



eIDAS-enabled Student Mobility

D2.2 Integration and Testing Plans

Document Identification			
Status	Final	Due Date	30/09/2018
Version	1.0	Submission Date	30/09/2018

Related Activity	Activity 2	Document Reference	D2.2
Related Deliverable(s)	D2.1	Dissemination Level (*)	PU
Lead Participant	ATOS	Lead Author	Ross Little
Contributors	UJI, UAEGEAN	UNIT, Reviewers	Francisco Aragó (UJI)
			Andreas Åkre Solberg (UNIT)

Keywords:
Education sector, eID, DSI, eIDAS, Cross-border, Domain Specific Attributes, DSA, eduPerson, eduGAIN

This document is issued within the frame and for the purpose of the ESMO project. This project has received funding from the European Union's Innovation and Networks Executive Agency – Connecting Europe Facility (CEF) under Grant AGREEMENT No INEA/CEF/ICT/A2017/1451951; Action No 2017-EU-IA-00329. The opinions expressed, and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the ESMO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the ESMO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the ESMO Partners.

Each ESMO Partner may use this document in conformity with the ESMO Consortium Grant Agreement provisions.

(*) Dissemination level.-**PU**: Public, fully open, e.g. web; **CO**: Confidential, restricted under conditions set out in Model Grant Agreement; **CI**: Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Raquel Cortés	ATOS
Ross Little	ATOS
Miryam Villegas	ATOS
Francisco José Aragón	UJI
Nikolaos Triantafyllou	UAEGEAN
Andreas Åkre Solberg	UNIT

Document History			
Version	Date	Change editors	Changes
0.1	24/07/2018	ATOS	ToC.
0.2	25/07/2018	ATOS	Comments received from UJI.
0.3	20/08/2018	ATOS	Methodology, and test cases specification.
0.4	07/09/2018	ATOS	Finalising test cases specification. More thoughts on the test methodology in microservices architecture. Some notes on the validation plan section.
0.5	13/09/2018	ATOS	Document prepared for ATOS internal check.
0.6	17/09/2018	ATOS	Document passed ATOS internal check.
0.7	21/09/2018	ATOS	Near final version prepared for Peer to Peer Review.
0.8	25/09/2018	ATOS	Inclusion UJI and UAEGEAN comments.
0.85	26/09/2018	ATOS	UAEGEAN Peer to Peer Review.
0.9	28/09/2018	ATOS	UNIT Peer to Peer Review.
1.0	30/09/2018	ATOS	Final version to be submitted.

Document name:	D2.2 Integration and Testing Plans			Page:	2 of 29
Reference:	D2.2	Dissemination:	PU	Version:	1.0
				Status:	Final

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Ross Little (ATOS)	28/09/2018
Quality manager	María Guadalupe Rodríguez (ATOS)	28/09/2018
Project Coordinator	Ross Little and María Guadalupe Rodríguez (ATOS)	30/09/2018

Document name:	D2.2 Integration and Testing Plans				Page:	3 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

Table of Contents

Document Information	2
Table of Contents	4
List of Tables.....	6
List of Figures	7
List of Acronyms.....	8
1 Introduction.....	9
1.1 Purpose of the document	9
1.2 Relation to other work.....	9
1.3 Structure of the document	9
2 Methodology	10
2.1 Roles and responsibilities.....	11
2.2 Testing procedures	12
2.2.1 Integration testing.....	12
2.2.2 End-to-end testing	12
2.3 ESMO deployment, integration and test process.....	14
2.3.1 Step 1: Software package release	15
2.3.2 Step 2: Download, build and setup.....	15
2.3.3 Step 3: Integration	15
2.3.4 Step 4: End-to-end Testing.....	16
2.3.5 Step 5: Operational testing in production.....	16
2.4 Test environment and tools	17
2.5 Issue tracking.....	18
3 Test Case Specification.....	19
3.1 Test case template	19
3.2 Test case example.....	19
4 Validation Test Plan.....	22
4.1 Authentication	24
4.2 Attribute aggregation.....	24
4.3 Interoperability	26
4.4 End user experience.....	27

Document name:	D2.2 Integration and Testing Plans			Page:	4 of 29
Reference:	D2.2	Dissemination:	PU	Version:	1.0
				Status:	Final

References 29

Document name:	D2.2 Integration and Testing Plans				Page:	5 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

List of Tables

<i>Table 1: Service Provider eService Test Case Template</i>	19
<i>Table 2: Example SP eService Test Case</i>	20
<i>Table 3: eIDAS Authentication</i>	24
<i>Table 4: Attribute aggregation</i>	24
<i>Table 5: Interoperability</i>	26
<i>Table 6: End user experience</i>	27

Document name:	D2.2 Integration and Testing Plans				Page:	6 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

List of Figures

<i>Figure 1: ESMO Deployment, Integration and Test Process Overview</i> _____	14
<i>Figure 2: ESMO Gateway integration with external nodes in preproduction</i> _____	17
<i>Figure 3: End-to-end test architecture</i> _____	23

Document name:	D2.2 Integration and Testing Plans				Page:	7 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

List of Acronyms

Abbreviation / acronym	Description
AA	Application and Admission service (UAegean use case)
AP	Attribute Provider
AuthN	Authentication
Dx.y	Deliverable number y belonging to WP x
DSA	Domain Specific Attributes
eDSS	e-Diploma Supplement Service (used in an UAegean use case)
eIDAS	Electronic IDentification Authentication and trust Services
ESMO	eIDAS-enabled Student Mobility
EU	European Union
EWP	ERASMUS Without Paper
GW	ESMO Gateway
HEI	Higher Education Institution
IdP	Identity Provider
MDS	Mandatory Data Set
MS	Member State
SP	Service Provider
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UA	User Agent
UX	User Experience
VLE	Virtual Learning Environment
WAYF	Where Are You From?

1 Introduction

1.1 Purpose of the document

The objective of this deliverable is to define a plan for testing and integrating the ESMO Gateway for cross-border eIDAS authentication and Domain Specific Attribute (DSA) exchange, so to deliver selected e-services at both pre-production and production level.

The scope of the testing is aimed at entities responsible for deploying and integrating the ESMO Gateway and will include the necessary integration with Service Providers, eIDAS Network and other Identity Providers, and Attribute Providers.

Also, as the ESMO Gateway will implement a mesh network with other ESMO Gateways for the exchange of DSAs, it is also needed to test and integrate with other ESMO Gateways and the Erasmus Without Paper (EWP) Network. EWP provides ESMO with a trusted Registry Service for securely connecting Gateways in the mesh network, as well as the ability for HEI SPs to connect to ESMO Gateways. For more information refer to D2.1 [1].

1.2 Relation to other work

This deliverable is delivered in milestone 2 along with the ESMO Gateway design specification [1], from which it obtains the ESMO Gateway overall architecture, and identifies the testing and integration that needs to be carried out during the next phases where country specific e-Services, eIDAS, and Attribute Providers will be integrated with the ESMO Gateway.

1.3 Structure of the document

Section 1: Introduction and scope of the test and integration plan.

Section 2: A general methodology is first defined in to establish how the deployment of the ESMO Gateway and its integration testing will be carried out.

Section 2 to 3: These sections focus on applying the general integration and test methodology for the specific ESMO Gateway deployments in the project. As such it will specify each deployment's specific preproduction and production deployments and establish their points of integration with external nodes to the ESMO Gateway. The specific test environment and tools used for testing will be defined, and finally the specific test cases to be carried out for each e-service deployed are specified.

Section 4: This provides a general validation plan for the integration and testing to make sure that the ESMO Gateway functionality, interoperability and user experience are validated and meeting the expected requirements for the e-Services being delivered.

Document name:	D2.2 Integration and Testing Plans			Page:	9 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

2 Methodology

The test plan methodology addresses the full process to carry out the correct integration and test validation of the implementation with key areas to cover as follows:

- All actors involved in the setup of the ESMO Gateway, pre-production test environment (including external nodes), and testing have their roles and responsibilities clearly defined.
- Ensure all requirements from the design specification are validated.
- Ensure that all external interfaces are interworking correctly as per the design specification.
- Establish the process for deploying and integrating the ESMO Gateway is in a preproduction test environment for all involved actors, for approving the service for deployment in production.
- Ensure feedback from all users involved e.g. from the end users of the service and views from Service Providers making use of the ESMO Gateway to offer their eServices.
- An overview of the test environment is described, and suitable test tools are identified for integration and testing including for any automated testing capability.
- Establish a suitable tool for the reporting and monitoring of bugs found during the integration and testing.

Document name:	D2.2 Integration and Testing Plans			Page:	10 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

2.1 Roles and responsibilities

The following actors, their roles and responsibilities are defined for the overall ESMO Gateway operational process covering its integration and test with external systems:

- **ESMO GW Software Developers** has the following responsibilities:
 - Develop ESMO Gateway software.
 - Produce ESMO Gateway wiki documentation.
 - Support ESMO Gateway software.
- **ESMO GW Administration Body** has the following responsibilities:
 - Deploy ESMO Gateway.
 - Integrate with local eIDAS country specific connection.
 - Integrate with EWP and other ESMO Gateways using EWP catalogue.
 - Provision the SPs and support their integration to the Gateway.
 - Provision the APs and support their integration to the Gateway.
 - Approve SPs and APs to be connected on live ESMO production gateway.
 - Operational support.
- **eIDAS-node Provider**, with the following responsibilities:
 - Implement Members State's Specific Parts (Connector/Proxy Service).
 - Support ESMO Gateway integration.
 - Approve ESMO Gateway to be connected to live eIDAS production system.
 - Operational support.
- **Service Provider**, with the following responsibilities:
 - Request their eServices to be connected to local ESMO Gateway.
 - Integrate and test eServices with ESMO Gateway.
 - Demonstrate eServices fully tested in pre-production.
 - Follow ESMO approval process to move into live production environment.
 - Operational support.
- **Attribute Provider**, with the following responsibilities:
 - Request their AP service to be connected to local ESMO gateway.
 - Integrate and test dummy eService with ESMO Gateway.
 - Demonstrate eServices fully tested in pre-production.
 - Follow ESMO approval process to move into live production environment.
 - Operational support.
- **EWP Administration Body:**
 - Provision country ESMO Gateways to the EWP Registry Service.
 - Support ESMO integration with EWP.
 - Approve ESMO Gateways to production.
 - Operational support.

Document name:	D2.2 Integration and Testing Plans			Page:	11 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

2.2 Testing procedures

When deploying the ESMO Gateway and integrating with Service Providers, Identity Providers, and Attribute Providers the tests to be carried out are integration and end-to-end tests.

2.2.1 Integration testing

The integration tests will make sure that the service provided by an external node works as expected with input queries returning deterministic output responses.

The mature services that the ESMO Gateway will interface with in country deployments are the eIDAS and EWP networks. For these services it is expected that integration testing in country deployments can be carried out as part of end-to-end tests.

For any SP services or AP datastores that are being developed or modified to integrate with the ESMO Gateway it is recommended to make use of stubs to prove basic query and responses are correct before deploying the service in preproduction. Stubs may also be developed to trigger fail scenarios that are difficult to produce in the real deployment.

Another strategy for SP Integration tests, prior going to preproduction, is to build a local version of the ESMO Gateway and stubs are used for dummy responses from eIDAS, EWP, APs, and other ESMO Gateway connections.

The ESMO Gateway makes use of cryptographic certificates for creating the trust network with other ESMO Gateways through the EWP network, as well as with SPs and APs, and therefore, it is needed that these are setup and shared before integration testing of these services can begin.

Likewise, services being deployed over SSL/TLS will have to make sure that they deploy the necessary certificates and are operating correctly.

2.2.2 End-to-end testing

The eIDAS authentication and Domain Specific Attribute retrieval services available over the ESMO Gateway are driven by the user, accessing cross-border HEI eServices (provided by HEI Service Providers) with their national eIDs.

Therefore, the end-to-end testing will be driven by the Service Provider use cases for each of the eServices that they will deploy.

A typical end-to-end test case scenario is summarized as follows:

1. HEI Service Provider eServices require that users are first authenticated with their national eIDs over eIDAS via the ESMO Gateway.
2. Next, it is needed to retrieve certain Domain Specific Attributes from Attribute Providers, for those eServices that have requested certain DSAs for authorization to access the eServices. This may be via the local Gateway to an AP or via the local originating Gateway to a terminating Gateway in another Member State.
3. The user may request to retrieve DSAs from other APs, and when no more APs are requested to be checked then all attributes (eIDAS and DSA) are returned to the eService.

Document name:	D2.2 Integration and Testing Plans			Page:	12 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

End-to-end testing will take place in each countries pre-production environment as per the eServices integrated with ESMO, and it will be sought to automate these tests as much as possible with dummy data, as will be produced in task 6.1. These tests aim to prove all functionality and design specification requirements of the ESMO gateway are fulfilled against a validation plan checklist (see section 4).

Once all testing in pre-production has been satisfied, real end user end-to-end testing will next be carried out in a live production environment as per task 6.2. As well as checking the design specifications are correctly implemented, these tests are designed to obtain end user feedback.

Document name:	D2.2 Integration and Testing Plans				Page:	13 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

2.3 ESMO deployment, integration and test process

The figure below presents an overview of the main steps of the ESMO deployment, integration and test process workflow, with main actor involvement in each of the steps.

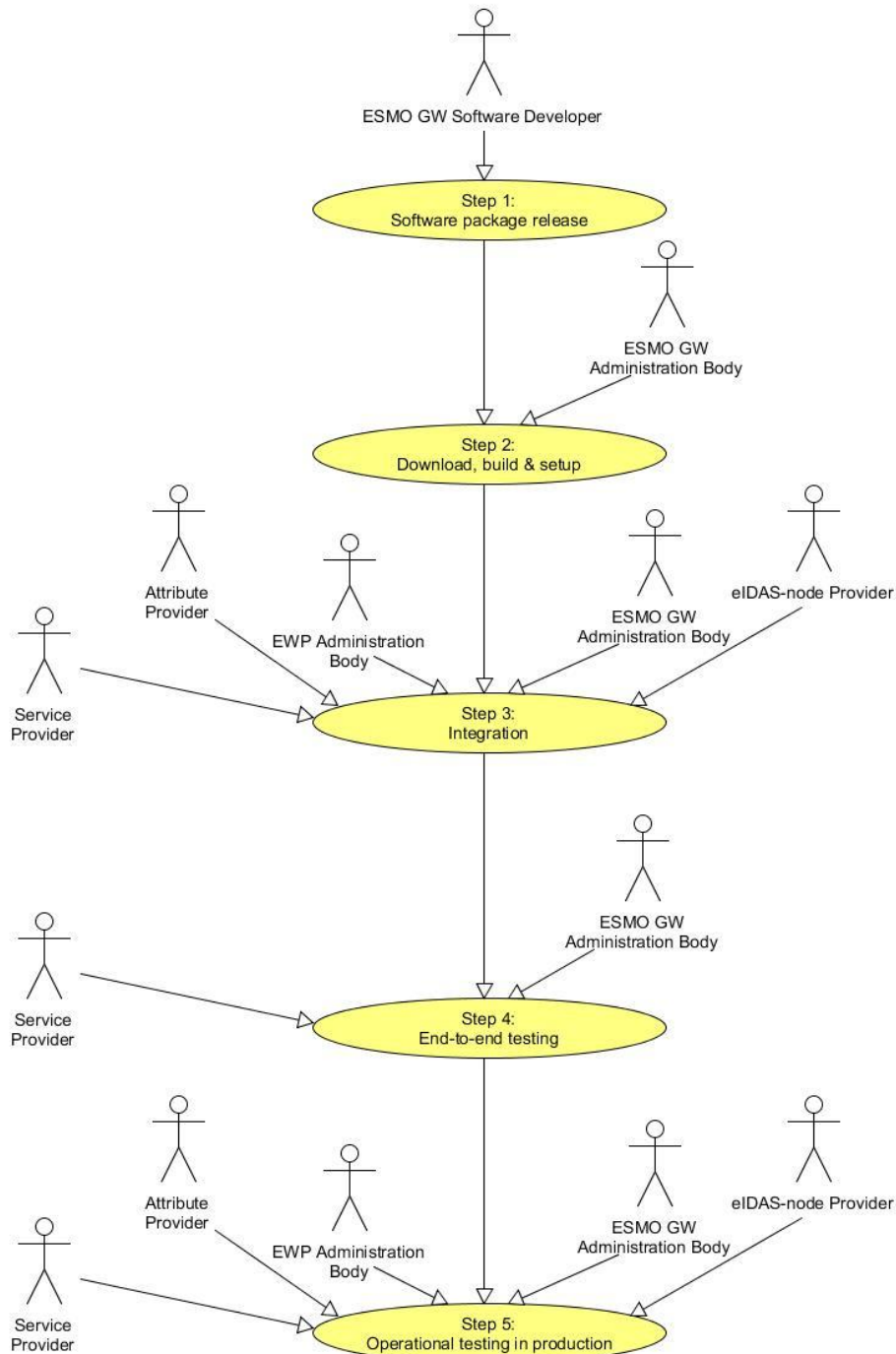


Figure 1: ESMO Deployment, Integration and Test Process Overview

Document name:	D2.2 Integration and Testing Plans	Page:	14 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Each of the process steps is described in more detail in the next sections.

2.3.1 Step 1: Software package release

ESMO GW Software Developers will:

1. The ESMO software package will be released on GitLab.
2. Country specific modules will be able to be selected, as applicable.
3. Add-on stubs used for test purposes will also be made available.
4. Documentation will be released on the GitLab wiki.
5. Provide support for bug reporting and solutions.

2.3.2 Step 2: Download, build and setup

ESMO GW Administration Body will:

1. Follow ESMO GitLab wiki documentation on how to install and setup the ESMO Gateway with country specific modules as applicable to the Member State.
2. Download and Build the ESMO Gateway package as according to the GitLab wiki guidelines.
3. Update and maintain ESMO GitLab wiki for country specific preproduction deployment and test environment.
4. Report any bugs to ESMO GW Software Developers as they arise.

2.3.3 Step 3: Integration

EWP Administration Body will:

1. Provision country ESMO Gateways to the EWP Registry Service.
2. Support ESMO integration with EWP.
3. Provide operational support.

eIDAS-node Provider will:

1. Support ESMO Gateway integration.
2. Approve ESMO Gateway to be connected to live eIDAS production system.
3. Provide operational support.

Service Provider will:

1. Request their eServices to be connected to local ESMO Gateway.
2. Integrate eServices with ESMO Gateway.
3. Document their test cases to be tested, as per the ESMO test case specification.
4. Report any bugs to ESMO GW Software Developers as they arise.

Attribute Provider will:

1. Request their AP service to be connected to local ESMO gateway.
2. Integrate and test dummy eService with ESMO Gateway.
3. Report any bugs to ESMO GW Software Developers as they arise.

ESMO GW Administration Body will:

1. Integrate with EWP network.
2. Integrate with eIDAS in preproduction.

Document name:	D2.2 Integration and Testing Plans			Page:	15 of 29
Reference:	D2.2	Dissemination:	PU	Version:	1.0
				Status:	Final

3. Provision Service Providers in preproduction ESMO Gateway and support their integration.
4. Provision Attribute Providers in preproduction ESMO Gateway and support their integration.

2.3.4 Step 4: End-to-end Testing

Service Provider will:

1. Demonstrate eServices fully tested in pre-production fulfill the ESMO Validation Test Plan.

ESMO GW Administration Body will:

1. Perform dummy eService to test interoperability and functionality with eIDAS, Attribute Providers and other ESMO gateways.
2. Approve SPs and APs to be connected on live ESMO production gateway after previous step is passed, and also on SP passing the ESMO validation Test Plan.
3. Provide operational support.

Attribute Provider will:

1. Provide operational support.

EWP Administration Body will:

1. Provide operational support.

eIDAS-node Provider will:

1. Provide operational support.

2.3.5 Step 5: Operational testing in production

ESMO GW Administration Body will:

1. Connect with EWP in production.
2. Connect with eIDAS in production.
3. Perform dummy eService to test interoperability and functionality with eIDAS, Attribute Providers and other ESMO gateways.
4. Provide operational support.

EWP Administration Body will:

1. Provision country ESMO Gateways to the EWP Registry Service in production.
2. Provide operational support.

eIDAS-node Provider will:

1. Approve ESMO Gateway to be connected to live eIDAS production system.
2. Support ESMO Gateway connectivity in production.
3. Provide operational support.

Attribute Provider will:

1. Request their AP service to be connected to local ESMO gateway in production.
2. Integrate and test dummy eService with ESMO Gateway.
3. Report any bugs to ESMO GW Software Developers as they arise.

Service Provider will:

1. Request their eServices to be connected to local ESMO Gateway in production.

Document name:	D2.2 Integration and Testing Plans			Page:	16 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

2. Connect their eServices with ESMO Gateway.
3. Provide real end user testing of live eServices to obtain end user experiences.
4. Report any bugs to ESMO GW Software Developers as they arise.

2.4 Test environment and tools

Pre-production will be the test environment employed to carry out the full integration of the ESMO Gateway with all external nodes, as depicted by the figure below.

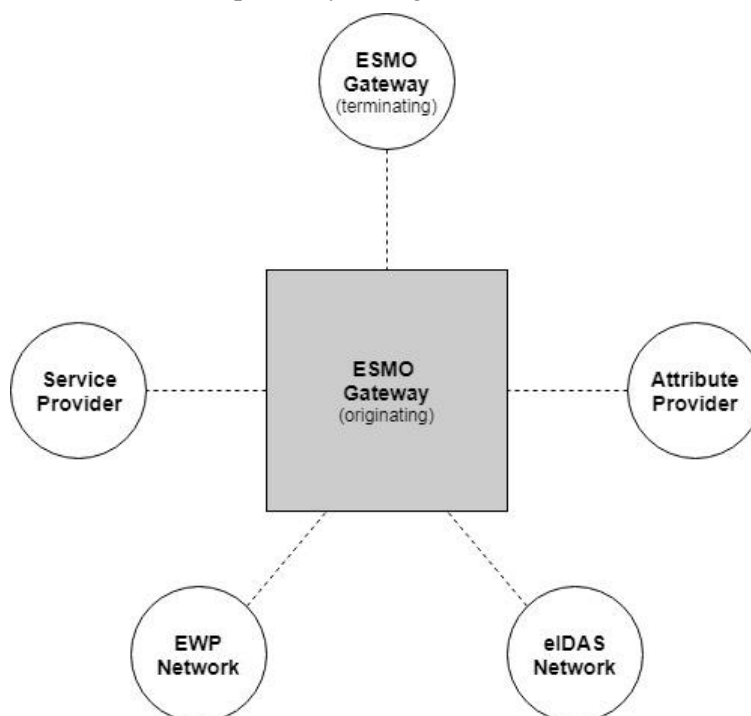


Figure 2: ESMO Gateway integration with external nodes in preproduction

The ESMO Gateway will be deployed on a Member State basis and will support connections to multiple SPs, APs and other ESMO Gateways belonging to other member states. Each country deployment needs to specify the ESMO Gateway modules deployed in their specific ESMO GitLab wiki to support the different country specific interfaces towards eIDAS, SPs and APs.

The preproduction test environment should reflect as much as possible the real production environment with platform infrastructure, firewalls, routing network etc.

The test environment will make use of test eID credentials made available from each of the Member State eIDAS-node Providers. These will vary from simple userId and password to software-based certificates with PIN.

All Service Provider eServices will be accessed via web browser, which will require that certificate-based credentials are installed.

For debugging purposes, it is recommended to capture traces on the ESMO Gateway, as well as on the network using the Wireshark tool [2].

Document name:	D2.2 Integration and Testing Plans			Page:	17 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

Where an integration issue is found it is recommended to return to the development integration environment making use of mock responses and updating the mock tool to test the issue. For this purpose, it is recommended to use the Swagger Inspector [3].

It is aimed to carry out end-to-end tests in an automated or semi-automated manner, as the eID credential allows. This will be based on the Selenium tool set [4] and its methodology will be defined in task 6.1. When re-running tests for regression or testing corrections, it is much more efficient using this tool to repeat the tests in an automated fashion.

It is aimed to carry out end-to-end tests in an automated or semi-automated manner, as the eID credential allows. This will be based on the Selenium tool set [5] and its methodology will be defined in task 6.1. When re-running tests for regression or testing corrections, it is much more efficient using this tool to repeat the tests in an automated fashion. Essentially, this tool augments the functionality of a similar tool that has been developed in the context of LEPS project [5].

2.5 Issue tracking

GitLab [6] is the repository for the ESMO Gateway software development.

The project will use GitLab's inbuilt Issue Tracker, for raising and managing bugs in the software and wiki documentation.

Document name:	D2.2 Integration and Testing Plans				Page:	18 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

3 Test Case Specification

As indicated in the methodology, each Service Provider is responsible for the thorough testing of their eServices. As part of this it is required that Test Cases are produced by each Service Provider that fully cover the testing of their eServices.

3.1 Test case template

A Test Case template is given below that should be used for specifying the test cases derived from the Service Provider eService use cases.

Table 1: Service Provider eService Test Case Template

Test case ID	SPname.eServiceTitle.TC###
Description	What is going to be tested.
Preconditions	The requirements to run this test.
Process	The steps to execute the test: <ol style="list-style-type: none"> 1. First step, ... 2.
Result	The expected result.
[Preproduction/ Production] conditions	According to the testing environment, different requirements could be specified here.

3.2 Test case example

An example SP eService test case for HEI student admissions is given below. It follows the typical example of a student first authenticating on eIDAS before being redirected over the ESMO Gateway Network to an HEI Attribute Provider. In the DSA query to the HEI AP it uses the eID identifier previously retrieved from eIDAS to retrieve the students Domain Specific Attributes. In the alternative case that the eID identifier is not recognised by the HEI AP it is needed for the student to re-authenticate. Once identified at the AP the attributes are returned to the ESMO Gateway and if no other APs are to be queried then the collected attribute values are confirmed by the student to be returned to the Service Provider eService.

Document name:	D2.2 Integration and Testing Plans	Page:	19 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Table 2: Example SP eService Test Case

Test case ID	XYZ.admissions.TC001
Description	Successful application for courses at XYZ University with eIDAS identity.
Preconditions	<ul style="list-style-type: none"> • The <i>nominated</i> (*) student has national electronic eID and credentials. • Required eIDAS Attributes: PersonIdentifier, FirstName, FamilyName. • Optional eIDAS Attributes: DateOfBirth. • Domain Specific Attributes required: eduPersonAffiliation (to check the student status), schacHomeOrganization, study program. • A student is nominated for exchange to a XYZ University from another eIDAS country. • The student is thereby registered as a possible applicant and receives an invitation e-mail containing a link including an invitation-token to the admission system. <p>(*) by invitation from a nomination process.</p>
Process	<p>the Application Service, the student selects to login using eIDAS.</p> <ol style="list-style-type: none"> 1. The student receives an admission's email from University XYZ and upon clicking on the link is re-directed to the ESMO Gateway. Included in the redirection are the eIDAS authentication attributes requested, and also the DSAs requested for the eService. 2. The student is requested by the ESMO Gateway to select the country for authentication of their eID. Once selected the student is redirected over eIDAS to her Member State's IdP. 3. The student authenticates with her Member state's eID provider. 4. eIDAS basic attributes are returned to the ESMO Gateway and requests the user to select the Member State and HEI AP to retrieve her HEI DSAs from. 5. The DSA request is found to be in another Member State and is redirected to the ESMO Gateway that serves on behalf of the HEI AP selected by the student. 6. The student's record is found on the AP, and the AP obtains the consent from the user to return the attributes to the Service Provider via the ESMO Gateway Network. Note: <u>Alternatively</u>, if the record is not found the student is required to re-authenticate at the AP. 7. The local originating ESMO Gateway receives the DSA response and queries the student if she wants to return these values back to the SP or look for more attributes from other HEI APs. 8. In this case the student selects to return all retrieved DSAs as well as the eIDAS attributes which are then returned to the SP Admissions eService. They are added to the Admissions Web user record, appended to the nomination data, linked through the invitation token. 9. The Admissions eService checks the student is still active at the home university. 10. The student completes her application. 11. The Admissions eService indicates that the student admissions application has been successfully completed.

Document name:	D2.2 Integration and Testing Plans	Page:	20 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Result	The foreign student completes an admissions application for a course at XYZ University.
[Preproduction/ Production] conditions	Test eIDs will be used in pre-production, whereas real eIDs must be used in production environment. The student has to be enrolled in an AP connected to the ESMO Gateway network as AP.

Document name:	D2.2 Integration and Testing Plans				Page:	21 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

4 Validation Test Plan

This section details the ESMO GW requirements that should be validated as part of the end-to-end testing. The end-to-end test cases will be specified as part of Activity 6.

Tables are used to capture the key requirements to be validated such as ESMO GW functionality, interoperability, end user perception on usability etc. The table “Test ID” column identifies the test and is formatted so to identify the requirement being tested with test number and sub test number.

For example, **AuthN001.0** validates eIDAS authentication (**AuthN**) works correctly over the ESMO Gateway. The **001** component identifies the high-level requirement being tested, and the following **.0** indicates the main requirement to validate whereas subsequent sequential **.1, .2** table entries indicate sub requirements to the main requirement.

The table “Description” column provides a short description of the requirement being validated.

The “Result” column gives a simple Boolean “OK/NOK” value if the test was passed. In the event that the test validation is not applicable, it should be entered “N/A”.

The end-to-end architecture deployment needed for testing the eServices and proving the required interaction with the ESMO Gateway is shown in the following figure.

Document name:	D2.2 Integration and Testing Plans				Page:	22 of 29	
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final

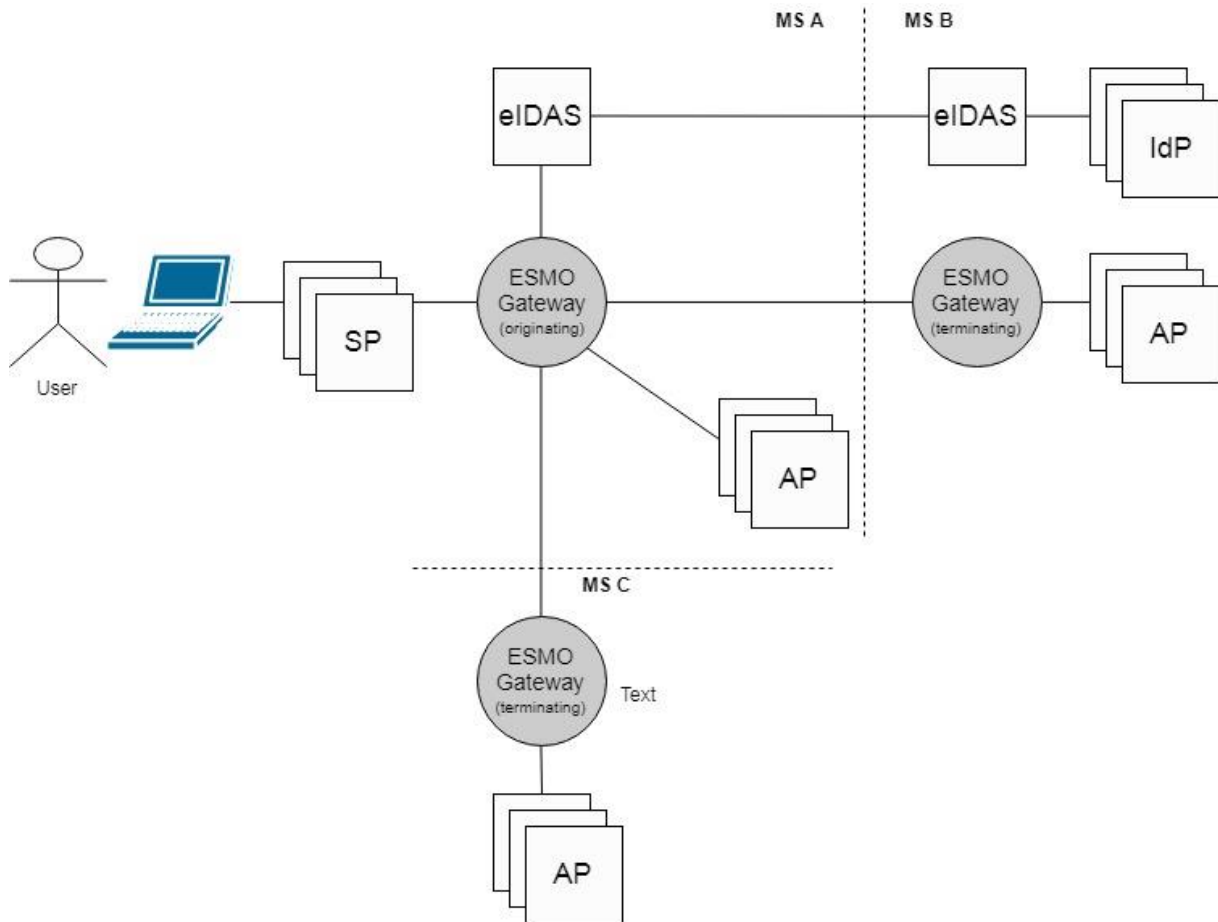


Figure 3: End-to-end test architecture

The originating ESMO Gateway will be tested for its interaction with SPs and their eServices, APs and eIDAS (cross-border authentication). The terminating ESMO Gateway’s will be tested that they provide the necessary functionality for connecting to remote APs residing in other Member States.

Document name:	D2.2 Integration and Testing Plans			Page:	23 of 29
Reference:	D2.2	Dissemination:	PU	Version:	1.0
				Status:	Final

4.1 Authentication

The following tests have been identified in relation to authentication (AuthN) over the ESMO Gateway to the eIDAS Network, and national IdPs.

Table 3: eIDAS Authentication

Test ID	Description	RESULT (OK/NOK)
AuthN001.0	User is successfully authenticated cross-border against eIDAS, in order to access the eService. No DSA were requested.	
AuthN001.1	User is able to select the country Member State to which their eID is authenticated on the ESMO Gateway, and not on the eIDAS Connector. No DSA were requested.	
AuthN001.2	User is able to select the country Member State to authenticate the user eID on the eIDAS Connector [8], and not on the ESMO Gateway. No DSA were requested. (This is alternative configuration to AuthN001.1).	
AuthN001.3	User is not successfully authenticated cross-border against eIDAS, if their credentials are not valid. No DSA were requested.	

4.2 Attribute aggregation

Several key tests (DSA prefix) have been identified in relation to ESMO functionalities managing academic Domain Specific Attributes as well as eIDAS attributes.

Table 4: Attribute aggregation

Test ID	Description	RESULT (OK/NOK)
DSA001.0	Academic attributes retrieved from an HEI/AP connected to the <i>originating</i> ESMO Gateway are successfully aggregated with eIDAS MDS and received by the eService. (DSA are requested in the cross-border Authentication request.)	
DSA001.1	User indicates the MS and AP in the discovery WAYF service.	
DSA001.2	User selects (consents) which attribute values are shared with the SP eService.	

Document name:	D2.2 Integration and Testing Plans	Page:	24 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Test ID	Description	RESULT (OK/NOK)
DSA002.0	Academic attributes retrieved from an HEI/AP connected to a <i>terminating</i> ESMO Gateway are successfully aggregated with eIDAS attributes and received by the eService. (DSA are requested in the cross-border Authentication request.)	
DSA002.1	On the Originating GW, the user indicates the MS and AP in the discovery WAYF service.	
DSA002.2	On the Originating GW, the user selects (consents) which academic attribute values are shared with the SP eService.	
DSA003.0	Academic attributes retrieved from <i>several</i> different APs connected to the originating ESMO Gateway are successfully aggregated with eIDAS MDS and received by the eService. (DSA are requested in the cross-border Authentication request.)	
DSA003.1	On the Originating GW, the user selects the MS and AP in the discovery WAYF service, for each AP that the user selects to query the DSA attributes. No discovery WAYF service is triggered on the terminating Gateway.	
DSA003.2	On the Originating GW, the user indicates the MS of the AP in the discovery WAYF service, for each AP the user selects to query the DSA attributes. The user will continue to select the AP on the discovery WAYF service in the corresponding terminating ESMO Gateways. (This is alternative configuration to DSA003.1).	
DSA003.3	On the Originating GW, the user's aggregated attributes (eIDAS & DSA) are displayed to the user to select (consent) to which attribute values are shared with the SP eService.	
DSA004.0	Academic attributes collected from <i>several</i> APs over different terminating ESMO Gateways are successfully aggregated with eIDAS MDS and received by the eService. (DSA are requested in the cross-border Authentication request.)	
DSA004.1	On the Originating GW, the user selects the MS and AP in the discovery WAYF service, for each AP that the user selects to query the DSA attributes. No discovery WAYF service is triggered on the terminating Gateway.	

Document name:	D2.2 Integration and Testing Plans	Page:	25 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Test ID	Description	RESULT (OK/NOK)
DSA004.2	On the Originating GW, the user indicates the MS of the AP in the discovery WAYF service, for each AP the user selects to query the DSA attributes. The user will continue to select the AP on the discovery WAYF service in the corresponding terminating ESMO Gateways. (This is alternative configuration to DSA004.1).	
DSA004.3	In the case that the user record is not found in the AP, the AP should offer the user to login to the AP using the user's credentials and so the user's DSAs are retrieved via the ESMO Gateway.	
DSA004.4	In the case that the eID is not provided in the DSA request to the AP, the AP should offer the user to login to the AP using the user's credentials and so the user's DSAs are retrieved via the ESMO Gateway.	
DSA004.5	On the Originating GW, the user's aggregated attributes (eIDAS & DSA) are displayed to the user to select (consent) to which attribute values are shared with the SP eService.	

4.3 Interoperability

ESMO GW is acting as facilitator of interoperability between HEI SP, and eIDAS for cross-border national eID authentication and AP systems for the retrieval of Domain Specific Attributes, supporting various protocols and industry standards. The following table, validates the various SP and AP protocols are integrated correctly in ESMO, as well as the interoperability with eIDAS, EWP and other ESMO Gateways in terminating scenarios.

Table 5: Interoperability

Test ID	Description	RESULT (OK/NOK)
Interop001.0	ESMO Gateway is interworking correctly with the SP.	
Interop001.1	The SP demonstrates a SAML interface, over the ESMO Gateway, is working correctly.	
Interop001.2	The SP demonstrates an OIDC interface, over the ESMO Gateway, that is working correctly.	
Interop002.0	ESMO Gateway is interworking correctly with the AP.	

Document name:	D2.2 Integration and Testing Plans	Page:	26 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Test ID	Description	RESULT (OK/NOK)
Interop002.1	The AP demonstrates a SAML interface over the ESMO Gateway is working correctly.	
Interop002.2	The AP demonstrates a SAML interface over the ESMO Gateway is working correctly.	
Interop002.3	The AP demonstrates an OAuth2 interface over the ESMO Gateway is working correctly.	
Interop002.4	The AP connected conforms to national integration specification.	
Interop002.5	The AP connected conforms to eduGAIN interwork specification.	
Interop004.0	ESMO Gateway is interworking correctly with EWP.	
Interop005.0	ESMO Gateway is interworking correctly with eIDAS.	
Interop006.0	ESMO Gateway is interworking correctly with a terminating ESMO Gateway.	

4.4 End user experience

Finally, some usability tests are defined in order to check a valid end user experience when ESMO network is used. The following table lists the UX tests.

Table 6: End user experience

Test ID	Description	RESULT (1 - bad to 5 - Good)
UX001.0	User is able to authenticate with eIDAS without any issue.	
UX001.1	User finds the login process intuitive and easy to follow.	
UX002.0	User can retrieve Domain Specific Attributes without any issue.	
UX002.1	User can easily find/select their HEI Attribute Provider(s).	
UX002.2	User finds the Domain Specific Attributes retrieval intuitive and easy to follow.	
UX002.3	User is content with interaction with AP not requiring 2 nd login.	

Document name:	D2.2 Integration and Testing Plans	Page:	27 of 29	
Reference:	D2.2	Dissemination:	PU	
	Version:	1.0	Status:	Final

Test ID	Description	RESULT (1 - bad to 5 - Good)
UX002.3	User is content with interaction with AP requiring a 2 nd login.	
UX003.0	User is able to login to eService, without any issue.	
UX003.1	User is content with the speed of login to their eService.	
UX003.2	User always knows which step is taking place during an ESMO interaction.	
UX003.3	User is content that they are in control of their data and can choose to not share any specific elements of their data, during login.	
UX003.4	User thinks the login process can be improved.	

References

- [1] Deliverable ESMO D2.1 - Cross-border mechanisms and Technical Design for the effective use of eID DSI. Ross Little. 2018
- [2] Wireshark. <https://www.wireshark.org/> 2018-09-05
- [3] Swagger Inspector. <https://swagger.io/tools/>. 2018-09-05
- [4] Selenium tools, <http://www.seleniumhq.org/>. 2018-09-06
- [5] LEPS project, <http://www.leps-project.eu/> .2018-09-26
- [6] GitLab. <https://gitlab.ATOSresearch.eu/>. 2018-09-03
- [7] EWP Network registration. <https://github.com/erasmus-without-paper/ewp-specs-api-discovery.2018-09-06>
- [8] eIDAS-Node National IdP and SP Integration Guide v2.1.pdf

Document name:	D2.2 Integration and Testing Plans			Page:	29 of 29		
Reference:	D2.2	Dissemination:	PU	Version:	1.0	Status:	Final