

Appendix G to Annex A

Technical specification of the Mobile Access Gateway Solution (draft – informative)

Version 1.3
Date: 22-6-2015

Table of Contents

1. Objectives	4
2. Context Diagram	4
3. Technology	5
4. WP1 Functional Requirements	5
4.1 Mobile Gateway functions.....	5
4.2 Authentication and Authorization Rules	6
4.3 Business Services interface.....	6
5. Use Cases Diagram.....	7
6. Requirements/Use Case Relationship	7
7. Use Case Definition	8
7.1 WP1_UC01 – User Authentication	8
7.1.1 Activity Diagram.....	9
7.2 WP1_UC02 – User Authorization	9
7.2.1 Activity Diagram.....	10
7.3 WP1_UC03 – Forgot Password.....	10
7.3.1 Activity Diagram.....	11
7.4 WP1_UC04 – Access Resource	11
7.4.1 Activity Diagram.....	12
7.5 WP1_UC05 – User Logout	12
7.5.1 Activity Diagram.....	13
8. Topology	14
8.1 Development Environment.....	14
8.2 Pre-Production Environment.....	15
8.3 Production Environment.....	16
9. Requirements	17
9.1 Hardware.....	17
9.1.1 Development Environment	17
9.1.2 Pre-Prod Environment	17
9.1.3 Production Environment	17
9.2 Software	17
9.3 Access Requirements	17
9.4 Connectivity Matrix.....	17
9.4.1 Development Environment	17
9.4.2 Pre-Prod Environment	18
9.4.3 Production Environment	19
9.5 Platforms Integration.....	19
9.5.1 Web Services To Publish and Secure	19
9.5.2 LDAP Group.....	20
9.5.3 Oracle Access Manager	20
9.6 API Gateway Services	20
9.6.1 EMSA User Login Service Specification.....	21
9.6.2 EMSA User Logout Service Specification	21
9.6.3 EMSA Forgot Password Service Specification.....	21
9.7 API Gateway Installation.....	22
9.7.1 API Gateway Core Server	22



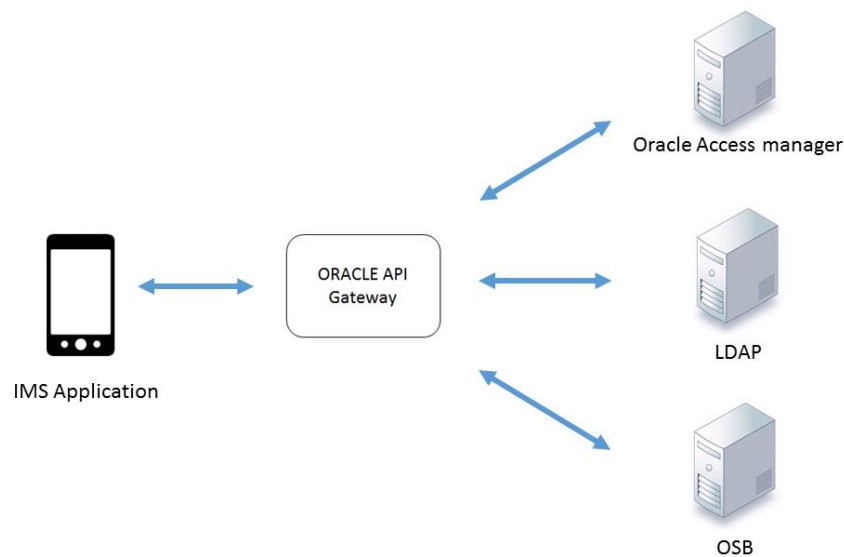
9.7.2	Policy Studio	22
9.7.3	API Gateway Explorer	23
9.7.4	Configuration Studio	24
9.7.5	API Gateway Manager.....	24
9.8	API Gateway Audit and Logs	25
9.8.1	Domain audit logs	25
9.8.2	API Gateway trace files	27
9.8.3	Log files list	28

1. Objectives

The objective of this document is to provide a technical specification of the Mobile Access Gateway Solution. The presented solution will extend the current EMSA IdM infrastructure to allow IMS Mobile application to make user authentication against the EMSA IdM infrastructure.

2. Context Diagram

The following image presents Context diagram of the Mobile Access Gateway Solution.



The Interfaces that will be used between the components presented on the previous image are the following:

IMS App – Oracle API Gateway

- Request for LoginIn/Authentication: When a user performs a Login in the IMS App, a HTTP Basic Authentication is sent the Oracle API Gateway (OAG).
- Request for Resources: Each time the IMS Mobile App needs to access a resource, the request is sent to the OAG.
- Request for Forget Password: When a user forget the password, he may use a Forget Password functionality that will send a Forget Password Request into the Oracle API Gateway.
- Request for LogOut: When a user performs a LogOut on the IMS Application, a Logout request is sent to the Oracle API Gateway in order to invalidate the TOKEN generated by the OAM, during the Authentication.

Oracle API Gateway – Oracle Access Manager

- Request for Authentication: All the Authentication/Log In action received from the IMS Mobile Application are sent to the Oracle Access Manager to validate the user credentials.
- Request for TOKEN Validation: Each time the OAG receive a request with an authentication token, it validates on the OAM if the TOKEN is still valid.



- Request for LogOut: When the OAG receives a Log out request it sends a request to OAM in order to invalidate the authentication Token.

Oracle API Gateway – LDAP

- Request for User Groups: The OAG access LDAP in order to validate if the Authenticated user belongs to a specific Group.

Oracle API Gateway – OSB

- Request for Resource: When the OAG receives an Authenticated and Authorized request for a resource, the request is forward to the resource.

3. Technology

The technology that is implemented during the project is Oracle API Gateway. During the project the acronym used is MAG that stands for Mobile Access Gateway.

4. WP1 Functional Requirements

In this chapter we present all the Functional Requirements identified

4.1 Mobile Gateway functions

Identifier:	EXTIDM_WP1_04
Title:	Mobile Gateway functions
Description	The Mobile Access Gateway should implement the functionalities to ensure that only EMSA authorized users will properly use the IMS Mobile Application and be able to access EMSA's resources. Functions shall cover (but not limited to): 1) Provide user authentication and authorization (e.g. for login/logout) 2) Identify the user's roles 3) Interface to current EMSA IdM infrastructure "Forgot password" function 4) Allow access to EMSA resources (e.g. Web Services)

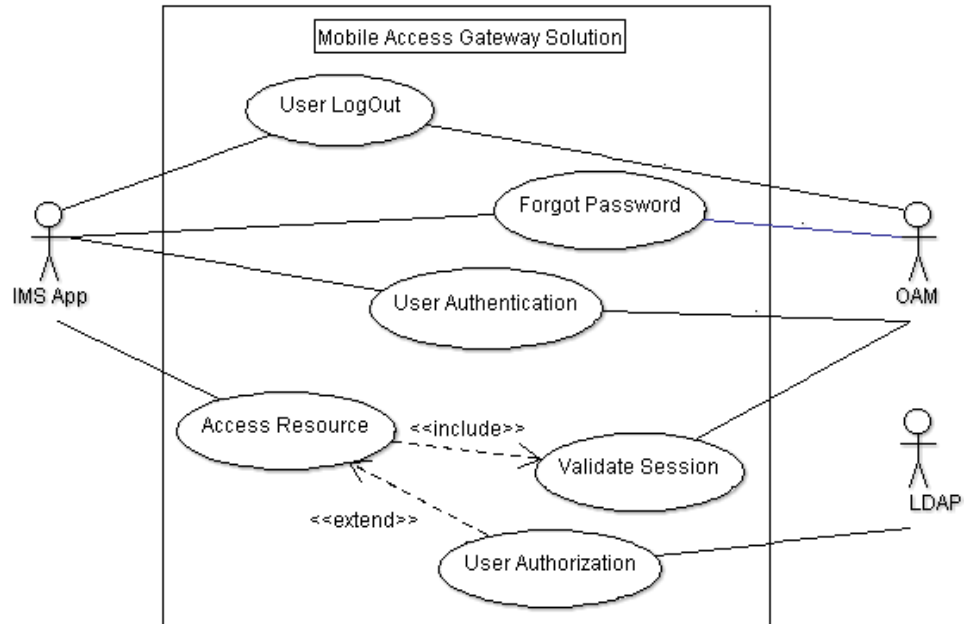
4.2 Authentication and Authorization Rules

Identifier:	EXTIDM_WP1_05
Title:	Authentication and Authorization Rules
Description	<p>Mobile Access Gateway shall provide user authentication and authorization. Authentication shall take in consideration three user attributes:</p> <ol style="list-style-type: none"> 1) User Id 2) User password 3) User Status (e.g. active or disable) <p>Authorization shall take in consideration user roles:</p> <ol style="list-style-type: none"> 1) If the user is member of one or more roles, authorization is to be granted. Otherwise access is rejected <p>User attributes and roles are organized as detailed in Appendix A and stored in an openLDAP.</p> <p>User attributes and roles should be obtained preferably through IdM APIs or as a second option, directly from openLDAP (read only access).</p> <p>The set of roles allowing access shall be configurable in a per Mobile Application base, without the need of rebuild any component of the system.</p>

4.3 Business Services interface

Identifier:	EXTIDM_WP1_06
Title:	Business Services interface
Description	<p>IMS Mobile Application will consume business services exposed in the Integration Tier through REST Web Services.</p> <p>Mobile Access Gateway shall be able to protect them with user authentication and authorization.</p>

The following image represent the Use Case Diagram with all the Use Cases that satisfy all the identified Requirements.



6. Requirements/Use Case Relationship

In this chapter we identify all the relevant Use Cases and their relationship between the Requirements.

Use Case	Requirement
WP1_UC01 – User Authentication	EXTIDM_WP1_04 EXTIDM_WP1_05
WP1_UC02 – User Authorization	EXTIDM_WP1_04 EXTIDM_WP1_05
WP1_UC03 – Forgot Password	EXTIDM_WP1_04
WP1_UC04 – Access Resource	EXTIDM_WP1_04 EXTIDM_WP1_06
WP1_UC05 – User Logout	EXTIDM_WP1_04

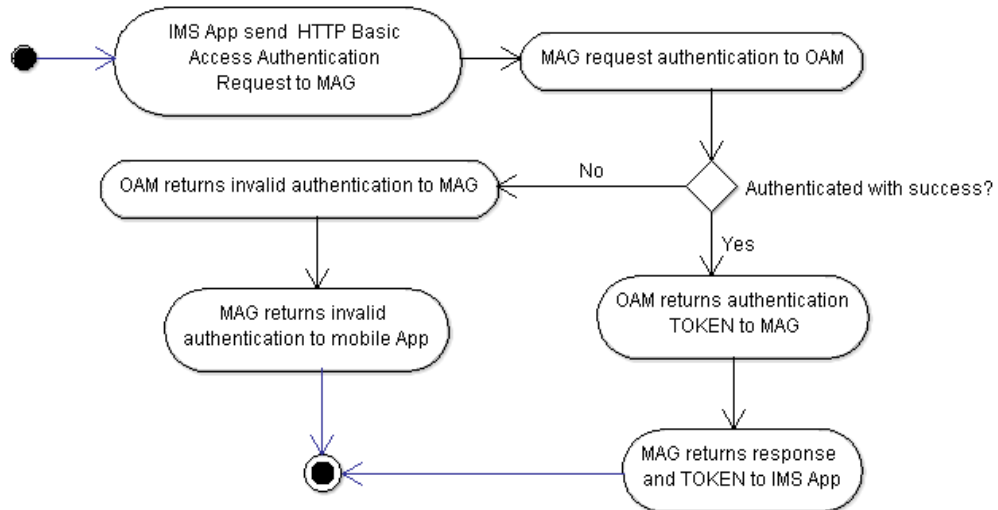
7. Use Case Definition

In this Chapter we describe all the Identified Use Cases, identifying all the Actors, Precondition and Principal and alternative flows.

7.1 WP1_UC01 – User Authentication

Identifier:	WP1_UC01
Title:	User Authentication

Actors:	IMS App; MAG; OAM
Description:	Authenticate user on the mobile App
Preconditions:	<ul style="list-style-type: none"> ● User exist on LDAP ● User has inserted user name and password on IMS APP
Trigger:	User needs to access the IMS App
Main Flow:	
1	IMS App requests direct authentication with Basic HTTP Authentication to MAG (username and password). Using the method "GET" with HTTP Basic Authentication, the client's username and password are concatenated, base64-encoded, and passed in the Authorization HTTP header (e.g. Authorization: Basic ZmF1c3RwYV9zc24zOkFiY2QxMjM0NQ==)
2	MAG request authentication to OAM
3	OAM validates user authentication and status with success
4	OAM returns validation with TOKEN to MAG
5	MAG returns validation with TOKEN to mobile App
6	User is logged in IMS App with success
Alternate Flow 6a:	
1	OAM doesn't validate with success due to user inactive or incorrect password
2	OAM returns invalid authentication to MAG
3	MAG returns invalid authentication to mobile App
4	User gets generic error message indicating that the authentication has failed.
Related Requirements:	<ul style="list-style-type: none"> ● EXTIDM_WP1_04 ● EXTIDM_WP1_05
Notes:	-

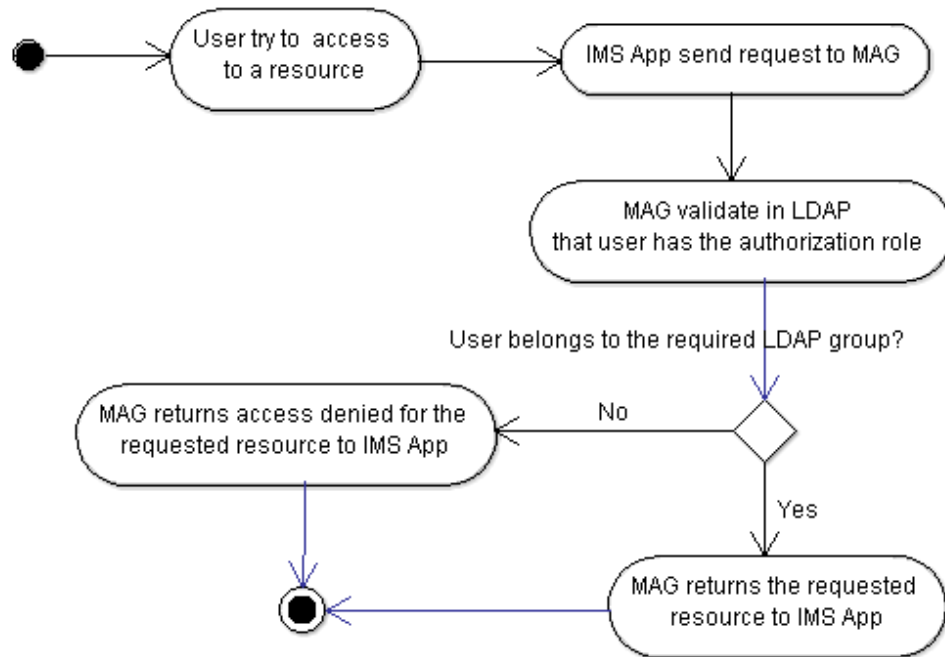


7.2 WP1_UC02 – User Authorization

Identifier:	WP1_UC02
Title:	User Authorization

Actors:	IMS App; MAG; LDAP
Description:	Authorize user access based on user roles
Preconditions:	<ul style="list-style-type: none"> ● User must have the role that grants access ● User is already authenticated
Trigger:	User tries to access a IMS App resource
Main Flow:	
1	User tries to access to a resource
2	IMS App send request to MAG
3	MAG validate in LDAP that user has the authorization role
4	MAG returns the requested resource to IMS App
Alternate Flow 3a:	
1	MAG validate in LDAP that the User hasn't the authorization role
2	MAG returns access denied for the requested resource to IMS App
Related Requirements:	<ul style="list-style-type: none"> ● EXTIDM_WP1_04 ● EXTIDM_WP1_05
Notes:	-

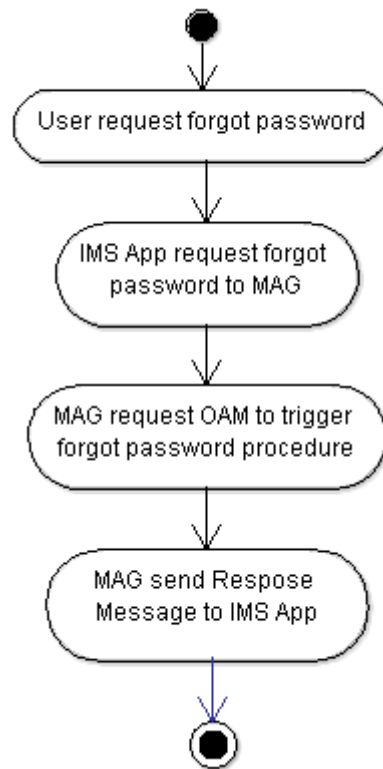
7.2.1 Activity Diagram



7.3 WP1_UC03 – Forgot Password

Identifier:	WP1_UC03
Title:	Forgot password

Actors:	IMS App; MAG; OAM
Description:	The user must be able to reset the password through self-service
Preconditions:	<ul style="list-style-type: none"> ● User must exist on LDAP ● User must have access to forgot password service
Trigger:	User doesn't remember his password
Main Flow:	
1	User request for a "forgot password" Service
2	IMS App request forgot password to MAG, sending the User Id
3	MAG access the forgot password IdM page URL in order to trigger the actual process of Lost Password. The actual Lost Password process will send an email to the user and the user must follow the procedures indicated on the email to reset the password.
4	MAG sends the response to IMS App indicating that one email has been sent to user, and indicating the ticket id of the request.
Related Requirements:	<ul style="list-style-type: none"> ● EXTIDM_WP1_04
Notes:	-



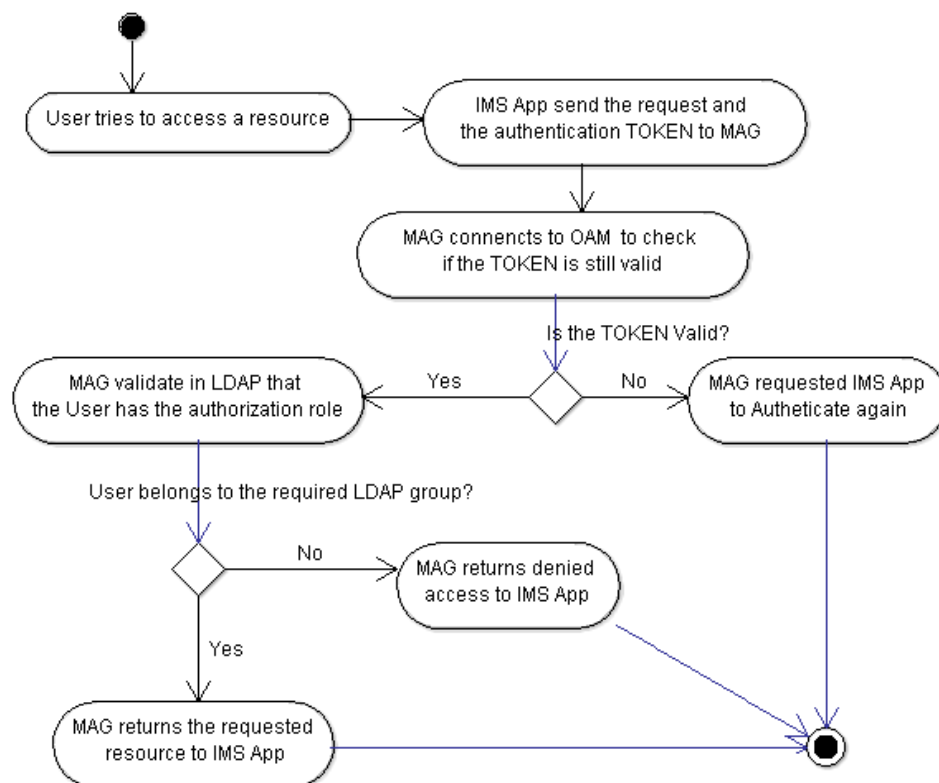
7.4 WP1_UC04 – Access Resource

Identifier:	WP1_UC04
Title:	Access Resource

Actors:	IMS App; MAG; OAM; LDAP
Description:	User has access to resources based on user roles
Preconditions:	<ul style="list-style-type: none"> ● User must have the role that grants access ● User is already authenticated
Trigger:	User tried to access a protected resource on the IMS App
Main Flow:	
1	User tries to access a resource
2	IMS App send request and the Authentication TOKEN to MAG. For every resource request the ssession token must be sent in the HTTP Header.
3	MAG request OAM to validate the TOKEN
4	OAM validates the TOKEN for the session authentication with success
5	MAG validate in LDAP that the User has the authorization role
6	MAG returns the requested resource to IMS App

Alternate Flow 4a:	
1	OAM validates the TOKEN for the session authentication without success
2	MAG requested authentication to IMS App
Alternate Flow 5a:	
1	MAG validate in LDAP that the User doesn't have the authorization role
2	MAG returns denied access to IMS App
Related Requirements:	● EXTIDM_WP1_05
Notes:	-

7.4.1 Activity Diagram



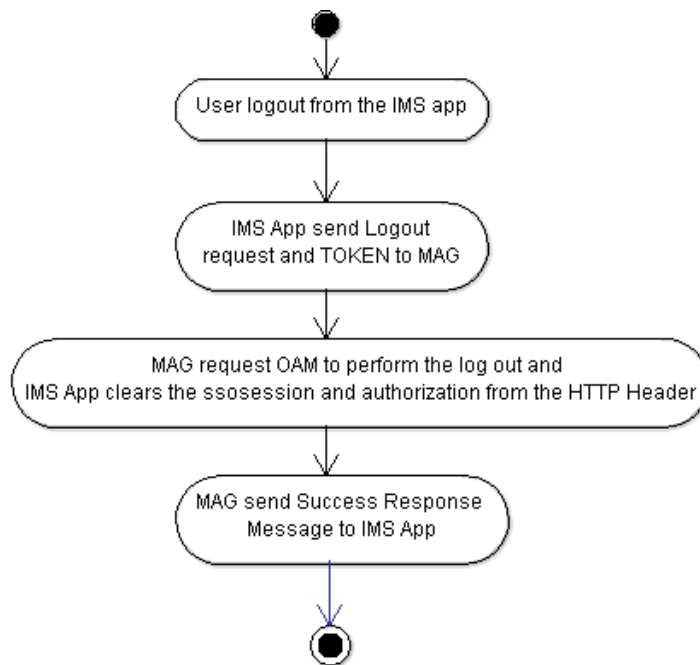
7.5 WP1_UC05 – User Logout

Identifier:	WP1_UC05
Title:	User Logout

Actors:	IMS App; MAG; OAM
Description:	User logout with token revoked
Preconditions:	● User must have the User Status equals to active ● IMS app is already authenticated

Trigger:	User wants to LogOut from the IMS App
Main Flow:	
1	User logout from the IMS app
2	IMS App send Logout request and TOKEN to MAG
3	MAG request OAM to perform the log out and IMS App clears the sso session and authorization from the HTTP Header
4	MAG send Success Response Message to IMS App
5	User is logged out
Related Requirements:	<ul style="list-style-type: none"> ● EXTIDM_WP1_04 ● EXTIDM_WP1_06
Notes:	-

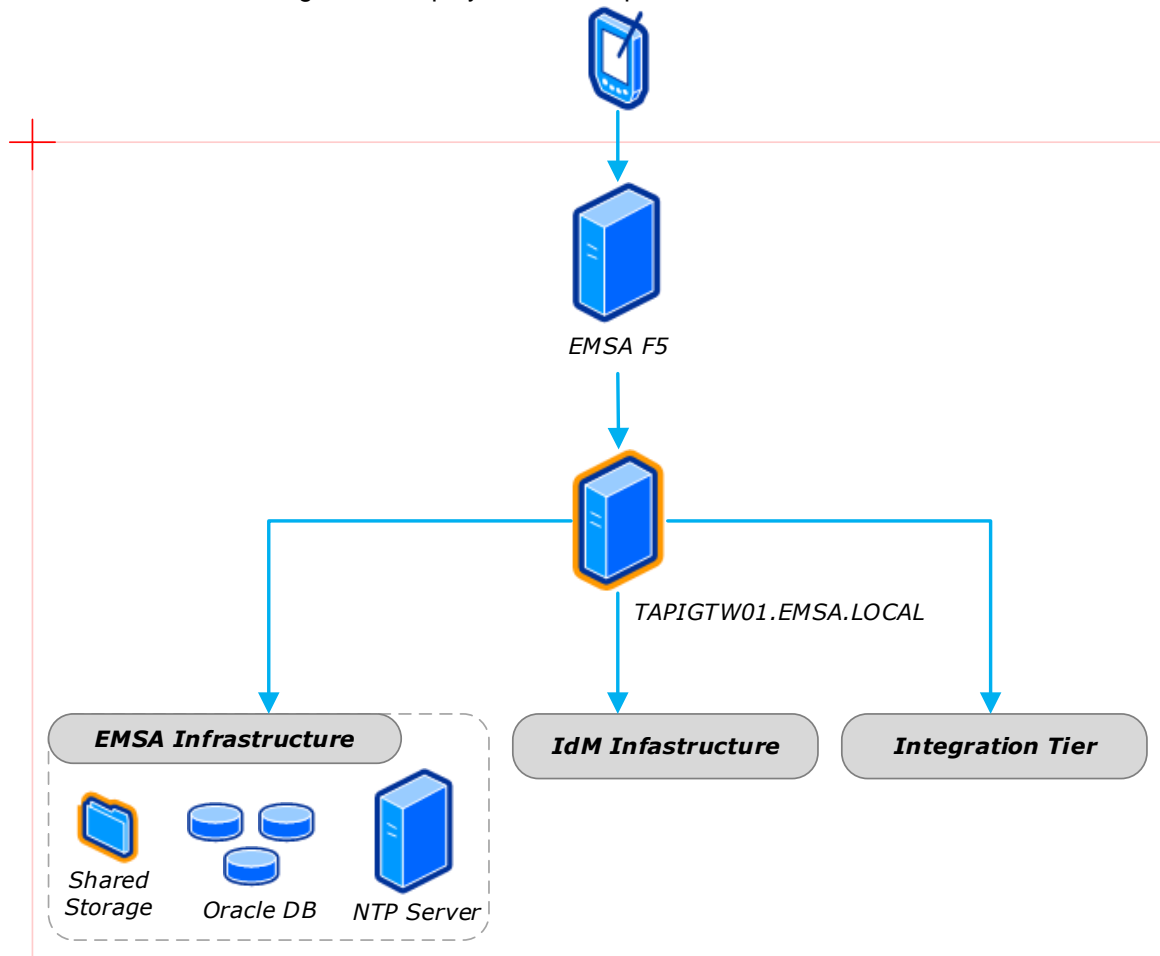
7.5.1 Activity Diagram



8. Topology

8.1 Development Environment

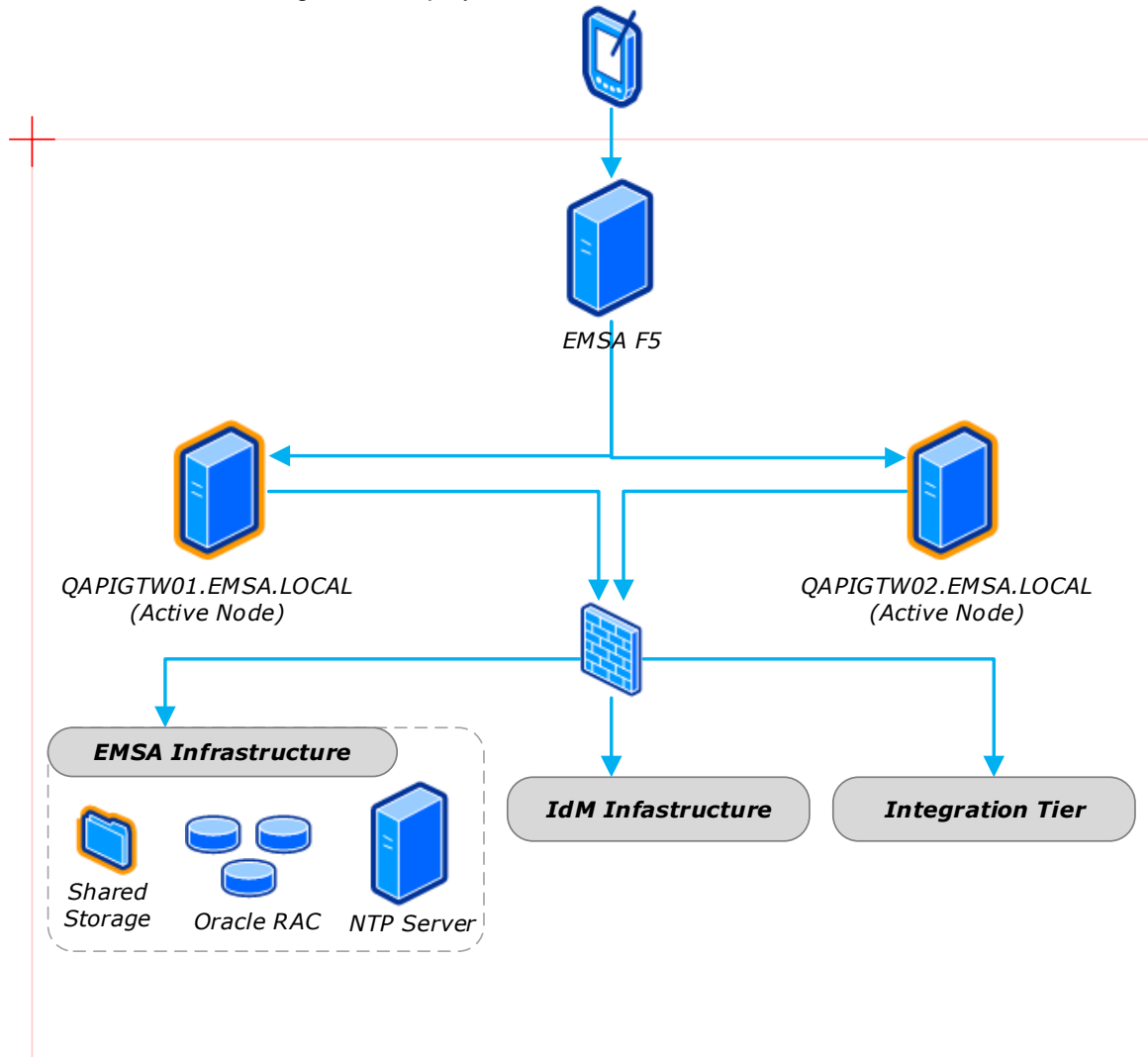
Below is the architecture design to be deployed in development environment.



European Maritime Safety Agency

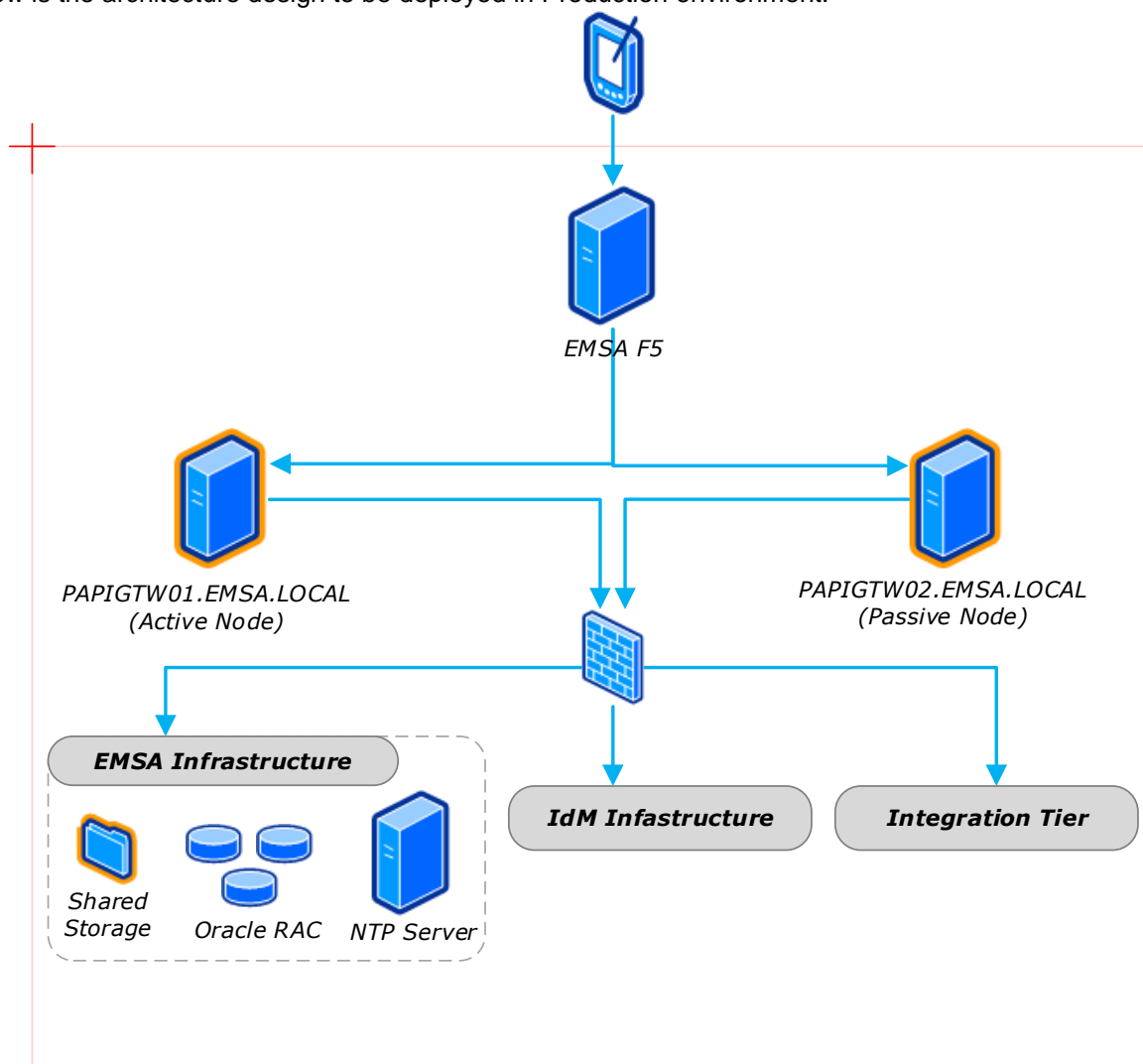
8.2 Pre-Production Environment

Below is the architecture design to be deployed in Pre-Production environment.



8.3 Production Environment

Below is the architecture design to be deployed in Production environment.



In this chapter we present all the Hardware and Software Requirement needed for the implementation of the Mobile Access Gateway Solution.

9.1 Hardware

9.1.1 Development Environment

The hardware requirement for the Development environment are the presented on the following table:

Server	Quantity	Hardware Requirements
QAPIGTW01	1	2X Dual core processor (Intel Core)
		4 GB RAM
		80 GB Storage
		1X Network adapter (1Gb)

9.1.2 Pre-Prod Environment

The hardware requirement for the Pre-Production environment are the presented on the following table:

Server	Quantity	Hardware Requirements
API Gateway	2	2X Quad core processor(Intel Core)
		4 GB RAM
		80 GB
		2X Network adapter (1Gb)

9.1.3 Production Environment

The hardware requirement for the Production environment are the presented on the following table:

Server	Quantity	Hardware Requirements
API Gateway	2	2X Quad core processor(Intel Core)
		4GB RAM
		80GB SATA
		2X Network adapter (1Gb)

9.2 Software

The software requirement needed for all the environments are the presented on the following table:

Server	Software Requirements
API Gateway Host	Red Hat Enterprise Linux 5 (UL3+)
	X-Windows environment
	GTK+ 2
	Firefox 13.0 or higher

9.3 Access Requirements

It will be required permission for *root* or *superuser* on the hosts in order to install and configure Services during Oracle API Gateway components installation.

9.4 Connectivity Matrix

In this chapter we present the required connectivity matrix for all the three environments.

9.4.1 Development Environment

Origin		Destiny		Protocol/Port
Server	Service	Server	Service	

Origin		Destiny		Protocol/Port
Server	Service	Server	Service	
Workstation(1,2,3,4)	SSH Client	tapigtw01.emsa.local	SSH	SSH/22
Workstation(1,2,3,4)	FTP Client	tapigtw01.emsa.local	SFTP	SSH/22
Workstation(1,2,3,4)	Browser	tapigtw01.emsa.local	Traffic	HTTP/8080
Workstation(1,2,3,4)	Browser	tapigtw01.emsa.local	Management	HTTP/8085
Workstation(1,2,3,4)	Browser	tapigtw01.emsa.local	Admin Node Manager	HTTP/8090
WorkStation(1,2,3,4)	Browser	tesb01.emsa.local	Oracle Service BUS	HTTP/7101
tapigtw01.emsa.local	API Gateway Server	Database	Oracle Database	TCP/1535
tapigtw01.emsa.local	API Gateway Server	toam3.emsa.local	Oracle Access Manager	HTTP/7777
tapigtw01.emsa.local	API Gateway Server	tesb01.emsa.local	Oracle Service BUS	HTTP/7101
tapigtw01.emsa.local	API Gateway Server	tldap.emsa.local	LDAP	LDAP/389
Oracle HTTP Server	Oracle HTTP Server	tapigtw01.emsa.local	Traffic	HTTP/8080 HTTP/8081
Oracle HTTP Server	Oracle HTTP Server	tapigtw01.emsa.local	Admin Node Manager	HTTP/8090
Oracle HTTP Server	Oracle HTTP Server	tapigtw01.emsa.local	Management	HTTP/8085

9.4.2 Pre-Prod Environment

Origin		Destiny		Protocol/Port
Server	Service	Server	Service	
Workstation(1,2,3,4)	SSH Client	qapigtw01.emsa.local	SSH	SSH/22
Workstation(1,2,3,4)	FTP Client	qapigtw01.emsa.local	SFTP	SSH/22
Workstation(1,2,3,4)	Browser	qapigtw01.emsa.local	Traffic	HTTP/8080
Workstation(1,2,3,4)	Browser	qapigtw01.emsa.local	Management	HTTP/8085
Workstation(1,2,3,4)	Browser	qapigtw01.emsa.local	Admin Node Manager	HTTP/8090
WorkStation(1,2,3,4)	Browser	qosb01.emsa.local	Oracle Service BUS	HTTP/7101
qapigtw01.emsa.local	API Gateway Server	Database	Oracle Database	TCP/1535
qapigtw01.emsa.local	API Gateway Server	qoam3.emsa.local	Oracle Access Manager	HTTP/7777
qapigtw01.emsa.local	API Gateway Server	qosb01.emsa.local	Oracle Service BUS	HTTP/7101
qapigtw01.emsa.local	API Gateway Server	qldap.emsa.local	LDAP	LDAP/389
Oracle HTTP Server	Oracle HTTP Server	qapigtw01.emsa.local	Traffic	HTTP/8080 HTTP/8081
Oracle HTTP Server	Oracle HTTP Server	qapigtw01.emsa.local	Admin Node Manager	HTTP/8090
Oracle HTTP Server	Oracle HTTP Server	qapigtw01.emsa.local	Management	HTTP/8085

Origin		Destiny		Protocol/Port
Server	Service	Server	Service	
Workstation(1,2,3,4)	SSH Client	papigtw01.emsa.local	SSH	SSH/22
Workstation(1,2,3,4)	FTP Client	papigtw01.emsa.local	SFTP	SSH/22
Workstation(1,2,3,4)	Browser	papigtw01.emsa.local	Traffic	HTTP/8080
Workstation(1,2,3,4)	Browser	papigtw01.emsa.local	Management	HTTP/8085
Workstation(1,2,3,4)	Browser	papigtw01.emsa.local	Admin Node Manager	HTTP/8090
WorkStation(1,2,3,4)	Browser	posb01.emsa.local	Oracle Service BUS	HTTP/7101
papigtw01.emsa.local	API Gateway Server	Database	Oracle Database	TCP/1535
papigtw01.emsa.local	API Gateway Server	poam1.emsa.local	Oracle Access Manager	HTTP/7777
papigtw01.emsa.local	API Gateway Server	posb01.emsa.local	Oracle Service BUS	HTTP/7101
papigtw01.emsa.local	API Gateway Server	pldap.emsa.local	LDAP	LDAP/389
Oracle HTTP Server	Oracle HTTP Server	papigtw01.emsa.local	Traffic	HTTP/8080 HTTP/8081
Oracle HTTP Server	Oracle HTTP Server	papigtw01.emsa.local	Admin Node Manager	HTTP/8090
Oracle HTTP Server	Oracle HTTP Server	papigtw01.emsa.local	Management	HTTP/8085

9.5 Platforms Integration

In this chapter we present all the information about the systems with which the Oracle API Gateway will integrate.

9.5.1 Web Services To Publish and Secure

In this section we present all the services that will be published and secured by the Oracle API Gateway.

9.5.1.1 Test environment Web Services

Service URL definitions for test environment	
Service	URL
Global	http://tesb01:7101/EMSAMobile/v1/
IMSMobile Alerts	http://tesb01:7101/EMSAMobile/v1/alerts?
IMSMobile Cmap	http://tesb01:7101/EMSAMobile/v1/cmap?
IMSMobile Grid	http://tesb01:7101/EMSAMobile/v1/grids?
IMSMobile Incidents	http://tesb01:7101/EMSAMobile/v1/incidents?
IMSMobile OilSpills	http://tesb01:7101/EMSAMobile/v1/oilSpills?
IMSMobile Particulars	http://tesb01:7101/EMSAMobile/v1/particulars?
IMSMobile Positions	http://tesb01:7101/EMSAMobile/v1/positions?
IMSMobile Track	http://tesb01:7101/EMSAMobile/v1/tracks?
IMSMobile Voyages	http://tesb01:7101/EMSAMobile/v1/voyages?

9.5.1.2 Pre-Production environment Web Services

Service URL definitions for pre-prod environment

Service	URL
Global	http://qosb:7101/EMSAMobile/v1/
IMSMobile Alerts	http://qosb:7101/EMSAMobile/v1/alerts?
IMSMobile Cmap	http://qosb:7101/EMSAMobile/v1/cmap?
IMSMobile Grid	http://qosb:7101/EMSAMobile/v1/grids?
IMSMobile Incidents	http://qosb:7101/EMSAMobile/v1/incidents?
IMSMobile OilSpills	http://qosb:7101/EMSAMobile/v1/oilSpills?
IMSMobile Particulars	http://qosb:7101/EMSAMobile/v1/particulars?
IMSMobile Positions	http://qosb:7101/EMSAMobile/v1/positions?
IMSMobile Track	http://qosb:7101/EMSAMobile/v1/tracks?
IMSMobile Voyages	http://qosb:7101/EMSAMobile/v1/voyages?

9.5.1.3 Production environment Web Services

Service URL definitions for prod environment	
Service	URL
Global	http://posb01:7101/EMSAMobile/v1/
IMSMobile Alerts	http://posb01:7101/EMSAMobile/v1/alerts?
IMSMobile Cmap	http://posb01:7101/EMSAMobile/v1/cmap?
IMSMobile Grid	http://posb01:7101/EMSAMobile/v1/grids?
IMSMobile Incidents	http://posb01:7101/EMSAMobile/v1/incidents?
IMSMobile OilSpills	http://posb01:7101/EMSAMobile/v1/oilSpills?
IMSMobile Particulars	http://posb01:7101/EMSAMobile/v1/particulars?
IMSMobile Positions	http://posb01:7101/EMSAMobile/v1/positions?
IMSMobile Track	http://posb01:7101/EMSAMobile/v1/tracks?
IMSMobile Voyages	http://posb01:7101/EMSAMobile/v1/voyages?

9.5.2 LDAP Group

The following table presents the LDAP group to which the authenticated user must belong in order to be authorized to access the protected resource.

LDAP Group
DN: cn=IMSMobile,ou=IMDATE,ou=groups,dc=emsa,dc=europa,dc=eu

9.5.3 Oracle Access Manager

In order to integrate the Oracle API Gateway with the Oracle Access Manager the following high level tasks must be performed on the OAM:

1. Create the Access Gate
2. Configure a Primary Access Server for the new Access Gate
3. Create Host Identifier for Oracle Api Gateway
4. Protect Resources based on LDAP Group

9.6 API Gateway Services

On the following table we present the Web Services end points that will be available through the Oracle API Gateway, and that will be used from the IMS Mobile APP.

Service URL for Oracle API Gateway	
Service	URL
EMSA User Login	http://papigtw01:8080/EMSAMobile/v1/login?
EMSA User Logout	http://papigtw01:8080/EMSAMobile/v1/logout?
EMSA Forgot Password	http://papigtw01:8080/EMSAMobile/v1/forgotpassword?
Global	http://papigtw01:8080/EMSAMobile/v1/
IMSMobile Alerts	http://papigtw01:8080/EMSAMobile/v1/alerts?
IMSMobile Cmap	http://papigtw01:8080/EMSAMobile/v1/CMAP?
IMSMobile Grid	http://papigtw01:8080/EMSAMobile/v1/grids?
IMSMobile Incidents	http://papigtw01:8080/EMSAMobile/v1/incidents?

IMSMobile OilSpills	http://papigtw01:8080/EMSAMobile/v1/oilSpills?
IMSMobile Particulars	http://papigtw01:8080/EMSAMobile/v1/particulars?
IMSMobile Positions	http://papigtw01:8080/EMSAMobile/v1/positions?
IMSMobile Track	http://papigtw01:8080/EMSAMobile/v1/tracks?
IMSMobile Voyages	http://papigtw01:8080/EMSAMobile/v1/voyages?

9.6.1 EMSA User Login Service Specification

Service	login			Version	1
Description	Performs the User Login on the Oracle Access Manager, and Returns the SSO Session SSO Token and all LDAP groups from the user.				
Http Method	GET				
Endpoint	https://<host>[:<port>]/EMSAMobile/v1/login				
Input Arguments					
Argument	Type	Occurs	Description		
Authorization	HTTP Header	1	User name and password		
Output					
Argument	Type	Occurs	Description		
ssosession	HTTP Header	0..1	If the user is authenticated with success, a sso token is returned		
roles	Array	0..1	Array of user roles		
role	String	1..1	LDAP group name		

9.6.2 EMSA User Logout Service Specification

Service	logout			Version	1
Description	Performs the User Logout on MAG and IMS App clears the sso session and authorization from the HTTP Header.				
Http Method	GET				
Endpoint	https://<host>[:<port>]/EMSAMobile/v1/logout				
Input Arguments					
Argument	Type	Occurs	Description		
ssosession	HTTP Header	1	User sso token		
Output					
Argument	Type	Occurs	Description		
status	String	1..1	Generic message indicating that the request was processed.		

9.6.3 EMSA Forgot Password Service Specification

Service	forgotpassword			Version	1
Description	This service executes the EMSA Forgot Password Process that sends an email to the User to change the password.				
Http Method	GET				
Endpoint	https://<host>[:<port>]/EMSAMobile/v1/forgotpassword? user=<user>				
Input Arguments					
Argument	Type	Occurs	Description		

user	string	1	User Login
Output			
Argument	Type	Occurs	Description
status	String	1..1	Generic message returned by the OAM. This message indicated that an email was sent, and also contains a ticket id from the request.

9.7 API Gateway Installation

In this Chapter we present all the components that will be installed for the Mobile Access Gateway Solution.

9.7.1 API Gateway Core Server

9.7.1.1 Installation Directory

The API Gateway Core Server will be installed on the following folder:
/oracle/oag/apigtw-inst01/

9.7.1.2 Starting the API Gateway

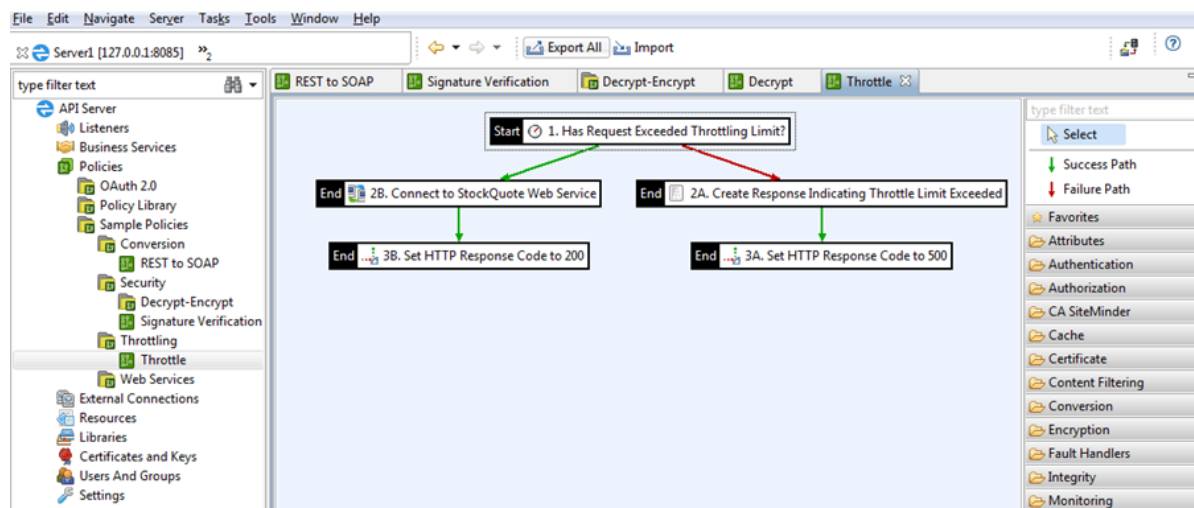
1. Open a command prompt.
2. Change to the directory /oracle/oag/apigtw-inst01/apigateway/posix/bin
3. Run the `startinstance` command, for example `startinstance -n "Server1" -g "Group1"`
4. To manage and monitor the API Gateway, you must ensure that the Admin Node Manager is running. Use the `nodemanager` command to start the Admin Node Manager from the same directory

9.7.2 Policy Studio

The Policy Studio tool is a graphic user interface (GUI) that allows the virtualization of APIs, policies development and includes the following features:

- APIs management
- Visualization in Flow-chart mode for easy development and management
- Interface drag-n-drop chart for the encoding rules, settings and policies
- Extensive library of Out-of-the-box filters for policy definitions

Below is represented how policies are configured:



The Policy Studio Tool will be installed on the following folder:
/oracle/oag/apigtw-inst01/

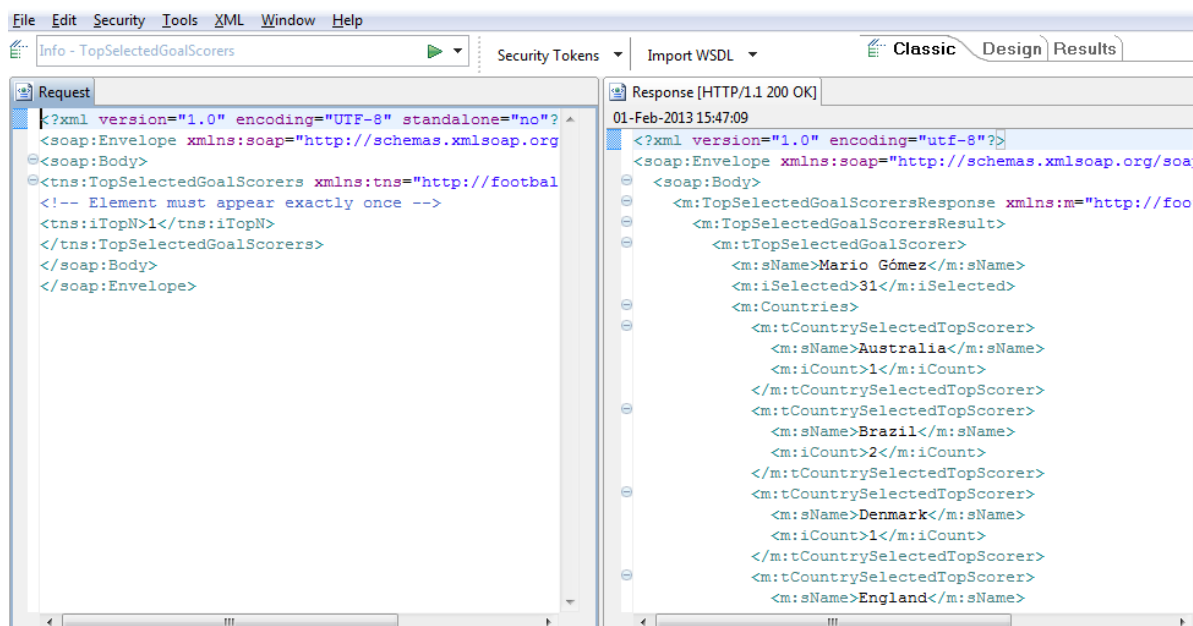
9.7.2.2 Starting Policy Studio

To launch Policy Studio after installation, perform the following steps:

1. Open a command prompt.
2. Change to your Policy Studio installation directory (/oracle/oag/apigtw-inst01/policystudio).
3. Start policystudio.

9.7.3 API Gateway Explorer

The API Gateway Explorer is a tool to test performance, scalability and security of APIs. For instance it can be used to send a specific request to validate the answer.



The API Gateway Explorer has the following features:

- REST API testing and SOAP Web Services
- Implementation of Security tokens (eg WS-Security and SAML)
- Manage attachments in SOAP messages
- Management of certificates and encryption keys
- Creation and implementation of stress and performance testing

9.7.3.1 Installing API Gateway Explorer

The API Gateway Explorer will be installed on the following folder:
/oracle/oag/apigtw-inst01/

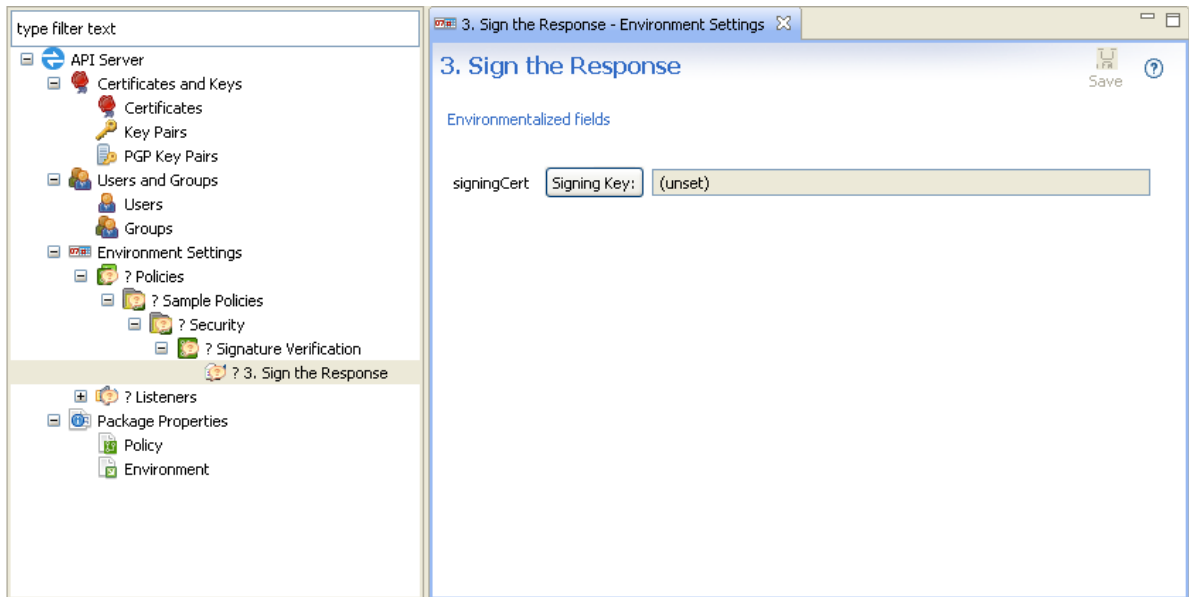
9.7.3.2 Starting API Gateway Explorer

To launch API Gateway Explorer after installation, perform the following steps:

1. Open a command prompt.
2. Change to your API Gateway Explorer installation directory (/oracle/oag/apigtw-inst01/apigatewayexplorer).
3. Start apigatewayexplorer.

9.7.4 Configuration Studio

The Configuration Studio is a graphic user interface tool to promote APIs from development environments to production environments. With this tool is possible to test settings and validate the granular level to eliminate non-conformities and errors policies.



The Configuration Studio tool performs the following tasks:

- Open a *policy package* (.pol) from development environment.
- Specify values for specific environments defined under development (eg policies, listeners and external connections).
- Import or define specific environment parameters.
- Set specific users or groups by environment.
- Export environment settings to a file or disk.

9.7.4.1 Installing API Gateway Explorer

The API Gateway Explorer will be installed on the following folder:
/oracle/oag/apigtw-inst01/

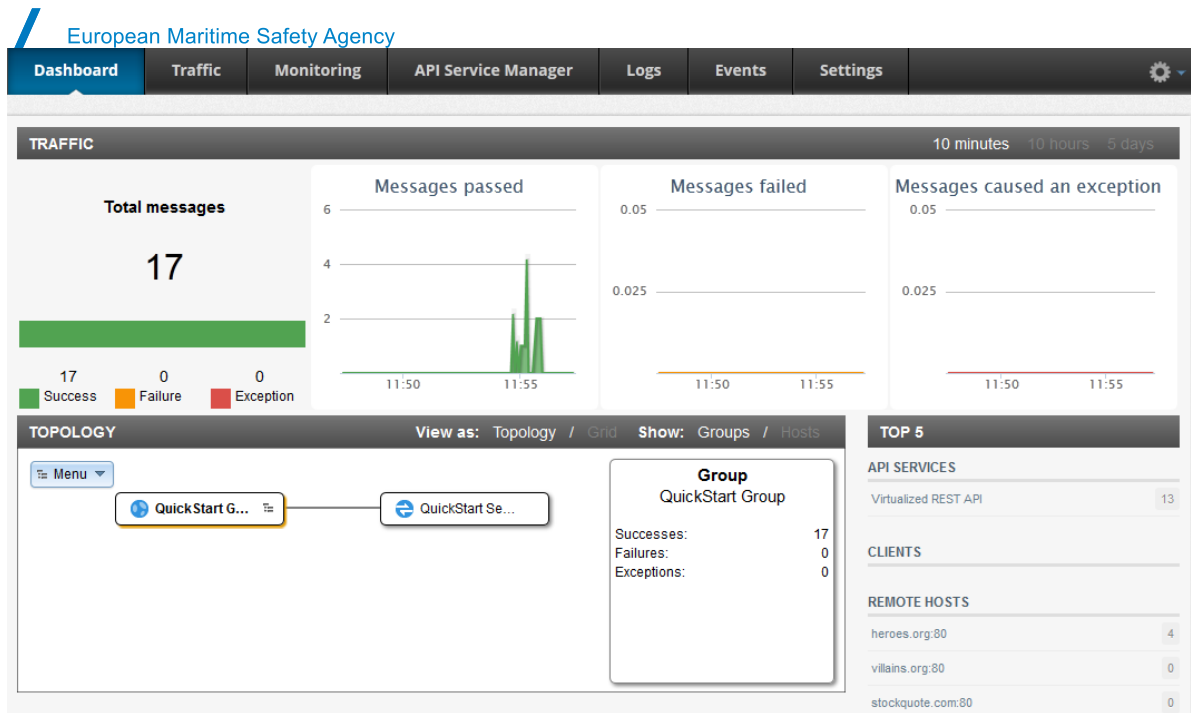
9.7.4.2 Starting API Gateway Explorer

To launch Configuration Studio after installation, perform the following steps:

1. Open a command prompt.
2. Change to your Configuration Studio installation directory (for example, /oracle/oag/apigtw-inst01/configurationstudio).
3. Start configurationstudio.

9.7.5 API Gateway Manager

API Gateway Manager is the admin web for operational management, monitoring and troubleshooting.



The API Gateway Manager has the following features:

- Dashboard topology with real-time traffic information by domain, group, or API Gateway
- Monitoring in real time traffic and content enabling the identification of a granular exceptions
- Real-time monitoring of performance metrics for API, system or remote host
- Aggregation alerts and SLA
- Centralized view logs in each instance of API Gateway

9.7.5.1 Installing API Gateway Manager

The API Gateway Manager is automatically installed with the installation of the Oracle API Gateway Core Server.

9.7.5.2 Accessing API Gateway Manager

To access the API Gateway Manager perform the following steps:

1. Open a compatible browser.
2. Access the following URL:
 1. [https:// tapigtw01.emsa.local:8090](https://tapigtw01.emsa.local:8090)

9.8 API Gateway Audit and Logs

9.8.1 Domain audit logs

The domain audit log captures management changes in the API Gateway domain that are written by the Admin Node Manager and by API Gateway instances. This includes details such as API Gateway configuration changes, logins, deployments, services registration, user, or topology changes. For example, the displayed event types include the following:

- Configuration
- Service
- Application
- Topology
- User store

- Key Property Store (KPS)

9.8.1.1 View in API Gateway Manager

To view domain audit log events in the API Gateway Manager web console, perform the following steps:

1. In the API Gateway Manager, select **Logs** > **Domain Audit**.
2. Configure the number of events displayed in the **Max results per server** field on the left. Defaults to 1000.
3. Configure the **Time Interval** for events. Defaults to 1 day.
4. Click the **Filter** button to add more viewing options (**Event Type** or **Groups and Servers**).
5. Click **Apply** when finished.

Dashboard	Monitoring	Traffic	Logs	Events	Messaging	Settings	
Domain Audit							
Domain Audit				Access Log	Transaction Log	Trace Log	Reload QuickStart Server
Filter + Apply							
MAX RESULTS PER SERVER 1000							
TIME INTERVAL 1 day							
Message	Event Type	Metadata	Date/Time	Group	Server		
Performing a lookup on performance metrics over a 24h interval	Service events		16/04/2014 15:50:11.359	Node Manager Group	Node Manager on devsupport2.vordel.com		
Performing search for jms traffic information over a null interval	Service events		16/04/2014 15:50:11.359	Node Manager Group	Node Manager on devsupport2.vordel.com		
Performing search for http traffic information over a null interval	Service events		16/04/2014 15:50:11.359	Node Manager Group	Node Manager on devsupport2.vordel.com		
Performing search for filetransfer traffic information over a null interval	Service events		16/04/2014 15:50:11.359	Node Manager Group	Node Manager on devsupport2.vordel.com		
Deployment data read by user 'admin'	Configuration events		16/04/2014 15:50:09.828	Node Manager Group	Node Manager on devsupport2.vordel.com		
User 'admin' connected with 3 defined user roles	User events		16/04/2014 15:50:08.015	Node Manager Group	Node Manager on devsupport2.vordel.com		
User 'apiadmin@localhost' logged in to the system	User events		16/04/2014 15:37:07.218	QuickStart Group	QuickStart Server		

9.8.1.2 domain audit log file

To view domain audit log file contents. The location for the Admin Node Manager file log:

```
/oracle/oag/apigtw-inst01/apigateway/logs/audit.log
```

For example:

```
{
  "timestamp": 1435135039120,
  "message": "User 'admin' connected with 3 defined user roles",
  "eventId": 107,
  "metadata": {
    "userID": "admin"
  }
}, {
  "timestamp": 1435135039991,
  "message": "Deployment data read by user 'admin'",
  "eventId": 1037,
  "metadata": {}
}, {
  "timestamp": 1435135042951,
  "message": "Configuration details for Service 'tapigtw-inst1' read by 'admin'",
  "eventId": 1040,
  "metadata": {
    "serviceID": "instance-1"
  }
}, {
  "timestamp": 1435143192088,
  "message": "Replicating configuration '240dc416-21f4-4bff-a319-251b3d264263', num bytes=323136 for group 'tapigtwcluster' Policy Props: [Name: Default Factory Configuration (Policy), Description: Default factory configuration for Oracle API Gateway (Policy), Version: v1 (Policy), VersionComment: Original factory configuration (Policy), ChangedBy: admin, ] Environment Props: [Name: Default Factory Configuration (Environment), Description: Default factory configuration for Oracle API Gateway (Environment), Version: v1 (Environment), VersionComment: Original factory configuration (Environment), ]",
  "eventId": 1003,
  "metadata": {
    "userID": "admin",
    "groupID": "group-2",
    "archiveID": "240dc416-21f4-4bff-a319-251b3d264263"
  }
}
```

The API Gateway outputs tracing and debugging information to record information about its execution. For example, this includes details such as services starting or stopping, and messages sent through the API Gateway. This information then can be used by API Gateway administrators and developers for diagnostics and debugging purposes, and is useful when contacting Oracle Support.

9.8.2.1 View in API Gateway Manager

To view domain trace log events in the API Gateway Manager web console, perform the following steps:

- **Logs > Trace** view in API Gateway Manager

Name	Size	Last Modified
tapigtw-inst1_20150624165522.trc	36647	24/06/2015 16:55
tapigtw-inst1_20150624093720.trc	16777273	24/06/2015 16:55
.tapigtw-inst1_20150609112131.trc.swp	24576	24/06/2015 16:54
tapigtw-inst1_20150623192853.trc	11734496	23/06/2015 20:03
tapigtw-inst1_20150623180424.trc	16777280	23/06/2015 19:28
tapigtw-inst1_20150623151729.trc	16777245	23/06/2015 18:04
tapigtw-inst1_20150611012331.trc	183525	11/06/2015 14:22
tapigtw-inst1_20150610000000.trc	13593310	10/06/2015 23:11
tapigtw-inst1_20150609231644.trc	9963680	09/06/2015 23:59
tapigtw-inst1_20150609220307.trc	16777289	09/06/2015 23:16

9.8.2.2 View the trace log file

Alternatively, you can view contents directly on the trace log file. Trace log files are named as *servername_timestamp.trc* (for example, *instance-1_20130118160212.trc*).

- Trace files in the following location:
 - Admin Node Manager:

```
/oracle/oag/apigtw-inst01/apigateway/trace
```

- API Gateway instance:

```
/oracle/oag/apigtw-inst01/apigateway/groups/<group-id>/<instance-id>/trace
```

Each time the API Gateway starts up, by default, it outputs a trace file to the API Gateway *trace* directory. The following example shows an extract from a default API Gateway trace file:

```
INFO    15/Jun/2012:09:54:01.047 [1b10] Realtime monitoring enabled
INFO    15/Jun/2012:09:54:01.060 [1b10] Storing metrics in database disabled
INFO    15/Jun/2012:09:54:03.229 [1b10] cert store configured
INFO    15/Jun/2012:09:54:03.248 [1b10] keypairs configured
...
```

The trace file output takes the following format:

```
TraceLevel    Timestamp [thread-id] TraceMessage
```

For example, the first line in the above extract is described as follows:

TraceLevel	INFO
-------------------	------

Timestamp	15/Jun/2012:09:54:01.047 (day:hours:minutes: seconds:milliseconds)
Thread-id	[1b10]
TraceMessage	Realtime monitoring enabled

The following extract shows a policy called when running a simple service:

```
DEBUG ... run circuit "/axis/services/urn:cominfo"...
DEBUG ... run filter [Service Handler for 'ComInfoServiceService'] {
DEBUG ...   Set the service name to be ComInfoServiceService
DEBUG ...   Web Service context already set to ComInfoServiceService
DEBUG ...   close content stream
DEBUG ...   Calling the Operation Processor Chain [1. Request from Client]...
DEBUG ...   run filter [1. Request from Client] {
DEBUG ...     run filter [Before Operation-specific Policy] {
DEBUG ...       run circuit "WS-Security UsernameToken AuthN"...
DEBUG ...       run filter [WS-Security Username Token] {
DEBUG ...         ...
DEBUG ...       } = 1, in 62 milliseconds
DEBUG ...     ... "WS-Security UsernameToken AuthN" complete.
DEBUG ...   } = 1, in 74 milliseconds
...

```

9.8.3 Log files list

Role	Log file path	Description
Node Manager audit log	/oracle/oag/apigtw-inst01/apigateway/logs/audit.log	The audit log captures management changes in the API Gateway domain that are written by the Admin Node Manager and by API Gateway instances. This includes details such as API Gateway configuration changes, logins, deployments, services registration, user, or topology changes.
Node Manager trace log	/oracle/oag/apigtw-inst01/apigateway/trace/serve_rname_timestamp.trc	The trace log records information about Node Manager execution, details such as services starting or stopping, and Deployment status.
Instance trace log	/oracle/oag/apigtw-inst01/apigateway/groups/<group-id>/<instance-id>/trace/servername_timestamp.trc	The trace log records information about the Instance execution, details such as services starting or stopping, and messages sent through the API Gateway.

European Maritime Safety Agency

Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu

