . .



A screenshot of a JSON editor window titled "file:///C:/z/apiRequester/medical/newmembers.json". The window shows a JSON object with several fields. A red oval highlights the "securityDefinitions" field, which contains an "apiKeyHeader" object. This object has "type": "apiKey", "name": "X-IBM-Client-ID", and "in": "header". Below it is an "https" scheme entry. The "paths" field is also highlighted by the oval, containing a "/nms/members/search" path with a "post" method.

```
version: "1.2.8"
title: "NewMembers"
contact:
  name: ""
securityDefinitions:
  apiKeyHeader:
    type: "apiKey"
    name: "X-IBM-Client-ID"
    in: "header"
  host: "wg31.washington.ibm.com"
  basePath: "/v1"
  schemes:
    0: "https"
paths:
  /nms/members/search:
    post:
```

## Via a HTTP header

GET /something HTTP/1.1

**X-API-Key: abcdef12345**

## Or via a query parameter

GET /something?api\_key=abcdef12345

# The application provides the API key to the request header



Either way, the generated request copy book includes a ReqHeaders structure which can be used to provide values for header properties

The image shows two windows side-by-side. The left window is titled "request.cpy - Notepad" and contains an AS/400 copybook (RECFM=V) with a ReqHeaders structure. The right window is titled "mpz3" and contains an AS/400 source program (RECFM=V) named USER1.ZCEE.SOURCE(GETAPIEN). Both windows show code in green and red font.

**Left Window (request.cpy - Notepad):**

```
*      12 dob2-length          PIC S9999 COMP-5
* SYNC.
*      12 dob2                PIC X(255).
*
*
* ++++++
06 ReqHeaders.
09 X-IBM-Client-ID-length    PIC S9999 COMP-5 SYNC.
09 X-IBM-Client-ID           PIC X(255).
09 X-HZN-ClientName-length   PIC S9999 COMP-5 SYNC.
09 X-HZN-ClientName          PIC X(255).
09 X-HZN-ClientSubmitDateTime PIC S9(15) COMP-3.

09 X-HZN-ClientTransaction-num PIC S9(9) COMP-5 SYNC.

09 X-HZN-ClientTransactionId.
12 X-HZN-ClientTransact-length PIC S9999 COMP-5
SYNC.
12 X-HZN-ClientTransactionId2 PIC X(255).

09 X-HZN-ClientSessionId-num  PIC S9(9) COMP-5 SYNC.

09 X-HZN-ClientSessionId.
12 X-HZN-ClientSessionId-length PIC S9999 COMP-5
SYNC.
12 X-HZN-ClientSessionId2    PIC X(255).

09 X-HZN-UserRole-num        PIC S9(9) COMP-5 SYNC.

09 X-HZN-UserRole.
12 X-HZN-UserRole2-length   PIC S9999 COMP-5
SYNC.
12 X-HZN-UserRole2          PIC X(255).

09 X-HZN-UserAssociationI-num PIC S9(9) COMP-5 SYNC.

09 X-HZN-UserAssociationI-length PIC S9(9) COMP-5 SYNC.
```

**Right Window (mpz3):**

```
EDIT      USER1.ZCEE.SOURCE(GETAPIEN) - 01.01      Columns 00001 00072
Command ==> *-----*
000081   *-----
000082   * Common code
000083   *-----
000084   * initialize working storage variables
000085   *      INITIALIZE GET-REQUEST.
000086   *      INITIALIZE GET-RESPONSE.
000087   MOVE "abcdef12345" to X-IBM-Client-ID
000088   MOVE 11 to X-IBM-Client-ID-length
000089   *-----*
000090   *-----*
000091   * Set up the data for the API Requester call
000092   *-----*
000093   MOVE employee of PARM-DATA TO employee IN GET-REQUEST.
000094   MOVE LENGTH of employee in GET-REQUEST to
000095   employee-length IN GET-REQUEST.
000096   *-----*
000097   * Initialize API Requester PTRs & LENs
000098   *-----*
000099   * Use pointer and length to specify the location of
000100   * request and response segment.
000101   * This procedure is general and necessary.
000102   SET BAQ-REQUEST-PTR TO ADDRESS OF GET-REQUEST.
000103   MOVE LENGTH OF GET-REQUEST TO BAQ-REQUEST-LEN.
000104   SET BAQ-RESPONSE-PTR TO ADDRESS OF GET-RESPONSE.
000105   MOVE LENGTH OF GET-RESPONSE TO BAQ-RESPONSE-LEN.
000106
000107
000108   *-----*
```



## Or by including generation properties related to API keys

Use these generation properties to add API key information to the request message when not defined in specification document

**apiKeyMaxLength** - Specify the maximum length of the values set for API keys. The value of this parameter can be a positive integer in the range 1 - 32767. By default, **apiKeyMaxLength** is set to 255.

**apiKeyParmNameInHeader** - Specify the name of an API key that is sent as a request header. The value of this parameter can be set in a comma separated list of a combination of client ID and client secret. For example, you can set **apiKeyParmNameInHeader**=header-IBM-Client-ID, header-IBM-Client-secret when a client ID and a client secret are used to protect an API.

**apiKeyParmNameInQuery** - Specify the name of an API key that is sent in a query string. The value of this parameter can be set in a comma separated list of a combination of client ID and client secret. For example, you can set **apiKeyParmNameInQuery**=query-IBM-Client-ID, query-IBM-Client-secret when a client ID and a client secret are used to protect an API.

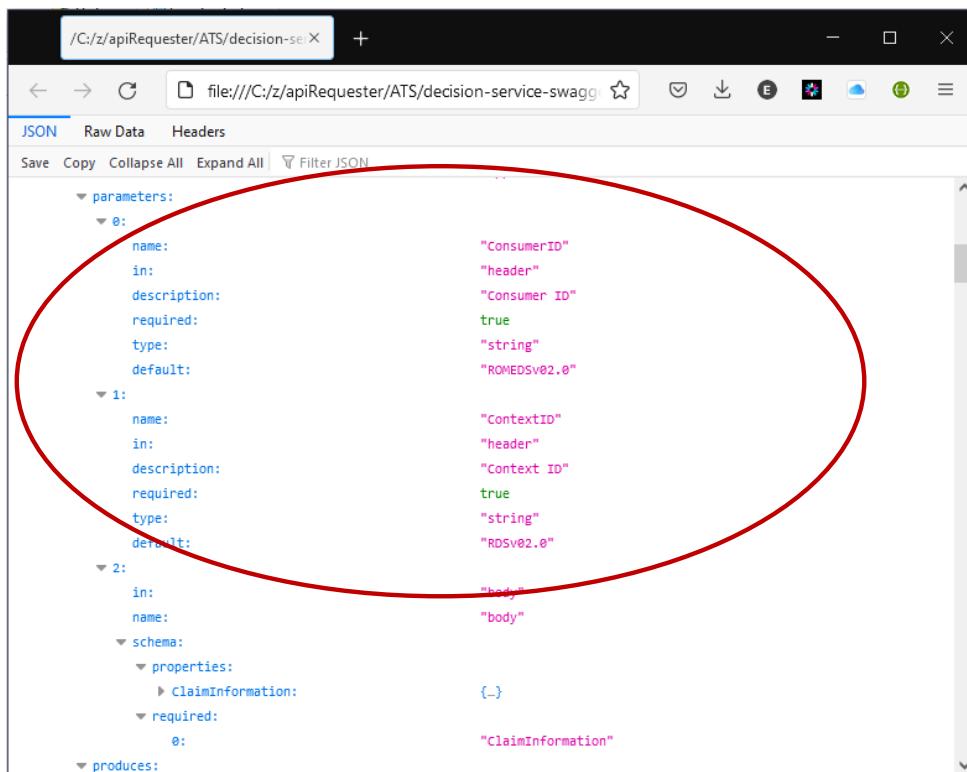
```
cscvinc.properties - Notepad
File Edit Format View Help
apiDescriptionFile=./cscvinc.json
dataStructuresLocation=./syslib
apiInfoFileLocation=./syslib
logFileDirectory=./logs
language=COBOL
connectionRef=cscvincAPI
requesterPrefix=ats
apiKeyMaxLength=40
apiKeyParmNameInHeader=X-IBM-Client-ID

Ln 8, Col 19 100% Unix (LF) UTF-8
```

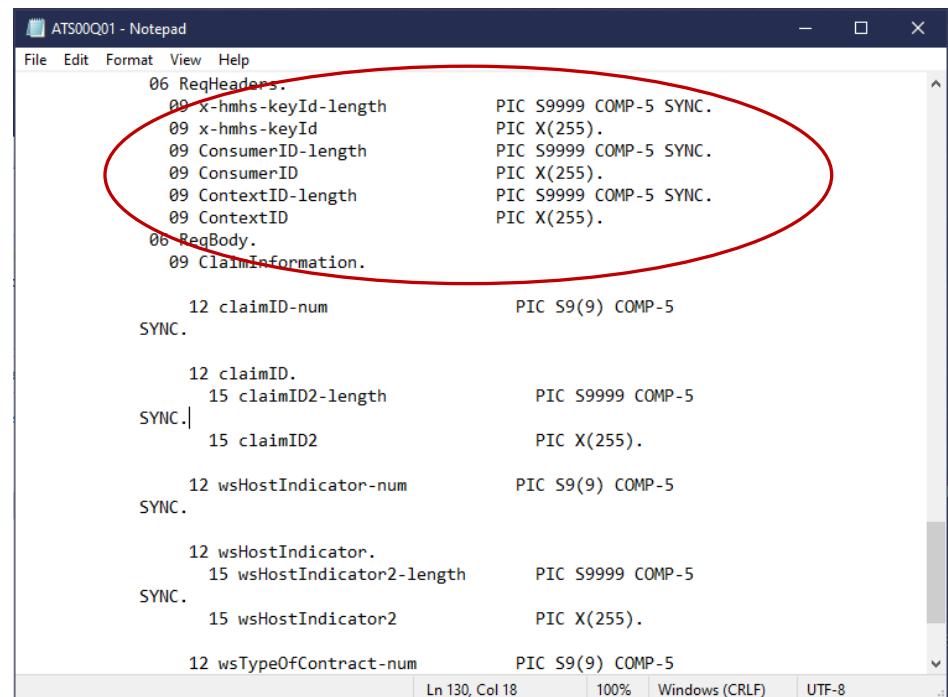


# And there may be other header properties can be required

The application can also set the values for other header properties that may be required by the API



```
/C:/apiRequester/ATS/decision-se X +  
file:///C:/apiRequester/ATS/decision-service-swagg  
JSON Raw Data Headers  
Save Copy Collapse All Expand All Filter JSON  
parameters:  
0:  
name: "ConsumerID"  
in: "header"  
description: "Consumer ID"  
required: true  
type: "string"  
default: "ROMEDSv2.0"  
1:  
name: "ContextID"  
in: "header"  
description: "Context ID"  
required: true  
type: "string"  
default: "RDSv02.0"  
2:  
in: "body"  
name: "body"  
schema:  
properties:  
ClaimInformation: (...)  
required:  
0: "ClaimInformation"  
produces:
```



```
ATS00Q01 - Notepad  
File Edit Format View Help  
06 ReqHeaders.  
09 x-hmhs-keyId-length PIC S9999 COMP-5 SYNC.  
09 x-hmhs-keyId PIC X(255).  
09 ConsumerID-length PIC S9999 COMP-5 SYNC.  
09 ConsumerID PIC X(255).  
09 ContextID-length PIC S9999 COMP-5 SYNC.  
09 ContextID PIC X(255).  
06 ReqBody.  
09 ClaimInformation.  
12 claimID-num PIC S9(9) COMP-5 SYNC.  
12 claimID.  
15 claimID2-length PIC S9999 COMP-5 SYNC.  
15 claimID2 PIC X(255).  
12 wsHostIndicator-num PIC S9(9) COMP-5 SYNC.  
12 wsHostIndicator.  
15 wsHostIndicator2-length PIC S9999 COMP-5 SYNC.  
15 wsHostIndicator2 PIC X(255).  
12 wsTypeOfContract-num PIC S9(9) COMP-5
```



# Steps to calling an external API

Use the z/OS Connect build toolkit, e.g., `zconbt`, to generate an API requester archive file and at most, 3 copy books per method found in the Swagger

```
zconbt.bat -p=./cscvinc.properties -f=./cscvinc.ara
BAQB0000I: z/OS Connect Enterprise Edition 3.0 Build Toolkit Version 1.5 (20210816-0926).
BAQB0008I: Creating API requester archive from configuration file ./cscvinc.properties.
BAQB0040I: The generated API requester is automatically named cscvincapi_1.0.0 based on the title cscvincapi and version 1.0.0 of the API to be called.
.
.
.
Total 4 operation(s) (success: 4, ignored: 0) defined in api description file: ./cscvinc.json
----- Successfully processed operation(s) -----
operationId: getCsvincSelectService, basePath: /cscvincapi, relativePath: /employee/{employee}, method: GET
- request data structure : CSC00Q01
- response data structure : CSC00P01
- api info file : CSC00I01

operationId: putCsvincUpdateService, basePath: /cscvincapi, relativePath: /employee/{employee}, method: PUT
- request data structure : CSC01Q01
- response data structure : CSC01P01
- api info file : CSC01I01

operationId: postCsvincInsertService, basePath: /cscvincapi, relativePath: /employee/{employee}, method: POST
- request data structure : CSC02Q01
- response data structure : CSC02P01
- api info file : CSC02I01

operationId: deleteCsvincDeleteService, basePath: /cscvincapi, relativePath: /employee/{employee}, method: DELETE
- request data structure : CSC03Q01
- response data structure : CSC03P01
- api info file : CSC03I01

BAQB0009I: Successfully created API requester archive file ./cscvinc.ara.
```

# BTW, the z/OS Connect Build Toolkit can be executed on z/OS



```
//JOHNSONS JOB (ACCOUNT),JOHNSON,NOTIFY=&SYSUID,REGION=0M,  
// CLASS=A,MSGCLASS=H,MSGLEVEL=(1,1)  
//*****  
///* SET SYMBOLS  
//*****  
//EXPORT EXPORT SYMLIST=(*)  
// SET WORKDIR='u/johnson/zconbt'  
// SET ZCONDIR='/usr/lpp/IBM/zosconnect/v3r0/zconbt/bin'  
//ZCONBT EXEC PGM=IKJEFT01,REGION=0M,MEMLIMIT=4G  
//SYSTSPPRT DD SYSOUT=*  
//SYSERR DD SYSOUT=*  
//STDOUT DD SYSOUT=*  
//SYSTSIN DD *,SYMBOLS=EXECSYS  
BPXBATCH SH +  
  export WORKDIR=&WORKDIR; +  
  export ZCONDIR=&ZCONDIR; +  
  cd $WORKDIR; +  
  $ZCONDIR/zconbt.zos -p cscvinc.properties -f=cscvinc.ara; +  
  cp -v $WORKDIR/syslib/* //'JOHNSON.ZCONBT.COPYLIB'"
```

## cscvinc.properties

```
apiDescriptionFile=./cscvinc.json  
dataStructuresLocation=./syslib  
apiInfoFileLocation=./syslib  
logFileDirectory=./logs  
language=COBOL  
connectionRef=cscvincAPI  
requesterPrefix=csc
```

This assumes the zconbt.zip files was expanded into directory /usr/lpp/IBM/zosconnect/v3r0/zconbt using command *jar -tf zconbt.zip* and that the property file and Swagger JSON document are encoded in ASCII in directory /u/johnson/zconbt.



# Tech-Tip: Copy books naming convention

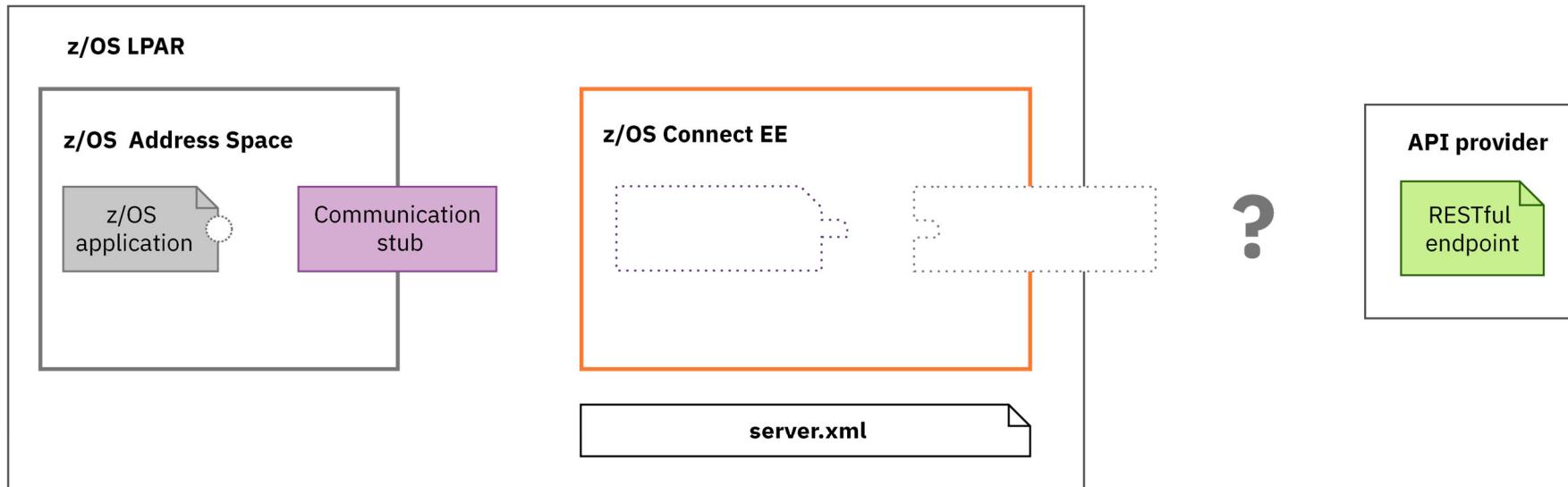
- The naming convention for the generated COBOL copy books is based on the *requesterPrefix* value specified in the properties file. That value was set to CSC in this case, e.g., CSC#####. The next 2 characters in the name are assigned sequentially as each API and method is processed, e.g., CSC00### and CSC01###, and CSC02###.
- The next character will be either a Q, P or an I. A “Q” for a **request** copy book, the “P” for a **response** copy book and the “I” for the copy book which contains **information**, e.g., method, path name etc. derived from the Swagger document
- Up to three copy books are generated for each method of each API found in the Swagger document.
  - In the previous example, there were 4 APIs with each having 1 method for a total of 12 copy books.
  - If there is no request message or no response message, then no copy book will be generated. But the messages stills need to have addressable storage in the application's working area.

```
* Request and Response
 01 GET-REQUEST.
    10 FILLER
      PIC X(1).
 01 GET-RESPONSE.
    COPY MQ000P01 SUPPRESS.
* Structure with the API information
 01 GET-INFO-OPER1.
    COPY MQ000I01 SUPPRESS.
```



# Steps for involving an external API from a COBOL program

Update the application by adding the generated copy books, a common BAQRINFO copy book and a call to communication stub



Configure a communication stub.

- For CICS region systems using URIMAP resources
- For non CICS client the configuration is done via environment variables

```
*-----*
* Call the communication stub
*-----*
*-----*
* Call the subsystem-supplied stub code to send
* API request to zCEE
    CALL COMM-STUB-PGM-NAME USING
        BY REFERENCE    GET-INFO-OPER1
        BY REFERENCE    BAQ-REQUEST-INFO
        BY REFERENCE    BAQ-REQUEST-PTR
        BY REFERENCE    BAQ-REQUEST-LEN
        BY REFERENCE    BAQ-RESPONSE-INFO
        BY REFERENCE    BAQ-RESPONSE-PTR
        BY REFERENCE    BAQ-RESPONSE-LEN
    END-CALL
    RETURN CODE 01 NO-ERRORS
```



# Steps to calling an external API

Include the generated copy books in a COBOL program

```
GETAPI X
  *--> ERROR MESSAGE STRUCTURE
  01  ERROR-MSG.
    03  EM-ORIGIN          PIC X(8)  VALUE SPACES.
    03  EM-CODE            PIC S9(9) COMP-5 SYNC VALUE 0.
    03  EM-DETAIL          PIC X(1024) VALUE SPACES.

  * Copy API Requester required copybook
  *-----*
  COPY BAQRINFO.

  * Request and Response
  01 API-REQUEST.
    COPY CSC02Q01.
  01 API_RESPONSE.
    COPY CSC02P01.

  * Structure with the API information
  01 API-INFO-OPER1.
    COPY CSC02I01.

  * Request and Response segment used to store request and
    ***
```

## API-REQUEST

```
CSC00I01  CSC00Q01 X
  * JSON schema keyword 'minLength' value: '0'.
  * JSON schema keyword 'maxLength' value: '6'.
  * This field contains a varying length array of characters or
  * binary data.
  *      09 employee-length          PIC S9999 COMP-5 SYNC.
  *      09 employee                PIC X(6).
  *
  * ++++++
  06 ReqPathParameters.
    09 employee-length          PIC S9999 COMP-5 SYNC.
    09 employee                PIC X(6).
```

## API-RESPONSE

```
CSC00I01  CSC00Q01  CSC00P01 X
  * ++++++
  06 RespBody.
    09 cscvincapSelectServiceOp-num  PIC S9(9) COMP-5 SYNC.
    09 cscvincapSelectServiceOperatio.
      12 Container1.

    15 RESPONSE-CONTAINER2-num     PIC S9(9) COMP-5
      SYNC.
```

## API-INFO-OPER1

```
CSC00I01 X
  03 BAQ-APINAME           PIC X(255)
    VALUE 'cscvincap1_1.0.0'.
  03 BAQ-APINAME-LEN        PIC S9(9) COMP-5 SYNC
    VALUE 16.
  03 BAQ-APIPATH            PIC X(255)
    VALUE '%2Fcvincap1%2Femployee%2F%7Bemployee%7D'.
  03 BAQ-APIPATH-LEN        PIC S9(9) COMP-5 SYNC
    VALUE 41.
  03 BAQ-APIMETHOD          PIC X(255)
    VALUE 'GET'.
  03 BAQ-APIMETHOD-LEN      PIC S9(9) COMP-5 SYNC
    VALUE 3.
```



# Steps to calling an external API

Add a call to the communication stub use pointers to pass working storage addresses of the copy books

The diagram illustrates the steps to calling an external API. It shows the GETAPI program, the communication stubs (CSC00101, CSC00Q01, CSC00P01), and the copy books (CSC00101, CSC00Q01, CSC00P01).

**GETAPI Program:**

```
* Set up the data for the API Requester call
*
MOVE numb      of PARM-DATA TO numb IN API-REQUEST.
MOVE LENGTH of numb in API-REQUEST to
numb-length IN API-REQUEST.

* Initialize API Requester PTRS & LENs
*
* Use pointer and length to specify the location of
* request and response segment.
* This procedure is general and necessary.
SET BAQ-REQUEST-PTR TO ADDRESS OF API-REQUEST.
MOVE LENGTH OF API-REQUEST TO BAQ-REQUEST-LEN.
SET BAQ-RESPONSE-PTR TO ADDRESS OF API_RESPONSE.
MOVE LENGTH OF API_RESPONSE TO BAQ-RESPONSE-LEN.

* Call the communication stub
*
* Call the subsystem-supplied stub code to send
* API request to zCEE
CALL COMM-STUB-PGM-NAME USING
BY REFERENCE API-INFO-OPER1
BY REFERENCE BAQ-REQUEST-INFO
BY REFERENCE BAQ-REQUEST-PTR
BY REFERENCE BAQ-REQUEST-LEN
BY REFERENCE BAQ-RESPONSE-INFO
BY REFERENCE BAQ-RESPONSE-PTR
BY REFERENCE BAQ-RESPONSE-LEN.

* The BAQ-RETURN-CODE field in 'BAQRINFO' indicates whether this
```

**Communication Stubs (CSC00101, CSC00Q01, CSC00P01):**

- CSC00101:
  - BAQ-APINAME: 'cscvincapi\_1.0.0'. PIC X(255)
  - BAQ-APINAME-LEN: PIC S9(9) COMP-5 SYNC
  - BAQ-APIPATH: VALUE 16. PIC X(255)
  - BAQ-APIPATH-LEN: PIC S9(9) COMP-5 SYNC
  - BAQ-APIMETHOD: 'GET'. PIC X(255)
  - BAQ-APIMETHOD-LEN: PIC S9(9) COMP-5 SYNC
- CSC00Q01:
  - employee-length: PIC S9999 COMP-5 SYNC.
  - employee: PIC X(6).
- CSC00P01:
  - ReqPathParameters:
    - employee-length: PIC S9999 COMP-5 SYNC.
    - employee: PIC X(6).
  - RespBody:
    - cscvincSelectServiceOp-num: PIC S9(9) COMP-5 SYNC.
    - cscvincSelectServiceOperatio: PIC X(12).
    - Container1: PIC S9(9) COMP-5 SYNC.
    - RESPONSE-CONTAINER2-num: PIC S9(9) COMP-5 SYNC.



# Steps to calling an external API

Accessing the results that have been stored in working storage

```
BY REFERENCE BAQ-RESPONSE-LEN.  
* The BAQ-RETURN-CODE field in 'BAQRINFO' indicates whether this  
* API call is successful.  
  
* When BAQ-RETURN-CODE is 'BAQ-SUCCESS', response is  
* successfully returned and fields in RESPONSE copybook  
* can be obtained. Display the translation result.  
IF BAQ-SUCCESS THEN  
    DISPLAY "NUMB: " Numb2 of API_RESPONSE  
    DISPLAY "NAME: " name2 of API_RESPONSE  
    DISPLAY "ADDRX: " addrx2 of API_RESPONSE  
    DISPLAY "PHONE: " phone2 of API_RESPONSE  
    DISPLAY "DATEX: " datex2 of API_RESPONSE  
    DISPLAY "AMOUNT: " amount2 of API_RESPONSE  
MOVE CEIBRESP of API_RESPONSE to EIBRESP  
MOVE CEIBRESP2 of API_RESPONSE to EIBRESP2  
DISPLAY "EIBRESP: " EIBRESP  
DISPLAY "EIBRESP2: " EIBRESP2  
DISPLAY "HTTP CODE: " BAQ-STATUS-CODE  
  
* Otherwise, some error happened in API, z/OS Connect EE server  
* or communication stub. 'BAQ-STATUS-CODE' and  
* 'BAQ-STATUS-MESSAGE' contain the detailed information  
* of this error.  
ELSE  
    DISPLAY "Error code: " BAQ-STATUS-CODE  
    DISPLAY "Error msg: " BAQ-STATUS-MESSAGE  
    MOVE BAQ-STATUS-CODE TO EM-CODE  
    MOVE BAQ-STATUS-MESSAGE TO EM-DETAIL  
    EVALUATE TRUE  
* When error happens in API, BAQ-RETURN-CODE is BAQ-ERROR-IN-API.  
* BAQ-STATUS-CODE is the HTTP response code of API.  
    LBNL BAQ-ERR001 IN API
```

mpz3

BROWSE ZCEE30.SBAQC0B(BAQRINFO)  
Command ==>

Field	Type	Length	Value
01 BAQ-RESPONSE-INFO.	PIC S9(9)	COMP-5 SYNC	VALUE 0.
03 BAQ-RESPONSE-INFO-COMP-LEVEL	PIC X(8)		
03 BAQ-STUB-NAME	PIC S9(9)	COMP-5 SYNC.	VALUE 0.
03 BAQ-RETURN-CODE	PIC S9(9)	COMP-5 SYNC.	VALUE 1.
88 BAQ-SUCCESS	PIC X(8)		VALUE 0.
88 BAQ-ERROR-IN-API	PIC X(8)		VALUE 1.
88 BAQ-ERROR-IN-ZCEE	PIC X(8)		VALUE 2.
88 BAQ-ERROR-IN-STUB	PIC X(8)		VALUE 3.
88 BAQ-ERROR-NO-RESPONSE	PIC X(8)		VALUE 4.
03 BAQ-STATUS-CODE	PIC S9(9)	COMP-5 SYNC.	VALUE 1.
03 BAQ-STATUS-MESSAGE	PIC X(1024)		
03 BAQ-STATUS-MESSAGE-LEN	PIC S9(9)	COMP-5 SYNC.	VALUE 1.

\*\*\*\*\* Bottom of Data \*\*\*\*\*

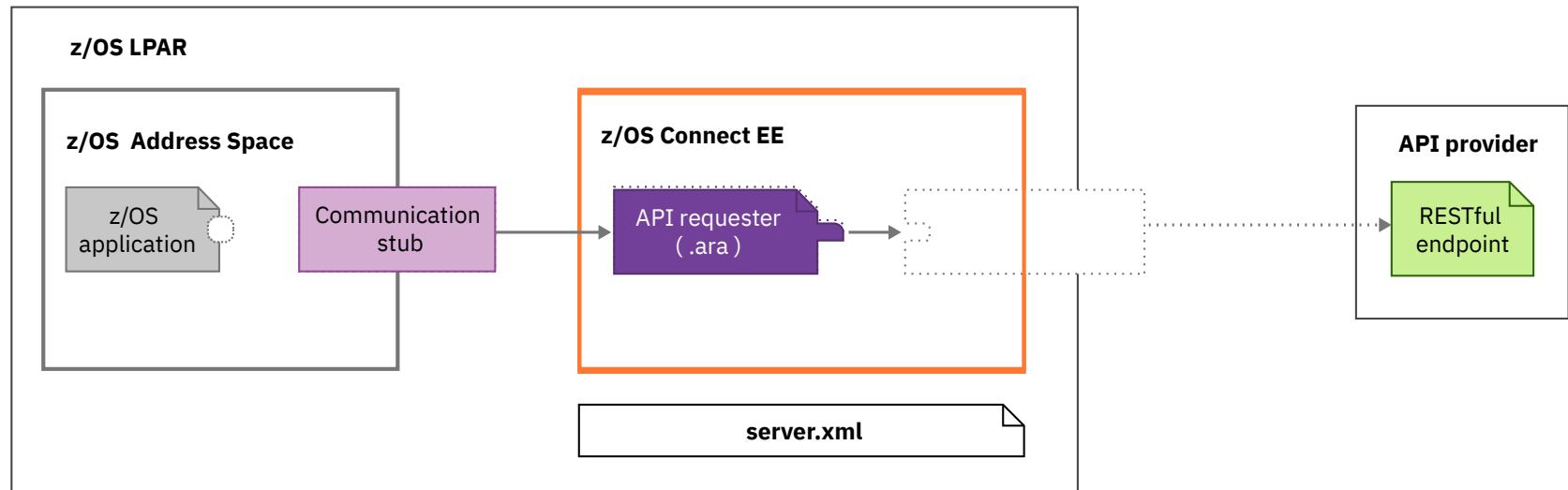
Connected to remote server/host mpz3 using lu/pool MPZ30021 and port 23

18 / 058



# Steps to calling an external API

Deploy the API requester (.ara) archive



Deploy your API requester archive to the *apiRequesters* directory.

# Steps to calling an external API – Resolving the endpoint URL

An administrator configures the endpointConnection providing the host and port of the URL

The screenshot shows a Swagger JSON editor window. The URL in the address bar is `/C:/apiRequester/cscvinc/swagger.json`. The JSON content displays the following configuration under the `info` section:

```
swagger: "2.0"
info:
  description: ""
  version: "1.0.0"
  title: "cscvinc"
  host: "localhost:8080"
  basePath: "/cscvinc"
```

Below this, there are sections for `schemes`, `consumes`, `produces`, and `paths`. Under `paths`, there is a `/employee` endpoint with a `post` method.

The screenshot shows an IBM i terminal window titled `CSC02I01`. It displays several system parameters (BAQ) related to the API endpoint:

- 03 BAQ-APINAME PIC X(255)  
VALUE 'cscvinc\_1.0.0'.
- 03 BAQ-APINAME-LEN PIC S9(9) COMP-5 SYNC  
VALUE 13.
- 03 BAQ-APIPATH PIC X(255)  
VALUE '/cscvinc/employee/{numb}'.
- 03 BAQ-APIPATH-LEN PIC S9(9) COMP-5 SYNC  
VALUE 24.
- 03 BAQ-APIMETHOD PIC X(255)  
VALUE 'GET'.
- 03 BAQ-APIMETHOD-LEN PIC S9(9) COMP-5 SYNC  
VALUE 3.

The screenshot shows the `Server Config` interface for `apiRequesterHTTPS.xml`. A red arrow points from the `basePath` configuration in the Swagger JSON editor to the `host` attribute of the `<zosconnect_endpointConnection` element in the XML configuration.

```
<zosconnect_endpointConnection id="cscvincAPI"
  host="https://dvipa.washington.ibm.com"
  port="9443"
  authenticationConfigRef="mySAFAuth"
  connectionTimeout="10s"
  receiveTimeout="4s" />
```

Another red arrow points from the `BAQ-APIPATH` parameter in the IBM i terminal to the `value` attribute of the `<zosconnect_authData` element in the XML configuration.

```
<zosconnect_authData id="mySAFAuth"
  user="USER1"
  password="user1" />
```

A final red arrow points from the `BAQ-APIMETHOD` parameter in the IBM i terminal to the `method` attribute of the `<zosconnect_endpointConnection` element in the XML configuration.

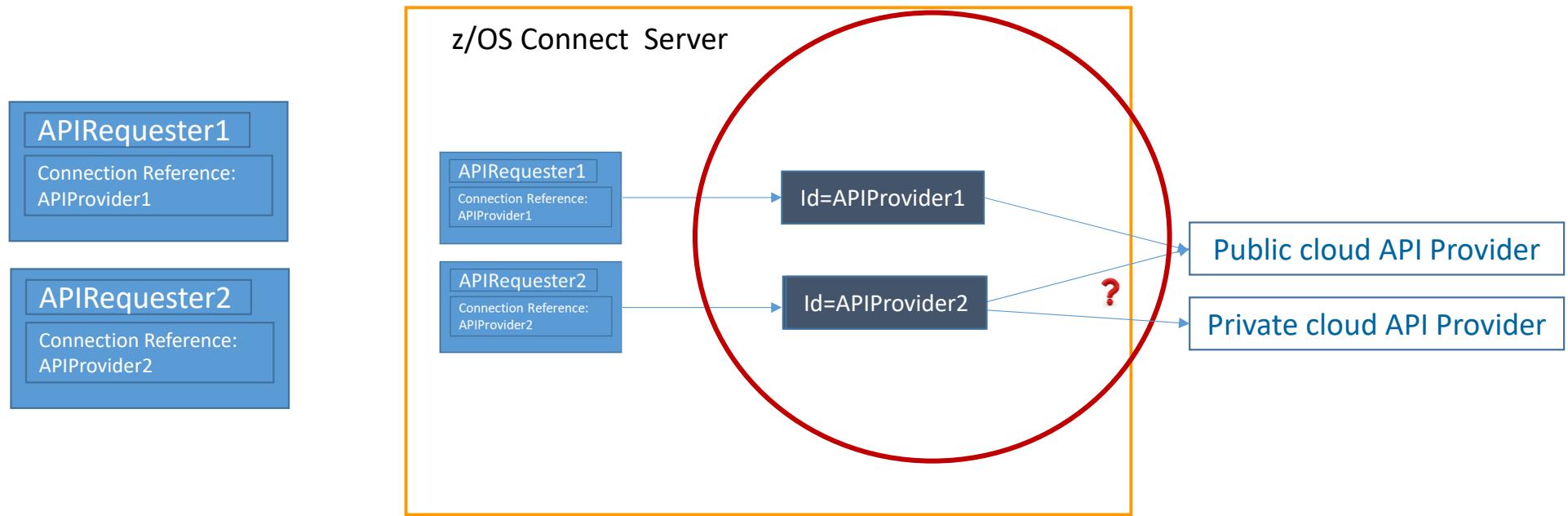
```
<zosconnect_endpointConnection id="cscvincAPI"
  host="https://dvipa.washington.ibm.com"
  port="9443"
  authenticationConfigRef="mySAFAAuth"
  connectionTimeout="10s"
  receiveTimeout="4s" />
```

The bottom right corner of the XML editor shows the resolved URL: <http://dvipa.washington.ibm.com:9443/cscvincapi/employee/{numb}>.



## Tech-Tip: Use naming conventions for connection references

Use application meaningful names or an extendable convention for connection reference names

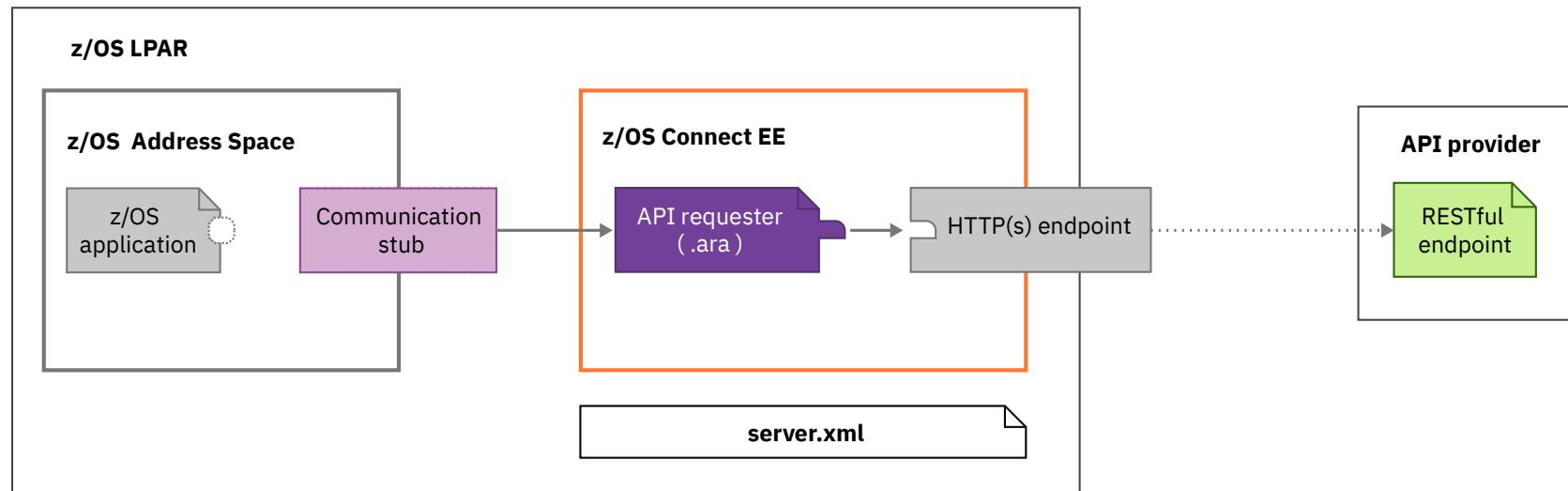


```
<zosconnect_apiRequesters>
  requireAuth="true|false"
  <apiRequester name="cscvincapi 1.0.0"
    connectionRef="APIProvider2"
  </zosconnect_apiRequesters>
```



# Steps to calling an external API

Configure HTTP(S) endpoint configuration element



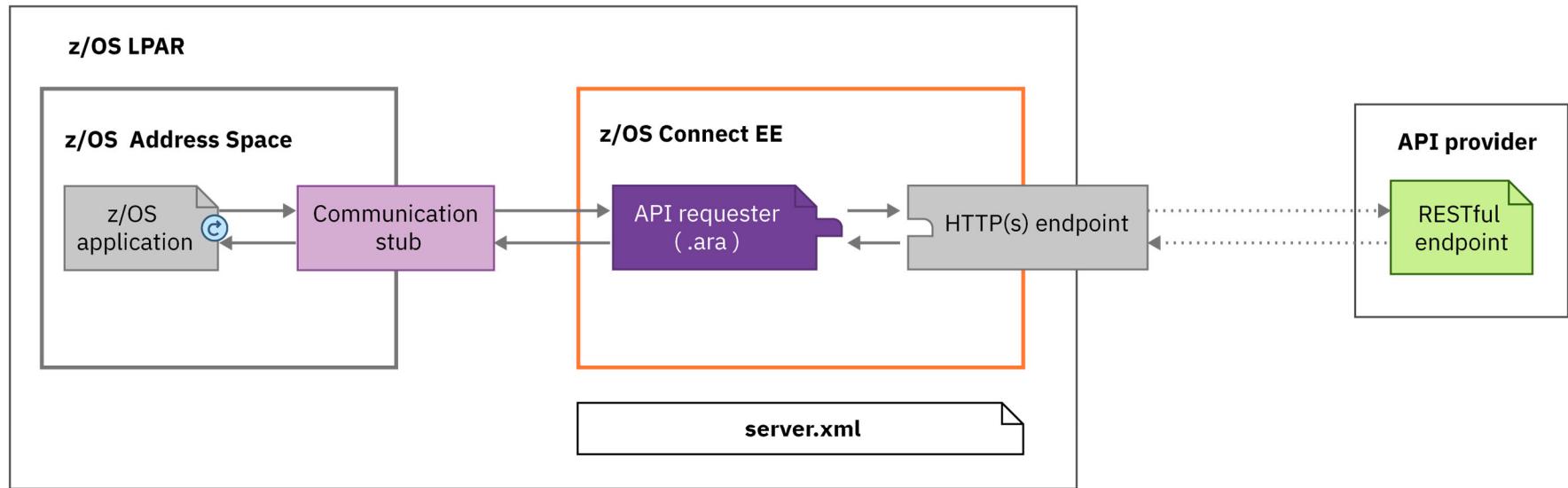
Configure the connection between z/OS Connect EE and the external API.

**i** [ibm.biz/zosconnect-configure-endpoint-connection](http://ibm.biz/zosconnect-configure-endpoint-connection)



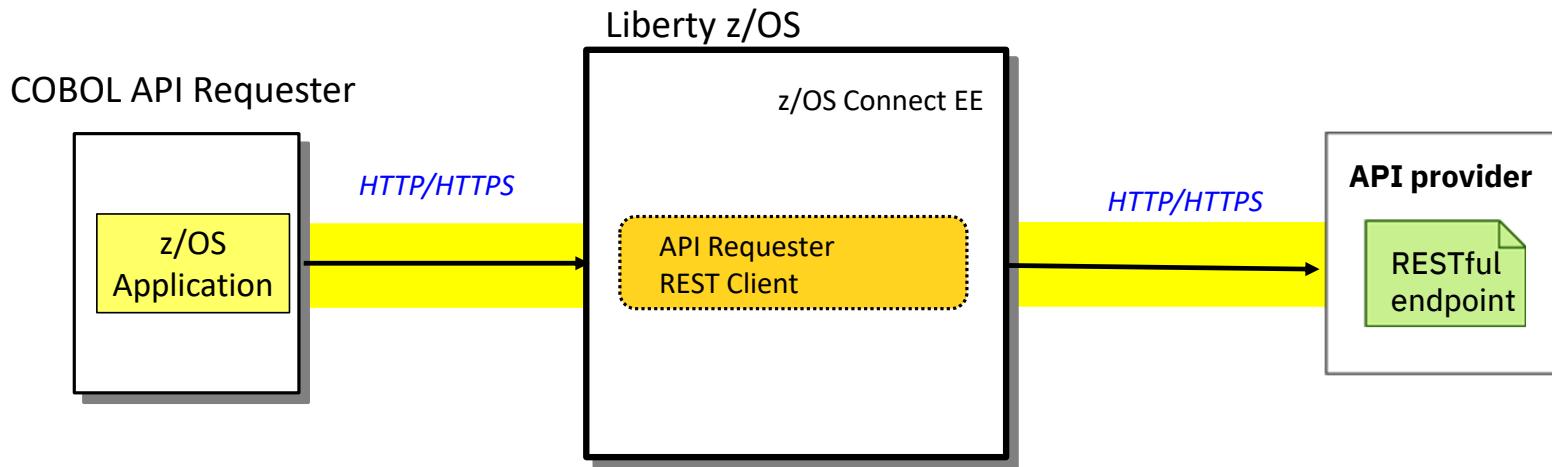
# Steps to calling an external API

Done





# End to end API requester to API Provider connection overview



MVS Batch, IMS HTTP and Db2 stored procedure connection details provided by:

- Environment Variables (BAQURI, BAQPORT)
  - Via JCL
  - LE Options (CEEROPTS)
  - Programmatically (CEEENV)
- HTTP or HTTPS

CICS HTTP connection details provided by:

- CICS URIMAP resource (default BAQURIMP)
  - HOST
  - PORT
  - SCHEME (HTTP/HTTPS)



# Configuring connections to the z/OS API requester server

## Default CICS URI MAP\*

```

WG31 - 3270
File Edit Settings View Communication Actions Window Help
I URIMAP
RESULT - OVERTYPE TO MODIFY
Urimap(BAQURIMP)
Usage(Client)
Enablestatus(Enabled)
Availstatus(Notapplic)
Scheme(Http)
Redirecttype( None )
Tcpinservice()
Port(09120)
Host(wg31.washington.ibm.com:9120)
Path(/)
Analyzerstat(Noanalyzer)
Hosttype(Hostname)
Ipresolved(0.0.0.0)
Ipfamily(Unknown)
Socketclose(0000030)
Sockpoolsize(0000000)
Transaction()
+ Converter()

SYSID=CICS APPLID=CICS53Z
TIME: 10.38.37 DATE: 02/14/22
PF 1 HELP 2 HEX 3 END      5 VAR      7 SBH 8 SFH      10 SB 11 SF
01/012
M A D
Connected to remote server/host wg31a using lu/pool TCP00120 and port 23
Adobe PDF on Documents\*.pdf

```

\* V3.0.37 added support for a CICS application to specify or request a specific URIMAP resource the using BAQ-ZCON-SERVER-URI variable in BAQRINFO

## LE Environment Variables

```

//DELTAPI EXEC PGM=DELTAPI,PARM='323232'
//STEPLIB DD DISP=SHR,DSN=USER1.ZCEE.LOADLIB
//          DD DISP=SHR,DSN=ZCEE30.SBAQLIB
//SYSOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CEEOPTS DD *
POSIX(ON),
ENVAR("BAQURI=wg31.washington.ibm.com",
"BAQPORT=9120")

```

```

mpz3
File Edit Settings View Communication Actions Window Help
Menu Utilities Compilers Help
BROWSE ZCEE30.SBAQCOB(BAQRINFO) Line 000000010 Col 001 080
Command ==> Scroll ==> PAGE
* (C) Copyright IBM Corp. 2017, 2021
* US Government Users Restricted Rights - Use, duplication or
* disclosure restricted by GSA ADP Schedule Contract with
* IBM Corp
*****
* This file contains the generated language structure(s) for
* Request and Response Info
*****
* BAQ-REQUEST-INFO-COMP-LEVEL permitted values
* VALUE
* 0 Base support
* 1 Added support for BAQ-OAUTH
* 2 Added support for BAQ-TOKEN (JWT)
* 3 Added support for setting z/OS Connect EE server URI
* 4 Added support for BAQ-OAUTH-EXT
*****
01 BAQ-REQUEST-INFO
03 BAQ-REQUEST-INFO-COMP-LEVEL PIC S9(9) COMP-5 SYNC VALUE 4.
03 BAQ-REQUEST-INFO-USER
05 BAQ-OAUTH
07 BAQ-OAUTH-USERNAME PIC X(256),
07 BAQ-OAUTH-USERNAME-LEN PIC S9(9) COMP-5 SYNC
07 BAQ-OAUTH-PASSWORD VALUE 0.
07 BAQ-OAUTH-PASSWORD-LEN PIC X(256),
PIC S9(9) COMP-5 SYNC
04/015
Connected to remote server/host mpz3 using lu/pool MPZ30044 and port 23

```



# Environment variables for non-CICS clients

Use these runtime environment variables when connecting to a z/OS Connect server

**BAQPASSWORD** - Specifies the password, in clear text, for the specified BAQUSERNAME to be authenticated with the z/OS Connect server. The username and password that are used for basic authentication, when SSL mutual authentication is not enabled.

**BAQPORT** - Specifies the port number for the z/OS Connect server.

**BAQTIMEOUT** - An optional 4-byte integer to set a timeout value in seconds for waiting for an API response. Valid range is 1 - 2,678,400 seconds. The default timeout value is 10 seconds.

**BAQURI** - Specifies either an IPv4 or IPV6 address, or a hostname of the host where the z/OS Connect server resides.

**BAQUSERNAME** - Specifies the username for connections if basic authentication is used.

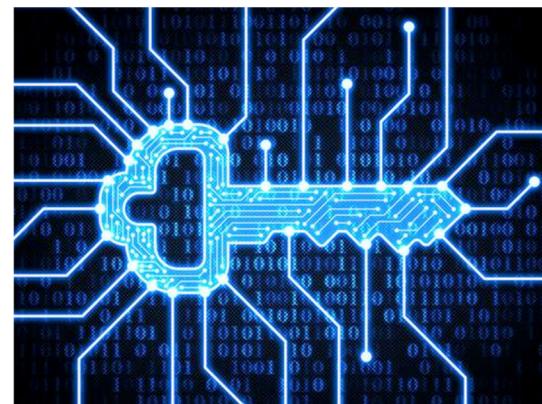
**BAQVERBOSE** - An optional value to turn on verbose messages to assist debugging of runtime and configuration issues. Valid values are **OFF**, **ON**, **ERROR**, **AUDIT** and **ALL**. See URL <https://www.ibm.com/docs/en/zos-connect/zosconnect/3.0?topic=car-configuring-other-zos-applications-access-zos-connect-api-calls> for more information.

**Now let's explore the security options for  
outbound API Requester connections  
and accessing remote resources**

## General security terms or considerations

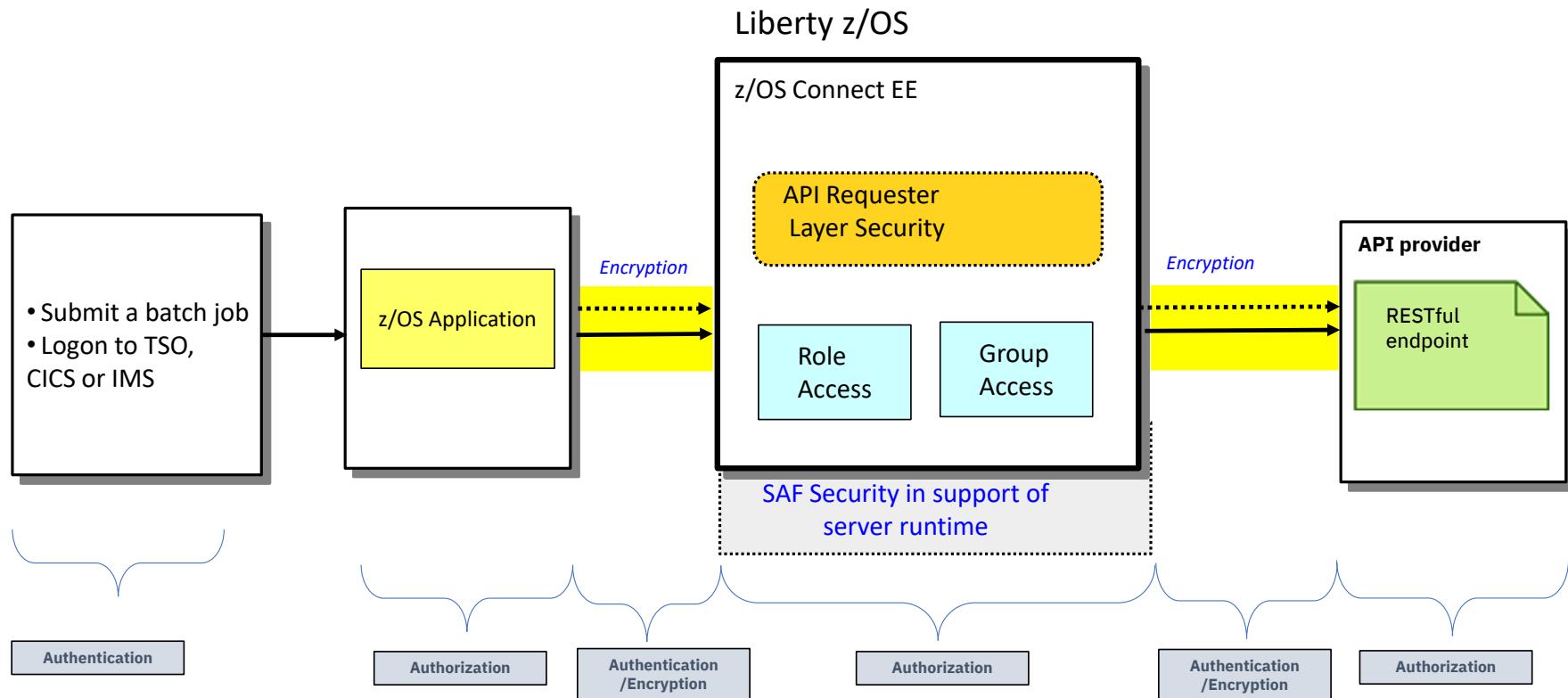
Security involves

- Identifying who or what is requesting access (**Authentication**)
  - Basic Authentication
  - Mutual Authentication using Transport Layer Security (TLS), formerly known as SSL
  - Third Party Tokens
- Ensuring that the message has not been altered in transit (**Data Integrity**) and ensuring the confidentiality of the message in transit (**Encryption**)
  - TLS (encrypting messages and using a digital signature)
- Controlling access (**Authorization**)
  - Is the authenticated identity authorized to access to z/OS Connect
  - Is the authenticated identity authorized to access a specific API, Services, etc.





# Outbound Authentication versus Authorization (OpenAPI 2)

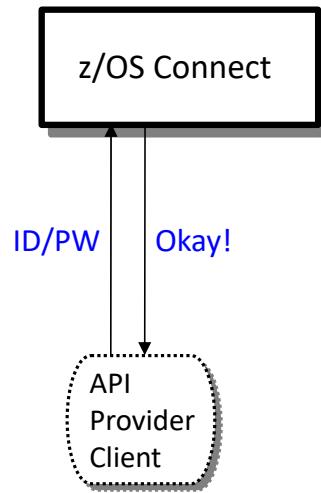




# API Requester – Security from the application to the z/OS Connect server

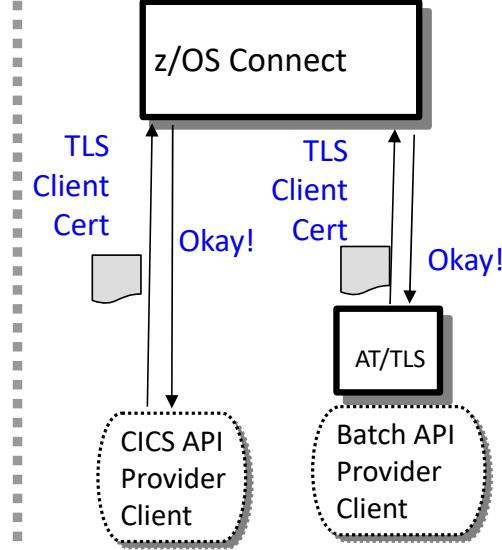
Two options for providing credentials for authentication

## Basic Authentication



**Application provides  
ID/PW or ID/PassTicket**

## Client Certificate



**z/OS Connect requests a  
client certificate**

**CICS or AT/TLS supplies a  
client certificate**



## Basic authentication – non-CICS COBOL API Requester

- ❑ A MVS batch, IMS or Db2 stored procedure requester application sends basic authentication information (identity and password) by using environment variables.
  - BAQUSERNAME
  - BAQPASSWORD
- ❑ The variables can be provided in JCL using CEEOPTS DD statement:

```
//CEELOPTS DD *  
  POSIX(ON),  
  ENVAR("BAQURI=wg31.washington.ibm.com",  
"BAQPORT=9080",  
"BAQUSERNAME=USER1",  
"BAQPASSWORD=USER1")
```

- ❑ Or, provided by using a CEEROPT or CEEUOPT module:

```
CEEROPT CSECT  
CEEROPT AMODE ANY  
CEEROPT RMODE ANY  
CEEXOPT POSIX=((ON),OVR),  
  ENVAR=((('BAQURI=wg31.washington.ibm.com',  
'BAQPORT=9120',  
'BAQUSERNAME=USER1',  
'BAQPASSWORD=USER1'),OVR),  
  RPTOPTS=((ON),OVR)  
END
```

**Tech/Tip: This is good opportunity to use a pass ticket rather than a password**

# Tech/Tip: A PassTicket provides an alternative to a password



- ❑ A PassTicket is generated by or for a client by using a secured sign-on key (whose value is masked or encrypted) to encrypt a valid *RACF identity* combined with the *application name* of the targeted resource. Also embedded in the PassTicket is a time stamp (based on the current Universal Coordinated Time (UCT)) which sets the time when the PassTicket will expire (usually 10 minutes).
- ❑ Access to PassTickets is managed using the RACF PTKTDATA class.
- ❑ For z/OS Connect, a RACF PassTicket can be used for basic authentication when connecting from any REST client on any platform to a z/OS Liberty server and for requests from a z/OS Connect server accessing IMS and Db2.
- ❑ *PassTickets do not have to be generated on z/OS using RACF services.* IBM has published the algorithm used to generate a PassTickets, see manual *z/OS Security Server RACF Macros and Interfaces, SA23-2288-40*. *Github has examples using Java, Python and other example are available on other sites.*

```
<safRegistry id="saf" />
  <safAuthorization racRouteLog="ASIS" />
  <safCredentials unauthenticatedUser="WSGUEST"
    profilePrefix="BBGZDFLT" />
```



## Tech/Tip: Generating PassTickets on z/OS

- On z/OS, a COBOL user application can generate a pass tickets by calling RACF service IRRSPK00:

```
77 COMM-STUB-PGM-NAME          PIC X(8) VALUE 'BAQCSTUB'.
77 PTKT-STUB-PGM-NAME         PIC X(8) VALUE 'ATSPKTTC'.
*-----
***** L I N K A G E   S E C T I O N *****
LINKAGE SECTION.
***** P R O C E D U R E S *****
PROCEDURE DIVISION using PARM-BUFFER.

*-----*
MAINLINE SECTION.

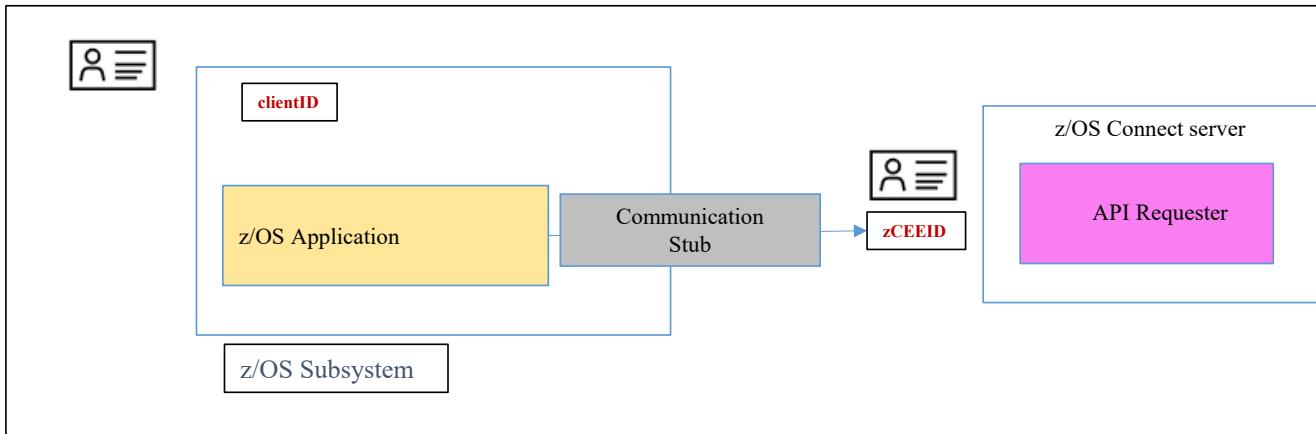
*-----*
* Common code *
*-----*
* initialize working storage variables
  INITIALIZE GET-REQUEST.
  INITIALIZE GET-RESPONSE.
  CALL PTKT-STUB-PGM-NAME.
```

### JOHNSON. PASSTCKT. SOURCE (ATSPKTTC)

```
*-----*
* Build IRRSPK00 parameters *
*-----*
      MOVE 0 to ws-length
      MOVE LENGTH OF identity to identity-length.
      INSPECT FUNCTION REVERSE (identity)
          TALLYING ws-length FOR ALL SPACES.
      SUBTRACT ws-length FROM identity-length.
      MOVE 0 to ws-length
      MOVE LENGTH OF applid to applid-length.
      INSPECT FUNCTION REVERSE (applid)
          TALLYING ws-length FOR ALL SPACES.
      SUBTRACT ws-length FROM applid-length.
      MOVE 8 to passTicket-length.
      MOVE 'NOTICKET' to passTicket.
      MOVE X'0003' to irr-functionCode.
      MOVE X'00000001' to irr-ticketOptions.
      SET irr-ticketOptions-ptr to ADDRESS OF irr-ticketOptions.
*-----*
* Call RACF service IRRSPK00 to obtain a pass ticket based *
*   on identity and applid                                     *
*-----*
      PERFORM CALL-RACF.
      IF irr-safrc NOT = zero then
          DISPLAY "SAF_return_code:      " irr-safrc
          DISPLAY "RACF_return_code:     " irr-racfrc
          DISPLAY "RACF_reason_code:    " irr-racfrsn
      End-if
*-----*
* Call IRRSPK00 requesting a pass ticket *
*-----*
      CALL-RACF.
      CALL W-IRRSPK00 USING irr-workarea,
          IRR-ALET, irr-safrc,
          IRR-ALET, irr-racfrc,
          IRR-ALET, irr-racfrsn,
          IRR-ALET, irr-functionCode,
          irr-optionWord,
          IRR-PASSTICKET,
          irr-ticketOptions-ptr,
          IRR-IDENTITY,
          IRR-APPLID
```



# API Requester - basic authentication and identity assertion



*clientID* – the identity under which the z/OS application is executing.

- For CICS, the CICS task identity
- For IMS, the transaction owner
- For batch, the job card's USERID

*zCEEID* – The identity that is used for authenticating connectivity the z/OS subsystem to the zCEE server. It is configured using basic authentication or for CICS, TLS client authentication. For MVS batch, IMS and Db2 stored procedures, the *zCEEID* is provided by the environment variable *BAQUSERNAME*. For CICS, the value for *zCEEID* is usually provided by the identity mapped to the CICS client certificate.

requireAuth	idAssertion	Actions performed by z/OS Connect
true	OFF	Identity assertion is disabled. The zCEE server authenticates <i>zCEEID</i> and checks whether <i>zCEEID</i> has the authority to invoke an API requester.
	ASSERT_SURROGATE	Identity assertion is enabled. The zCEE server authenticates <i>zCEEID</i> and checks whether <i>zCEEID</i> is a surrogate of <i>clientID</i> . If <i>zCEEID</i> is a surrogate of <i>clientID</i> , the server further checks whether <i>clientID</i> has the authority to invoke an API requester; otherwise, a BAQR7114E message occurs.
	ASSERT_ONLY	Identity assertion is enabled. The zCEE server authenticates <i>zCEEID</i> and directly checks whether <i>clientID</i> has the authority to invoke an API requester
false	OFF	Identity assertion is disabled. A BAQR0407W message occurs.
	ASSERT_SURROGATE	Identity assertion is enabled. The zCEE server checks whether <i>clientID</i> has the authority to invoke an API requester, and a warning message occurs to indicate that the ASSERT_ONLY value is used instead of the ASSERT_SURROGATE value.
	ASSERT_ONLY	Identity assertion is enabled. The zCEE server checks whether <i>clientID</i> has the authority to invoke an API requester

```

<zosconnect_zosConnectManager
    requireAuth="true|false"
    requireSecure="true|false"/>

<zosconnect_apiRequesters idAssertion="OFF">

<zosconnect_apiRequester name="cscvinc_1.0.0"
    requireAuth="true|false"
    requireSecure="true|false"/>
    idAssertion="ASSERT_ONLY"> *

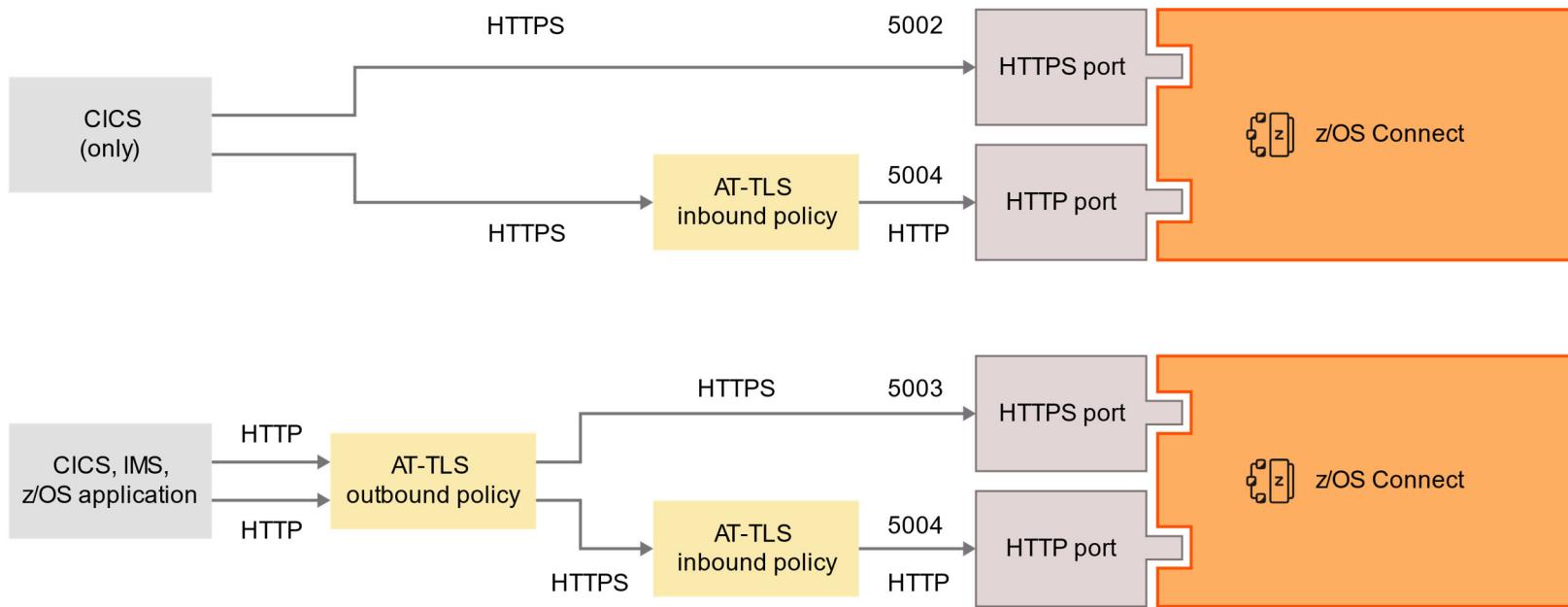
<zosconnect_apiRequester name="db2employee_1.0.0"
    requireAuth="true|false"
    requireSecure="true|false"/>
    idAssertion="ASSERT_SURROGATE"> *

</zosconnect_apiRequesters>

```



# TLS Connection options from an application to the z/OS Connect server





# Tech/Tip: API Requester - HTTP v HTTPS

MVS Batch and IMS with and without an outbound AT-TLS policy

```
CEE0PTS DD *
  POSIX(ON),
  ENVAR("BAQURI=wg31.washington.ibm.com",
  "BAQPORT=9080")
```

```
CEE0PTS DD *
  POSIX(ON),
  ENVAR("BAQURI=wg31.washington.ibm.com",
  "BAQPORT=9443")
```

## CICS URIMAPS

```
WG31
File Edit Settings View Communication Actions Window Help
OVERTYPE TO MODIFY
CEDA ALTER Urimap( BAQURIMP )
Urimap      : BAQURIMP
Group       : SYSGRP
Description ==> URIMAP for z/OS Connect EE server
Status      ==> Enabled   Enabled | Disabled
Usage       ==> Client    Server | Client | Pipeline | Atom
              | Jvmserver
UNIVERSAL RESOURCE IDENTIFIER
Scheme     ==> HTTP      HTTP | HTTPS
Port       ==> 09120    No | 1-65535
HOST       ==> wg31.washington.ibm.com
Path       ==> /
(Mixed Case) ==>
==>
==>
==>
+ OUTBOUND CONNECTION POOLING
SYSID=CICS APPL
PF 1 HELP 2 COM 3 END      6 CRSR 7 SBH 8 SFH 9 MSG 10 SB 11
MBI C
Connected to remote server/host wg31 using lu/pool TCP00133 and port 23
```

```
CICS RELEASE = 0710
File Edit Settings View Communication Actions Window Help
OVERTYPE TO MODIFY
CEDA ALTER Urimap( BAQURIMP )
Urimap      : BAQURIMP
Group       : SYSGRP
Description ==> URIMAP for z/OS Connect EE server
Status      ==> Enabled   Enabled | Disabled
Usage       ==> Client    Server | Client | Pipeline | Atom
              | Jvmserver
UNIVERSAL RESOURCE IDENTIFIER
Scheme     ==> HTTPS     HTTP | HTTPS
Port       ==> 09443    No | 1-65535
HOST       ==> wg31.washington.ibm.com
Path       ==> /
(Mixed Case) ==>
==>
==>
==>
+ OUTBOUND CONNECTION POOLING
SYSID=CICS APPLID=CICS53Z
PF 1 HELP 2 COM 3 END      6 CRSR 7 SBH 8 SFH 9 MSG 10 SB 11 SF 12 CNCL
MBI C
Connected to remote server/host wg31 using lu/pool TCP00133 and port 23
13/022
```

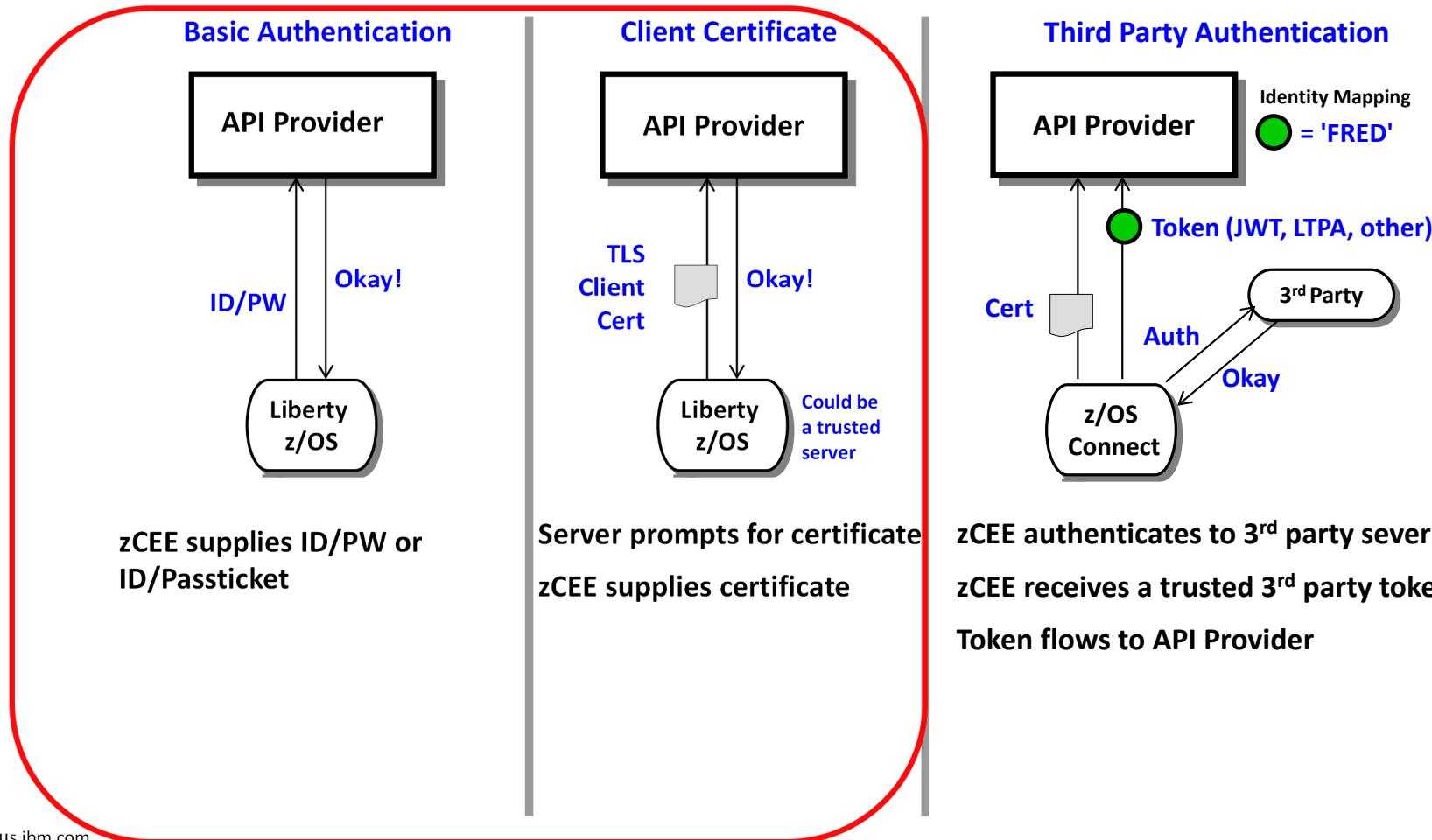
Field BAQ-ZCON-SERVER-URI was added to BAQRINFO in V3.0.37.

MOVE "URIMAP01" TO BAQ-ZCON-SERVER-URI.



# API Requester – Security from the z/OS Connect server to the API provider

Several different ways this can be accomplished:



# Configuring Basic and/or TSL support – z/OS Connect API Requester



Basic authentication with HTTP protocol

```
<zosconnect_endpointConnection id="cscvincAPI"  
    host="http://wg31.washington.ibm.com" port="9080"  
    authenticationConfigRef="myAuthData" />  
  
<zosconnect_authData id="myAuthData"  
    user="zCEEClient" password="secret"/>
```

TLS with HTTPS protocol

```
<zosconnect_endpointConnection id="cscvincAPI"  
    host="https://wg31.washington.ibm.com" port="9443"  
    authenticationConfigRef="myAuthData" 1  
    sslCertsRef="OutboundSSLSettings" />  
  
<zosconnect_authData id="myAuthData" 1  
    user="zCEEClient" password="secret"/>
```

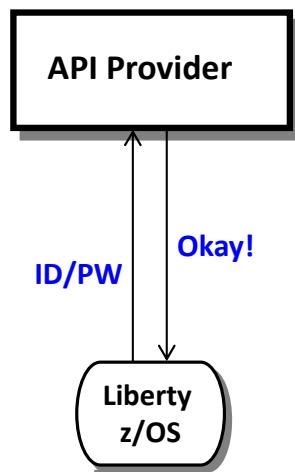
<sup>1</sup> Optional, if mutual authentication is enabled by the server endpoint

# API Requester – Security from the z/OS Connect server to the API provider



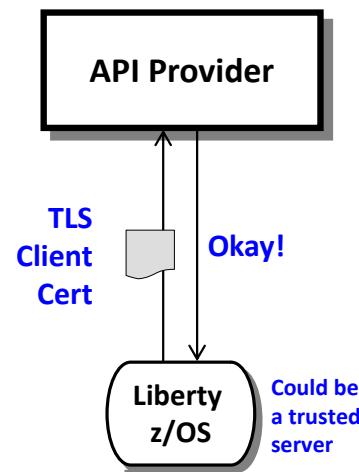
Several different ways this can be accomplished:

## Basic Authentication



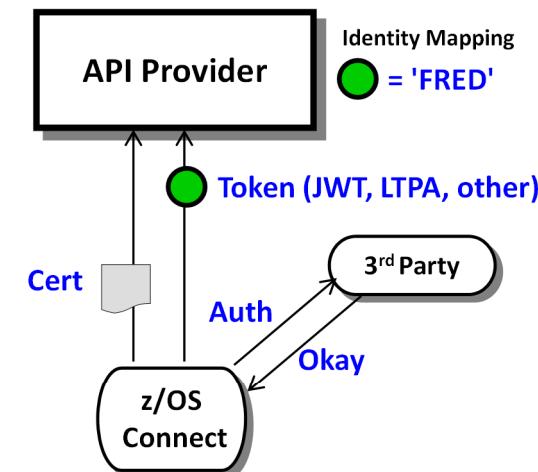
zCEE supplies ID/PW or  
ID/Passticket

## Client Certificate



Server prompts for certificate  
zCEE supplies certificate

## Third Party Authentication



zCEE authenticates to 3<sup>rd</sup> party sever  
zCEE receives a trusted 3<sup>rd</sup> party token  
Token flows to API Provider



# Third Party Authentication Examples

The image displays two examples of third-party authentication:

**Left Example: UPS Sign Up**

This screenshot shows the UPS Sign Up page. At the top, there's a banner stating "UPS is open for business: Service impacts related to Coronavirus ...More". Below the banner, the UPS logo is displayed. There are links for "Sign up / Log in" and "Search or Track". A "Feedback" button is located on the right side. The main section is titled "Sign Up" and includes a link for "Already have an ID? Log in". It says "Use one of these sites." followed by icons for Google, Facebook, Amazon, Apple, and Twitter. Below this, there's a section for "Or enter your own information." with fields for Name\*, Email\*, User ID\*, Password\*, and Phone.

**Right Example: myNCDMV Log In**

This screenshot shows the myNCDMV Log In page. The background features a scenic view of autumn-colored trees. At the top, there are "Log In" and "Sign Up" buttons. The "Log In" button is highlighted. The log in form requires "Email Address" (with placeholder "name@example.com") and "Password" (with placeholder "\*\*\*\*\*"). There's a "Remember Me" checkbox, a "Log In" button, a "Forgot Password" link, and a "Continue as Guest" link. Below the form, there are links for "Continue with Apple", "Continue with Facebook", and "Continue with Google". A note at the bottom states: "NOTICE FOR PUBLIC COMPUTER USERS - If you sign in with Google, Apple, or Facebook you are also signing into that account on this computer. Remember to sign out when you're done." The page is powered by "payit".



# Open security standards

- **OAuth** is an open standard for access delegation, used as a way to grant websites or applications access to their information without requiring a password.
- **OpenID Connect** is an authentication layer on top of OAuth. It allows the verification of the identity of an end-user based on authentication performed by an authorization server.
- **JWT (JSON Web token)** defines a compact and self-contained way for securely transmitting information between parties as a JSON object

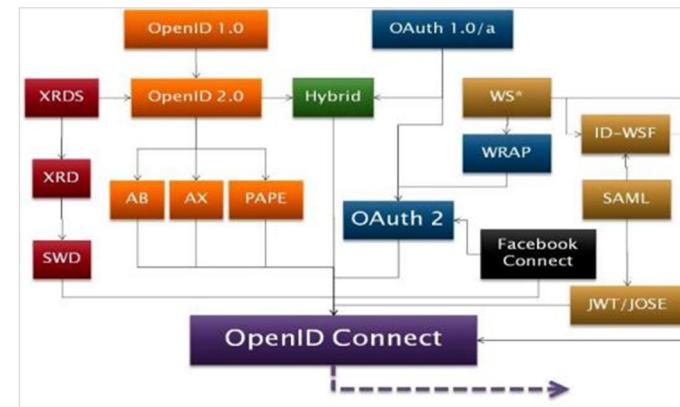
See the YouTube videos:

*OAuth 2.0 and OpenID Connect (in plain English)*

<https://www.youtube.com/watch?v=996OjexHze0>

*OpenID Connect on Liberty*

<https://www.youtube.com/watch?v=fuajCS5bG4c>





# What is a JWT (JSON Web Token) ?

- JWT is a compact way of representing claims that are to be transferred between two parties
- Normally transmitted via HTTP header
- Consists of three parts
  - Header
  - Payload
  - Signature

The screenshot shows the jwt.io debugger interface. On the left, under 'Encoded', is a long string of characters representing the JWT. On the right, under 'Decoded', are the JSON objects for the HEADER and PAYLOAD. A red oval highlights the 'exp' field in the PAYLOAD, which is annotated with 'Mon Nov 02 2020 11:05:58 GMT-0500 (Eastern Standard Time)'.

```
HEADER:
{
  "kid": "4qjX-bkX0Uw_F_uccjRMKB9ivMjXSQwj0RrkYRJq8DM",
  "alg": "RS256"
}

PAYLOAD:
{
  "sub": "Fred",
  "token_type": "Bearer",
  "scope": [
    "openid",
    "profile",
    "email"
  ],
  "azp": "rpSsl",
  "iss": "https://wg31.washington.ibm.com:26213/oidc/endpoint/0",
  "aud": "myZcee",
  "exp": 1604333158,
  "iat": 16043330858,
  "realmName": "zCEERealm",
  "uniqueSecurityName": "Fred"
}
```

Values derived from the OAUTH configuration:

- signatureAlgorithm="**RS256**"
- accessTokenLifetime="**300**"
- resourceIds="**myZcee**"

<https://jwt.io>

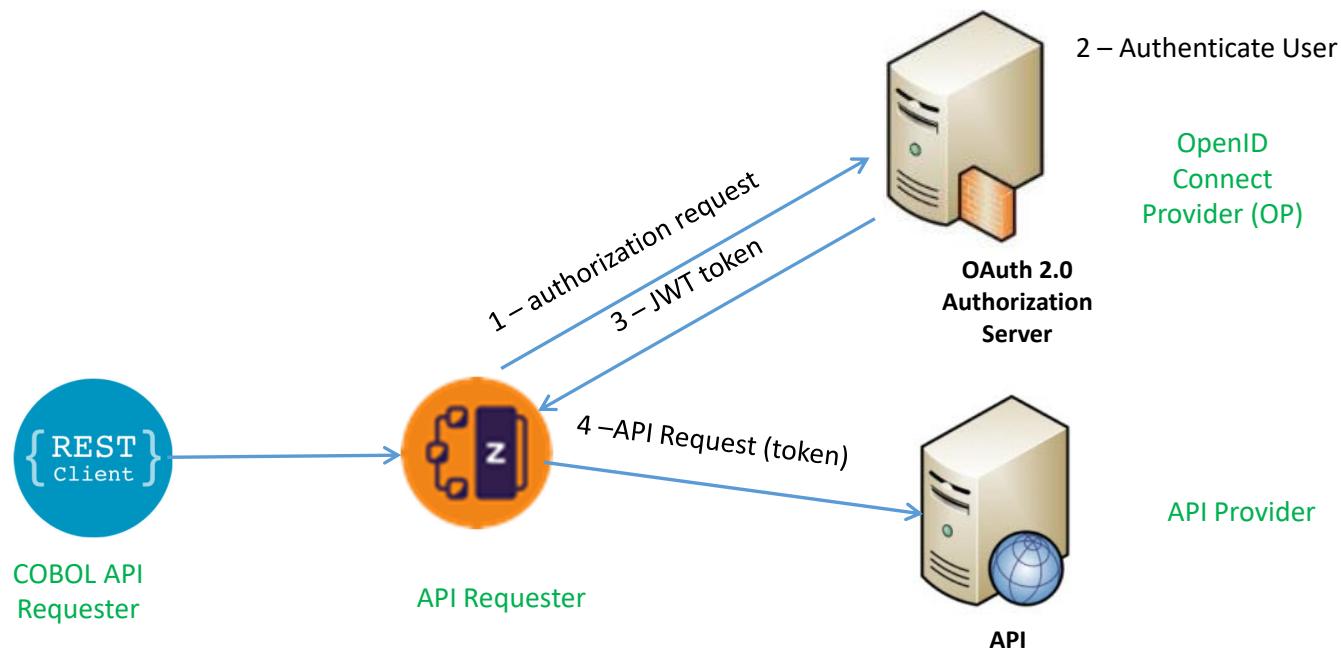
# **z/OS Connect API Requester - Token Support**



z/OS Connect EE provides *three* ways of calling an API secured with a token

1. Use the OAuth 2.0 support when the request is part of an OAuth 2.0 flow. With OAUTH configured, the token can be an opaque token or a JWT token.
1. In a non-OAuth 2.0 scenario, a JWT token is used in a custom flow, for example: when you need to specify the HTTP verb that is used in the request to the authentication server.
  - When you need to specify the HTTP verb that is used in the request to the authentication server
  - When you need to specify how the JWT is returned from the authentication server (for example, in an HTTP header or in a custom field in a JSON response message).
  - When you need to use a custom header name for sending the JWT to the request endpoint.
3. Use the locally generated JWT support when you need to send a JWT that is generated by the z/OS Connect EE server.

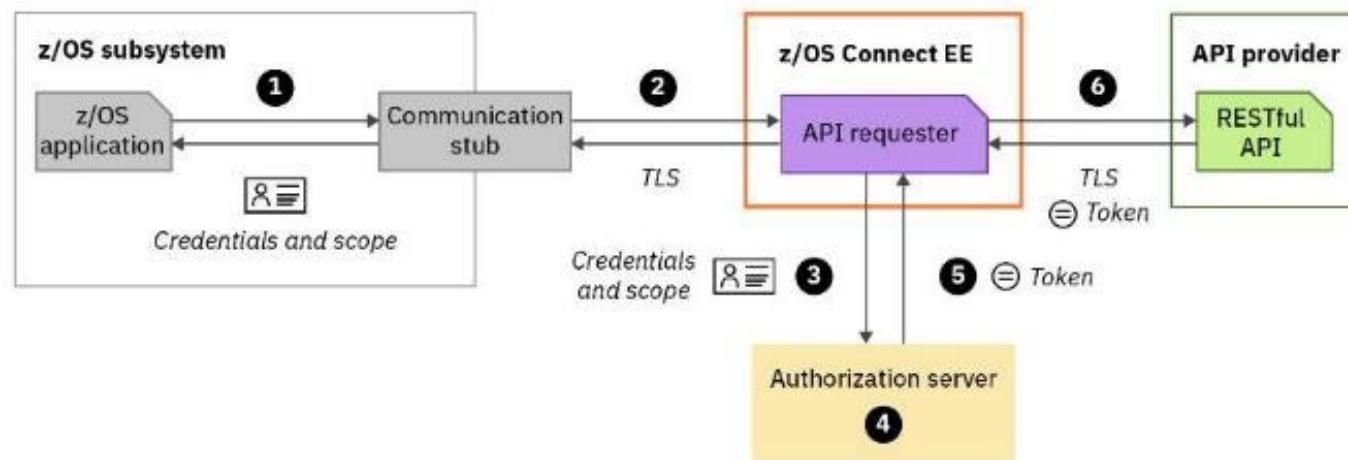
# z/OS Connect OAuth Flow for API requester



## Grant Types:

- client\_credentials
- password

# Calling an API with OAuth 2.0 support





## OAuth Grant Types Supported by z/OS Connect

**client\_credentials** - the identity associated with the combination of the CICS, IMS, or z/OS region and the z/OS Connect EE server that calls the RESTful API on behalf of the CICS, IMS, or z/OS application When this grant type is used, the z/OS Connect EE server sends the client credentials and the access scope to the authorization server.

```
<zosconnect_oAuthConfig id="myoAuthConfig"  
    grantType="client_credentials"  
    authServerRef="myoAuthServer"/>
```

**password** - The identity of the specific identity provided by the CICS, IMS, or z/OS application, or it might be another entity. When this grant type is used, the z/OS Connect EE server sends the resource owner's credentials, the client credentials, and the access scope to the authorization server.

```
<zosconnect_oAuthConfig id="myoAuthConfig"  
    grantType="password"  
    authServerRef="myoAuthServer"/>
```

# OpenID Connect/OAuth and z/OS Connect



- **From the z/OS Connect Knowledge Center:** z/OS Connect EE security can operate with traditional z/OS security, for example, System Authorization Facility (SAF) and also with open standards such as Transport Layer Security (TLS), JSON Web Token (JWT), and **OpenID Connect**.
- **From the OpenID Core specification:** OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.
- **OAuth 2.0 Core (RFC 6749) Specifications:** <https://tools.ietf.org/html/rfc6749>
- **OpenID Connect Core Specifications:** [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)
- **Again, for a very good explanation of this topic see YouTube video OAuth 2.0 and OpenID Connect (in plain English)**  
<https://www.youtube.com/watch?v=996OixHze0>

# Configuring OAuth support – BAQRINFO copy book



```
File Edit Settings View Communication Actions Window Help
Menu Utilities Compilers Help
BROWSE ZCEE30.SBAQCOB(BAQRINFO) Line 0000000028 Col 001 080
Command ==> Scroll ==> PAGE
01 BAQ-REQUEST-INFO.
03 BAQ-REQUEST-INFO-COMP-LEVEL PIC S9(9) COMP-5 SYNC VALUE 4.
03 BAQ-REQUEST-TINFO-USER.
05 BAQ-DAUTH.
07 BAQ-DAUTH-USERNAME PIC X(256).
07 BAQ-DAUTH-USERNAME-LEN PIC S9(9) COMP-5 SYNC
    VALUE 0.
07 BAQ-DAUTH-PASSWORD PIC X(256).
07 BAQ-DAUTH-PASSWORD-LEN PIC S9(9) COMP-5 SYNC
    VALUE A.
07 BAQ-DAUTH-CLIENTID PIC X(256).
07 BAQ-DAUTH-CLIENTID-LEN PIC S9(9) COMP-5 SYNC
    VALUE 0.
07 BAQ-DAUTH-CLIENT-SECRET PIC X(256).
07 BAQ-DAUTH-CLIENT-SECRET-LEN PIC S9(9) COMP-5 SYNC
    VALUE A.
07 BAQ-DAUTH-SCOPE-PTR USAGE POINTER.
07 BAQ-DAUTH-SCOPE-LEN PIC S9(9) COMP-5 SYNC
    VALUE 0.
05 BAQ-AUTHTOKEN.
07 BAQ-TOKEN-USERNAME PIC X(256).
07 BAQ-TOKEN-USERNAME-LEN PIC S9(9) COMP-5 SYNC
    VALUE 0.
07 BAQ-TOKEN-PASSWORD PIC X(256).
07 BAQ-TOKEN-PASSWORD-LEN PIC S9(9) COMP-5 SYNC
    VALUE 0.
05 BAQ-ZCON-SERVER-URI PIC X(256)
    VALUE SPACES.
MA A 04/015
Connected to remote server/host wg31z using lu/pool TCP00145
```

**Grant Type: *password*** - The identity of the user provided by the CICS, IMS, or z/OS application, or it might be another entity.  
Client\_credentials can be supplied by the program or in the server XML configuration.

**Grant Type: *client\_credentials*** - the identity associated with the combination of the CICS, IMS, or z/OS application, and the z/OS Connect EE server that calls the RESTful API on behalf of the CICS, IMS, or z/OS application

**Scope is always required.**

OAuth 2.0 specification entity	password	client_credentials	Where Set
Client ID	required	Required	server.xml or by application
Client Secret	optional	Required	server.xml or by application
Username	required	N/A	by application
Password	required	N/A	by application



# Tech/Tip: Accessing environment variables from COBOL application

```
*****  
** Get the BAQ-OAUTH-USERNAME environment variable  
*****  
MOVE "ATSOAUTHUSERNAME" TO envVariableName.  
PERFORM CALL-CEEENV THRU CALL-CEEENV-END  
IF valueLength NOT = 0 THEN  
    MOVE VAR(1:valueLength) TO BAQ-OAUTH-USERNAME  
    MOVE valueLength TO BAQ-OAUTH-USERNAME-LEN  
    DISPLAY "BAQ-OAUTH-USERNAME: " "  
          BAQ-OAUTH-USERNAME (1:BAQ-OAUTH-USERNAME-LEN)  
ELSE  
    DISPLAY "BAQ-OAUTH-USERNAME: Not found"  
ENDIF.  
*****  
** Get the BAQ-OAUTH-PASSWORD environment variable  
*****  
MOVE "ATSOAUTHPASSWORD" TO envVariableName.  
PERFORM CALL-CEEENV THRU CALL-CEEENV-END  
IF valueLength NOT = 0 THEN  
    MOVE VAR(1:valueLength) TO BAQ-OAUTH-PASSWORD  
    MOVE valueLength TO BAQ-OAUTH-PASSWORD-LEN  
    DISPLAY "BAQ-OAUTH-PASSWORD: " "  
          BAQ-OAUTH-PASSWORD (1:BAQ-OAUTH-PASSWORD-LEN)  
ELSE  
    DISPLAY "BAQ-OAUTH-PASSWORD: Not found"
```

```
CALL-CEEENV.  
MOVE 1 TO functionCode.  
MOVE ZERO TO ws-length.  
INSPECT FUNCTION REVERSE (envVariableName)  
      TALLYING ws-length FOR LEADING SPACES.  
COMPUTE envVariableNameLength =  
      LENGTH OF envVariableName - ws-length.  
MOVE " " TO VAL.  
MOVE 0 TO valueLength.  
CALL "CEEENV" USING functionCode,  
      envVariableNameLength,  
      envVariableName,  
      valueLength,  
      valuePointer,  
      feedbackCode.  
  
IF valueLength NOT = 0 THEN  
    SET ADDRESS OF VAR TO valuePointer .  
  
CALL-CEEENV-END.,
```

# Configuring OAuth support – z/OS Connect API Requester



```
<zosconnect_endpointConnection id="cscvincAPI"
    host="http://wg31.washington.ibm.com" port="9080"
    authenticationConfigRef="myoAuthConfig"/>

<zosconnect_oAuthConfig id="myoAuthConfig"
    grantType="client_credentials|password"
    authServerRef="myoAuthServer"/>

<zosconnect_authorizationServer id="myoAuthServer"
    tokenEndpoint=https://wg31.washington.ibm.com:59443/oidc/endpoint/OP/token1
    basicAuthRef="tokenCredential" 2
    sslCertsRef="OutboundSSLSettings" />

<zosconnect_authData id="tokenCredential" 2
    user="zCEEClient" password="secret"/>
```

```
openidConnectProvider id="OP"
    signatureAlgorithm="RS256"
    keyStoreRef="jwtStore"
    oauthProviderRef="OIDCssl" >
</openidConnectProvider>
```

<sup>1</sup>See URL [https://www.ibm.com/support/knowledgecenter/SS7K4U\\_liberty/com.ibm.websphere.wlp.zseries.doc/ae/twlp\\_oidc\\_token\\_endpoint.html](https://www.ibm.com/support/knowledgecenter/SS7K4U_liberty/com.ibm.websphere.wlp.zseries.doc/ae/twlp_oidc_token_endpoint.html)

<sup>2</sup> These credentials can be specified by the application

# Security Scenarios



```
BAQ-OAUTH-USERNAME: distuser1  
BAQ-OAUTH-PASSWORD: pwd  
EmployeeNumber: 111111  
EmployeeName: C. BAKER  
USERID: USER1
```

*distuser1* is mapped to RACF identity USER1 who has full access

```
BAQ-OAUTH-USERNAME: distuserx  
BAQ-OAUTH-PASSWORD: pwd  
Error code: 00000500
```

```
Error msg:{ "errorMessage": "BAQR1092E: Authentication or authorization failed for the z/OS Connect EE server." }
```

*distuserx* is unknown by the OAuth Provider

```
BAQ-OAUTH-USERNAME: auser  
BAQ-OAUTH-PASSWORD: pwd  
Error code: 0000000403  
rror msg:{ "errorMessage": "BAQR1144E: Authentication or authorization failed for the z/OS Connect EE server." }  
Syslog:  
ICH408I USER(ATSSERV ) GROUP(ATSGRP ) NAME(LIBERTY SERVER  
DISTRIBUTED IDENTITY IS NOT DEFINED:  
auser zCEERealm
```

*auser* is not mapped to a valid RACF identity

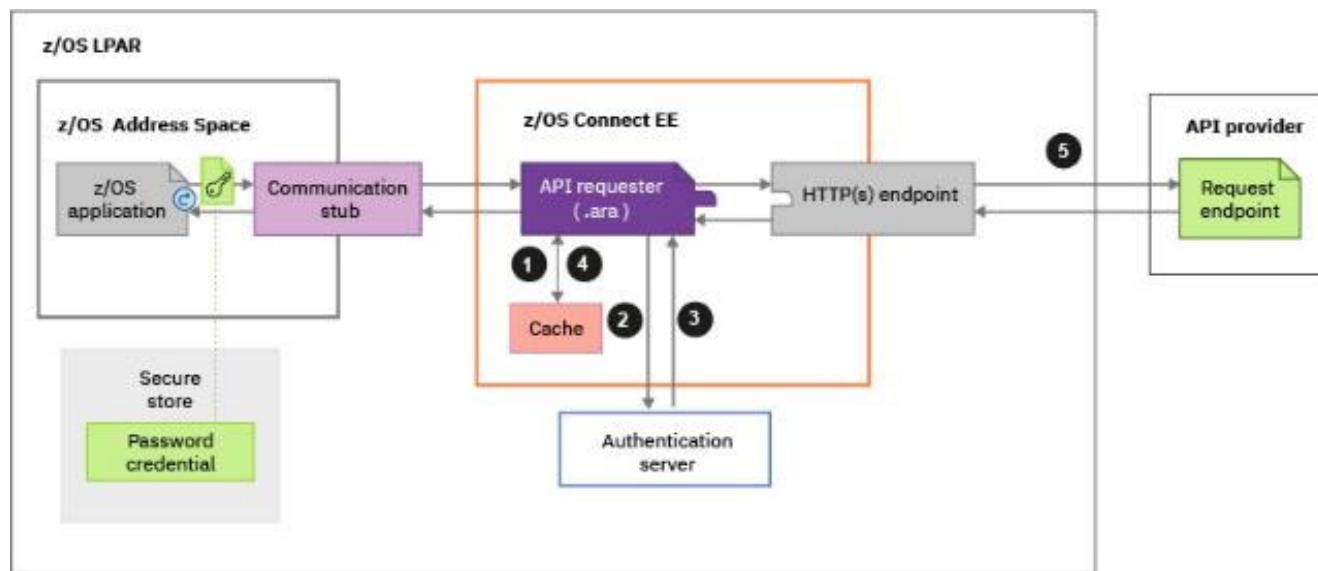
```
BAQ-OAUTH-USERNAME: distuser2  
BAQ-OAUTH-PASSWORD: pwd  
Error code: 0000000403  
Error msg:{ "errorMessage": "BAQR1144E: Authentication or authorization failed for the z/OS Connect EE server." }  
Syslog:  
ICH408I USER(USER2 ) GROUP(SYS1 ) NAME(WORKSHOP USER2  
ATSZDFLT.zos.connect.access.roles.zosConnectAccess  
CL(EJBROLE )  
INSUFFICIENT ACCESS AUTHORITY  
ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

*distuser2* is mapped to RACF identity USER2 which has no access to the EJBRole protecting z/OS Connect

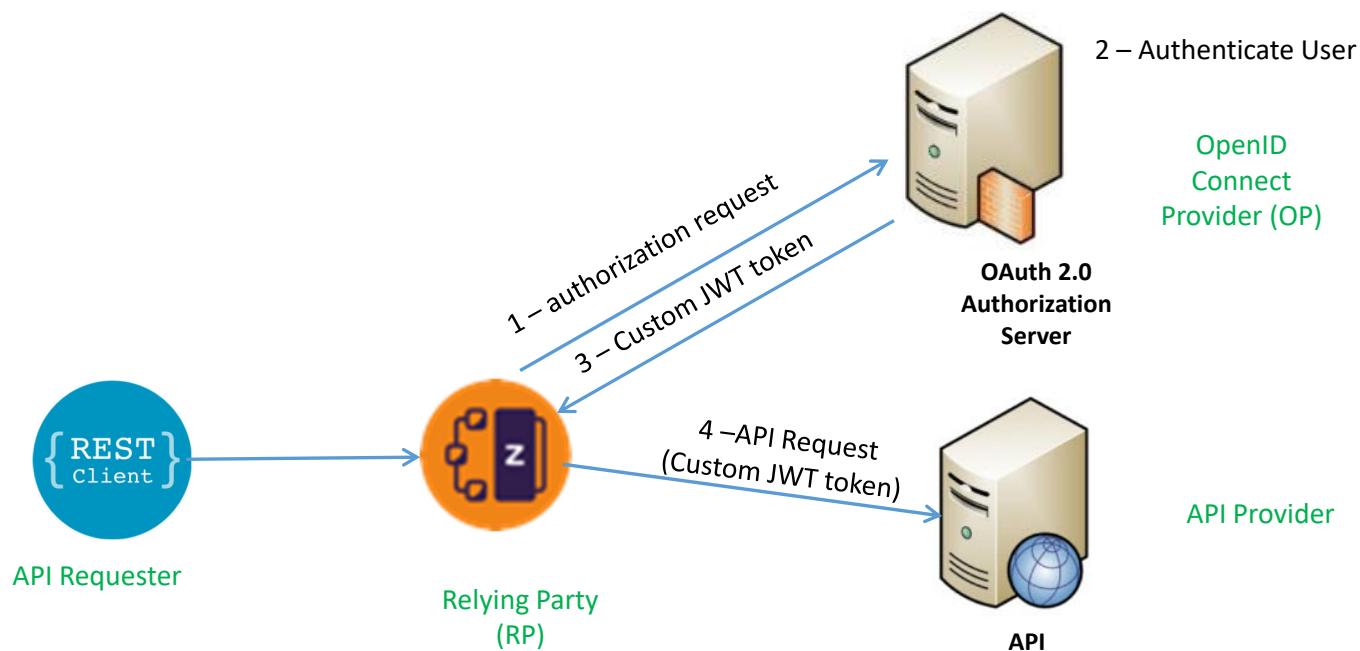


## Calling an API with using a JWT custom flow

- ❑ In a non-OAuth 2.0 scenario, a JWT token is used in a custom flow, for example:
  - When you need to specify the HTTP verb that is used in the request to the authentication server.
  - When you need to specify how the JWT is returned from the authentication server (for example, in an HTTP header or in a custom field in a JSON response message).
  - When you need to use a custom header name for sending the JWT to the request endpoint.



# z/OS Connect OAuth Custom Flow





# API Requester – JWT Custom flow

## BAQRINFO copy book

```
BROWSE ZCEE30.SBAQC0B(BAQRINFO) Line 0000000028 Col 001 080
Command ==> Scroll ==> PAGE
01 BAQ-REQUEST-INFO.
  03 BAQ-REQUEST-INFO-COMP-LEVEL PIC S9(9) COMP-5 SYNC VALUE 4.
  03 BAQ-REQUEST-INFO-USER.
    05 BAQ-DAUTH.
      07 BAQ-DAUTH-USERNAME PIC X(256).
      07 BAQ-DAUTH-USERNAME-LEN PIC S9(9) COMP-5 SYNC
        VALUE 0.
      07 BAQ-DAUTH-PASSWORD PIC X(256).
      07 BAQ-DAUTH-PASSWORD-LEN PIC S9(9) COMP-5 SYNC
        VALUE 0.
      07 BAQ-DAUTH-CLIENTID PIC X(256).
      07 BAQ-DAUTH-CLIENTID-LEN PIC S9(9) COMP-5 SYNC
        VALUE 0.
      07 BAQ-DAUTH-CLIENT-SECRET PIC X(256).
      07 BAQ-DAUTH-CLIENT-SECRET-LEN PIC S9(9) COMP-5 SYNC
        VALUE 0.
      07 BAQ-DAUTH-SCOPE-PTR USAGE POINTER.
      07 BAQ-DAUTH-SCOPE-LEN PIC S9(9) COMP-5 SYNC
        VALUE 0.
  05 BAQ-AUTHTOKEN.
    07 BAQ-TOKEN-USERNAME PIC X(256).
    07 BAQ-TOKEN-USERNAME-LEN PIC S9(9) COMP-5 SYNC
      VALUE 0.
    07 BAQ-TOKEN-PASSWORD PIC X(256).
    07 BAQ-TOKEN-PASSWORD-LEN PIC S9(9) COMP-5 SYNC
      VALUE 0.
  05 BAQ-ZCON-SERVER-URI PIC X(256)
    VALUE SPACES.
04/015
Connected to remote server/host wg31z using lu/pool TCP00145
```

## COBOL application

```
MOVE "ATSTOKENUSERNAME" to envVariableName.
PERFORM CALL-CEEENV THRU CALL-CEEENV-END
MOVE VAR(1:valueLength) to BAQ-TOKEN-USERNAME
MOVE valueLength TO BAQ-TOKEN-USERNAME-LEN
MOVE "ATSTOKENPASSWORD" to envVariableName.
PERFORM CALL-CEEENV THRU CALL-CEEENV-END
MOVE VAR(1:valueLength) to BAQ-TOKEN-PASSWORD
MOVE valueLength to BAQ-TOKEN-PASSWORD-LEN
```

*Note that this example is using environment variables to provide token credentials, as documented in the z/OS Connect Advanced Topics Guide.*



# Configuring JWT Custom flow

```
<zosconnect_endpointConnection id="cscvincAPI"
    host="http://wg31.washington.ibm.com" port="9080"
    authenticationConfigRef="myJWTConfig"/>

<zosconnect_authToken id="myJWTConfig" authServerRef="myJWTServer"
    header="myJWT-header-name"
    <tokenRequest/>      See next slide
    <tokenReponse/>     See next slide
</zosconnect_authToken>

<zosconnect_authorizationServer id="myJWTServer"
    tokenEndpoint=https://wg31.washington.ibm.com:59443/oidc/endpoint/OP/token1
    basicAuthRef="tokenCredential" 2
    sslCertsRef="OutboundSSLSettings" />

<zosconnect_authData id="tokenCredential" 2
    user="zCEEClient" password="secret"/>
```

<sup>1</sup>See URL [https://www.ibm.com/support/knowledgecenter/SS7K4U\\_liberty/com.ibm.websphere.wlp.zseries.doc/ae/twlp\\_oidc\\_token\\_endpoint.html](https://www.ibm.com/support/knowledgecenter/SS7K4U_liberty/com.ibm.websphere.wlp.zseries.doc/ae/twlp_oidc_token_endpoint.html)

<sup>2</sup> These credentials can be specified by the application



# Configuring Custom JWT flow

## Request Token Example 1

```
<tokenRequest  
    credentialLocation="header"  
    header="Authorization"  
    requestMethod="GET" />
```

## Response Token

```
<tokenResponse  
    tokenLocation="header"  
    header="JWTAuthorization" />
```

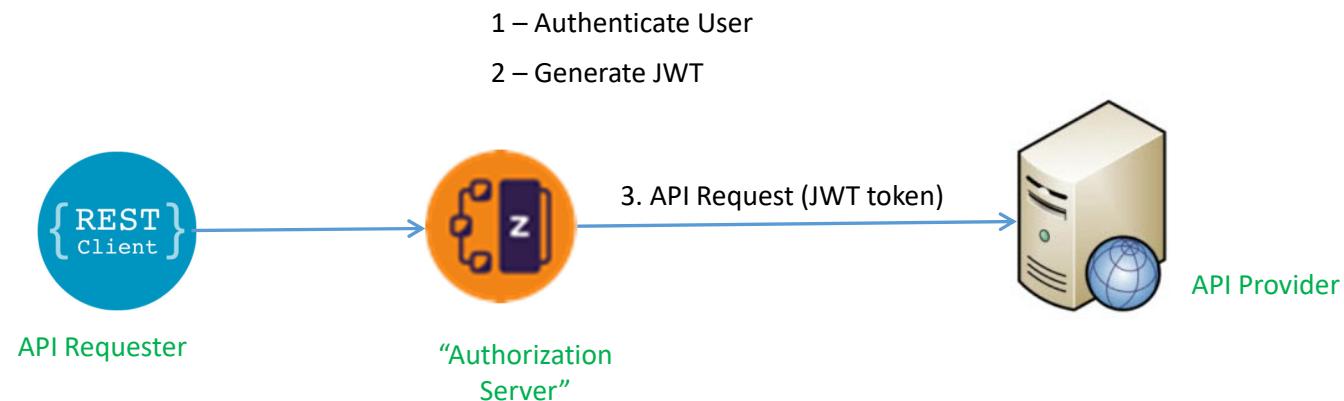
## Response Token Example 2

```
<tokenRequest credentialLocation="body"  
    requestMethod="POST"  
    // Use XML escaped characters in requestBody  
    requestBody="
```

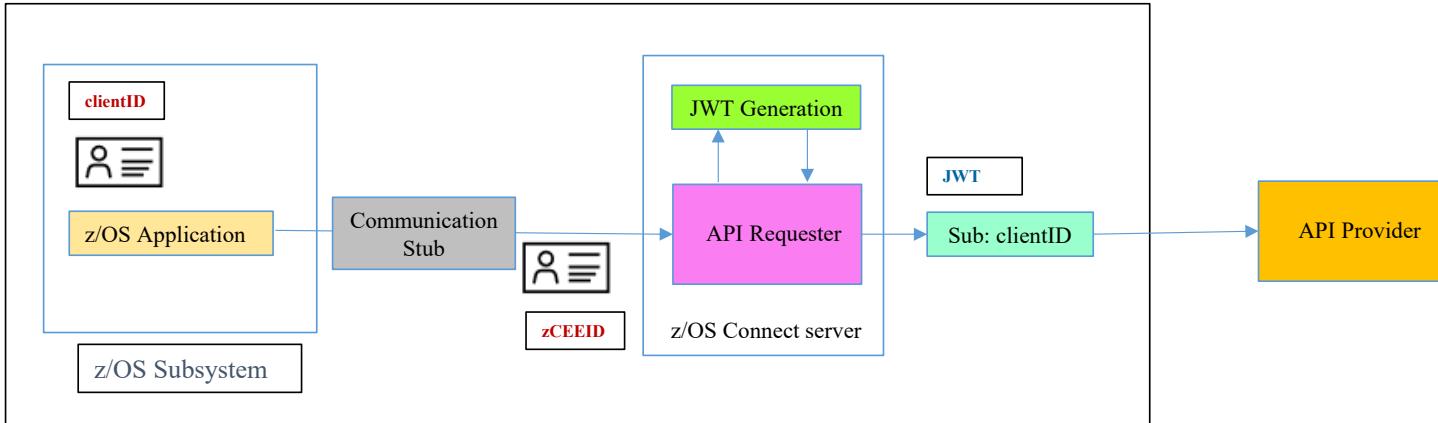
## Response Token

```
<tokenResponse  
    tokenLocation="body"  
    responseFormat="JSON"  
    tokenPath="$&.tokenname" />
```

# z/OS Connect JWT Generation – V3.0.43



# API Requester – JWT Generation



***zCEEID*** – The identity that is used for authenticating connectivity the z/OS subsystem to the zCEE server. It is configured using basic authentication or for CICS, TLS client authentication.

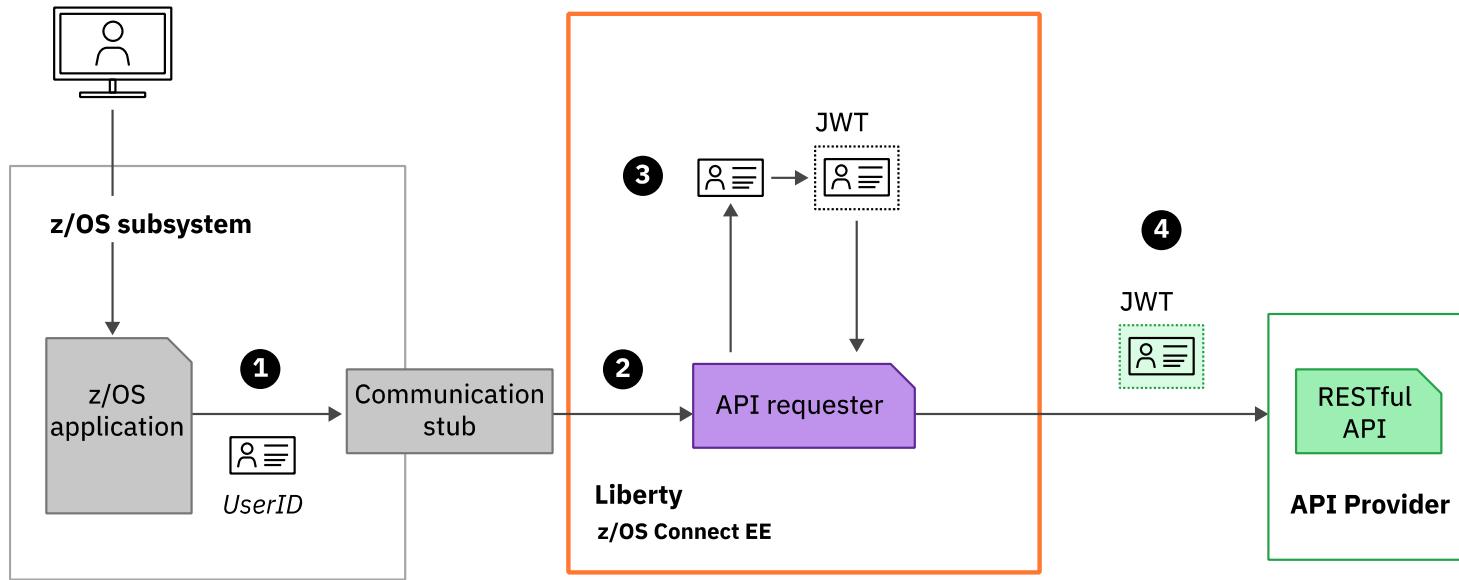
***clientID*** – the identity under which the z/OS application is executing.

- For CICS, the task owner
- For IMS, the transaction owner
- For batch, the job owner

requireAuth	idAssertion	Actions performed by z/OS Connect
true	ASSERT_SURROGATE	Identity assertion is enabled. The zCEE server authenticates <b><i>zCEEID</i></b> and checks whether <b><i>zCEEID</i></b> is a surrogate of <b><i>clientID</i></b> . If <b><i>zCEEID</i></b> is a surrogate of <b><i>clientID</i></b> , the server further checks whether <b><i>clientID</i></b> has the authority to invoke an API requester; otherwise, a BAQR7114E message occurs.
	ASSERT_ONLY	Identity assertion is enabled. The zCEE server authenticates <b><i>zCEEID</i></b> and directly checks whether <b><i>clientID</i></b> has the authority to invoke an API requester
false	ASSERT_SURROGATE	Identity assertion is enabled. The zCEE server checks whether <b><i>clientID</i></b> has the authority to invoke an API requester, and a warning message occurs to indicate that the ASSERT_ONLY value is used instead of the ASSERT_SURROGATE value.
	ASSERT_ONLY	Identity assertion is enabled. The zCEE server checks whether <b><i>clientID</i></b> has the authority to invoke an API requester



# JWT Generation



- 1** Communication stub extracts the ID from the application environment
- 2** z/OS Connect generates a JWT token containing the z/OS application asserted user ID
- 3** The JWT is used to authorise the request to the API endpoint



## Configuring JWT Generation support

```
<zosconnect_endpointConnection id="conn"
    host="http://api.server.com" port="8080"
    authenticationConfigRef="jwtConfig" />

<zosconnect_authTokenLocal id="jwtConfig"
    tokenGeneratorRef="jwtBuilder"
    header="Authorization" >
    <claims>{ "name":"JohnSmith",
        "ID":"1234567890" }
    </claims> One or more Public claim (e.g., aud,exp,nbf,iat,jti) or
one or more private claims

<jwtBuilder id="jwtBuilder"
    scope="scope1"
    audiences="myApp1"
    jti="true"
    signatureAlgorithm="RS256"
    keyStoreRef="myKeyStore"
    keyAlias="jwtsigner"
    issuer="z/OS Connect EE Default"/>
```

The "sub" claim value will be application asserted user ID.

# Configuring JWT Generation support



```
<zosconnect_endpointConnection id="conn1"  
    host="http://api.server.com" port="8080"  
    authenticationConfigRef="jwtConfig" />  
<zosconnect_endpointConnection id="conn2"  
    host="http://api.server.com" port="8080"  
    authenticationConfigRef="jwtConfig" />  
<zosconnect_authTokenLocal id="jwtConfig"  
    tokenGeneratorRef="jwtBuilder"  
    header="Authorization" >  
    <claims>{"scope":"Scope1"}</claims>  
<zosconnect_authTokenLocal id="jwtConfig"  
    tokenGeneratorRef="jwtBuilder"  
    header="Authorization" >  
    <claims>{"scope":"Scope2"}</claims>  
<jwtBuilder id="jwtBuilder"  
    scope="scope"  
    audiences="myApp1"  
    jti="true"  
    signatureAlgorithm="RS256"  
    keyStoreRef="myKeyStore"  
    keyAlias="jwtSigner"  
    issuer="z/OS Connect EE Default"/>
```

# server XML Configuration

```
→<jwtBuilder id="jwtBuilder"
  scope="scope1"
  audiences="myApp1"
  jti="true"
  signatureAlgorithm="RS256"
  keyStoreRef="myKeyStore"
  keyAlias="jwtSigner"
  issuer="z/OS Connect EE Default"/>

→<zosconnect_authTokenLocal id="jwtConfig"
  tokenGeneratorRef="jwtBuilder"
  header="JWTAuthorization" >
  <claims>{"name":"JohnSmith,
    "ID":"1234567890"}</claims>
</zosconnect_authTokenLocal >
<zosconnect_endpointConnection id="conn"
  host="http://api.server.com" port="8080"
  authenticationConfigRef="jwtConfig" />
```

Configure the Liberty jwtBuilder element in server.xml.

Configure the zosconnect\_authTokenLocal element, specifying any additional private claims required and the name of the header used to send the JWT to the endpoint.

header default value is Authorization

Finally, reference the JWT configuration from the zosconnect\_endpointConnection element.

# **z/OS Connect Wildfire Github Site** <https://ibm.biz/BdPRGD>



The image displays three GitHub repository pages side-by-side, each featuring a red oval highlighting specific file uploads.

**Left Repository:** <https://github.com/ibm-wsc/zCONNEE-Wildfire-Workshop>

- Commits:** emitchj Add files via upload (8e503b5)
- Files:**
  - AdminSecurity Delete ZC2OMVS2.jcl
  - OpenAPI2 Delete Developing
  - cobol Add files via upload
  - xml Add files via upload
  - README.md Update README.md
  - ZCADMIN - zOS Connect Administrat... Add files via upload
  - ZCESEC - zOS Connect Security.pdf Add files via upload
  - ZCINTRO - Introduction to zOS Conn... Add files via upload
  - ZCREQUEST - Introduction to zOS Co... Add files via upload** (highlighted by a red oval)
  - zOS Connect EE V3 Advanced Topics ... Add files via upload
  - zOS Connect EE V3 Getting Started.pdf Add files via upload
- README.md**
- Notes:** This repository contains material from the z/OS Connect EE Wildfire workshops run by the IBM Center. It is should be referenced frequently for updates to the presentations, exercises, sam...

**Middle Repository:** <https://github.com/ibm-wsc/zCONNEE-Wildfire-Workshop> (Public)

- Commits:** emitchj Delete Developing (d880029 on Apr 23)
- Files:**
  - Developing CICS API Requester Applications.pdf Add files via upload (2 months ago)
  - Developing IMS API Requester Applications.pdf Add files via upload (2 months ago)
  - Developing MVS Batch API Requester Applications.pdf Add files via upload (2 months ago)

**Bottom Repository:** <https://github.com/ibm-wsc/zCONNEE-Wildfire-Workshop> (Public)

- Commits:** emitchj Add files via upload (428fc6c 5 days ago)
- Files:**
  - Developing CICS API Requester Applications.pdf Add files via upload (5 days ago)
  - Developing IMS API Requester Applications.pdf Add files via upload (5 days ago)
  - Developing MVS Batch API Requester Applications.pdf Add files via upload (5 days ago)

- **Contact your IBM representative to schedule access to these exercises**

WSC wants your  
feedback!

## What you will see:

**From:** IBM Client Feedback <[ibm@feedback.ibm.com](mailto:ibm@feedback.ibm.com)>  
**Subject:** Got a minute? Two questions on your IBM Z Washington Systems Center experience

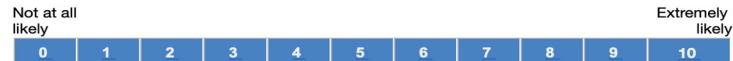


**Dear**

Thank you for engaging with our team. At IBM Z Washington Systems Center, we make it a priority to listen to our clients and want to continuously improve your experience. So, we would love your candid feedback on how we are doing. Please take a moment to answer two short questions about your experience.

You can begin the survey by answering this question.

## **How likely are you to recommend IBM Z Washington Systems Center to others?**



Sincerely,

IBM Advocacy Team

**\*\*you will NOT receive a new survey if you already responded to an IBM Survey from Medallia in the last **60 days** OR if you haven't responded within the last **30 days**\*\***



Thank you for listening and your questions.

**And thank you for completing the Medallia survey**

mitchj@us.ibm.com

© 2018, 2023 IBM Corporation  
Slide 92