Project Title	Trust-aware, Reliable and Distributed Information Security in the Cloud
Project Acronym	TREDISEC
Project No	644412
Instrument	Research and Innovation Action
Thematic Priority	Cybersecurity, Trustworthy ICT
Start Date of Project	01.04.2015
Duration of Project	36 Months
Project Website	www.tredisec.eu

<D6.2 - EVALUATION CRITERIA>

Work Package	WP 6, Development, delivery and evaluation of the TREDISEC framework
Lead Author (Org)	Beatriz Gallego-Nicasio (ATOS) and David Vallejo (ARSYS)
Contributing Author(s) (Org)	Andreas Fischer (SAP) Hubert Ritzdorf (ETH) Dimitris Mitropoulos (GRNET) Julien Keuffer (MORPHO)
Reviewers	Wenting Li (NEC), Jose Ruiz (ATOS)
Due Date	M24
Date	31.03.2017
Version	2.3

Dissemination Level

☒ PU: Public

□ CO: Confidential, only for members of the consortium (including the Commission)

The work described in this document has been conducted within the project TREDISEC. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 644412. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Versioning and contribution history

Version	Date	Author	Notes
0.1	26.01.2017	Beatriz Gallego-Nicasio	First version
0.5	16.02.2017	Andreas Fischer, Julien Keuffer, Dimitris Mitropoulos, Hubert Ritzdorf, David Vallejo	Section 3.1 reviewed
0.6	22.02.2017	David Vallejo	Section 2.1 reviewed
0.7	22.02.2017	David Vallejo	Section 3.3.3 reviewed And section 3.1.1 with security area added
0.8	23.02.2017	Andreas Fischer	Section 2.1 reviewed
0.9	27.02.2017	Julien Keuffer and Beatriz Gallego-Nicasio	Section 3.3 contributions
1.0	27.02.2017	Andreas Fischer and David Vallejo	Section 3.3 contributions
1.1	28.02.2017	David Vallejo	Section 1
1.2	01.03.2017	Andreas Fischer	Section 3.3.6 updated
1.3	06.03.2017	Andreas Fischer and Dimitris Mitropoulus	Section 3.3 updated
1.4	06.03.2017	David Vallejo and Dimitris Mitropoulus	Exec summary and Section 3.3 updated
1.5	07.03.2017	David Vallejo	Exec summary ready, and comments deleted
1.6	08.03.2017	David Vallejo	Section 3.3.3 updated, and conclusions
1.7	08.03.2017	David Vallejo	Section 3.3.3 updated
1.8	09.03.2017	David Vallejo	Section 2.2 and 3.3.7 removed comments and reviewed.
2.0	20.03.2017	David Vallejo	Updated with feedback of the reviewers
2.2	28.03.2017	David Vallejo	Updated with feedback of the approver
2.3	30.03.2017	David Vallejo	Updated with feedback from quality check

Disclaimer

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Table of Contents

List of Tables

List of Figures

No table of figures entries found.

Executive Summary

In this deliverable we describe the methodologies that we plan to use in order to evaluate the outcomes of TREDISEC. We present our approach to assess whether the results of the project fulfil the requirements and necessities of the use cases, identified in deliverable D2.1 "Description of the context scenarios and use cases definition",[1] and to measure to what extent these requirements are met.

TREDISEC has two major technological outcomes: the TREDISEC Framework and the security primitives. In our approach, we perform the assessment of the maturity level of these results by deploying the TREDISEC Framework and security primitives in the use cases of the project and other internal testing environments.

Along the evaluation process we will validate compliance to the requirements identified in WP2 (cf. D2.2 "Requirements Analysis and Consolidation"[2]), and assess the degree of enhancement brought by the TREDISEC technological outcomes in each use case. On one side, we will evaluate the overall project success by concluding whether the objectives have been achieved. In this case, we refer to the evaluation criteria defined by all the use case owners and the framework owners. On the other side, we evaluate the TREDISEC technological outcomes, i.e. the framework and the security primitives, by deploying them in the use cases and using the corresponding indicators to perform measurements.

In order to homogenise the different evaluations, we have defined two different types of domain-specific indicators to evaluate TREDISEC technologies: use case process indicator, which focuses on the process described in each use case; and technology-related indicators, which focuses on functional and non-functional characteristics of the technologies developed. For each of the objectives a success criterion is defined together with the measurement methodologies.

Notice that for all use cases and the framework, the focus areas to be evaluated along the processes and requirements fulfilment are defined in detail by all use case and framework owners.

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to describe the evaluation criteria that will be considered for the TREDISEC outcomes. Additionally, this deliverable also aims to define the way to assess the maturity level of the TREDISEC technological outcomes, which include the TREDISEC Framework and the security primitives.

1.2 Structure of the document

The document is structured in two main sections. Section 2 describes the overview of the evaluation approach, including the general concept of how to evaluate the overall project success and the project outcomes. It also introduces the success criteria and measurements methodologies.

Section 3 describes the measurement metrics that will be evaluated. We define the use case processes as well as their requirements, together with a list of criteria descriptions for each of the 6 use cases and the framework. Finally, Section 4 presents the conclusions and lessons learned for the design of the evaluation process and how we plan to execute it later in the project.

2 TREDISEC Evaluation

The TREDISEC outcomes will be evaluated along two main areas: the TREDISEC Framework and the security primitives. The TREDISEC Framework allows the creation, storing, downloading and management of security primitives and TREDISEC Recipes. More specifically, a security primitive is a specification of a security and functional property for the cloud domain. In TREDISEC it can be either a security primitive pattern (which defines the design and other high-level description of the solution) or a security primitive implementation (which defines an implementation of the previously mentioned artefact) A TREDISEC Recipe is a software package with one or more security primitive implementations that includes scripts for installing/integrating it in a specific target cloud environment. More information about these components can be found in Deliverable 2.3 “TREDISEC architecture and initial framework”[3].

2.1 General Objectives of the Evaluation

In this sub-section we define the high-level objectives of the evaluation task and identify the set of criteria that assess, at a general level, its success.

All in all, **the final goal of the evaluation is to assess the maturity level of the TREDISEC technological outcomes, which are the TREDISEC Framework and the security primitives.**

As defined in the DoA[4], the TREDISEC technological results maturity level must reach TRL 6[5], i.e. it aims at demonstrating technology in a relevant environment (industrially relevant environment in the case of key enabling technologies).

Following, we have decomposed the general objective described previously into the following high-level objectives related to the TREDISEC outcomes:

- Develop and instantiate an evaluation environment which represents a set of industrially relevant scenarios. In TREDISEC these scenarios are represented by the use cases described in WP2 (cf. D2.1)
- Deploy and evaluate the TREDISEC Framework in the evaluation environment (i.e. the use cases instances).
- Deploy and evaluate all the primitives developed in the evaluation environment (i.e. the use cases instances).

In addition, the evaluation task is an opportunity for the TREDISEC consortium to ensure high-quality software and services that will be delivered to market. This way, we aim at:

- Gathering end-user satisfaction and first-hand feedback from experts.
- Gathering metrics to support better exploitation of the outcomes (e.g. key metrics).
- Gathering cloud providers’ feedback to improve the commercial and marketing strategies.
- Gathering user experience and main interests regarding TREDISEC technology.

More specifically, the evaluation of the technological outcomes is two-fold:

- Assessment of their compliance to the requirements identified in WP2 (cf. D2.2),
- Assessment of the degree of enhancement or hindrance that using the TREDISEC technological outcomes introduce to the Use Cases, in comparison to common practice.

Therefore, we define the list of our evaluation criteria according to the above two aspects.

2.2 Evaluation process

This is a preliminary description of the process to conduct the evaluation of TREDISEC in the use cases. A detailed planning, design and report on the execution of the evaluation sessions will be described in deliverable D6.4, due in M36. This will include:

- Define the process to be followed for conducting the evaluation.
- Define the evaluation team, the roles required, etc.
- Define the methodology to be followed: interviews with end-users/users, comparison before/after TREDISEC, observation of user interaction, assessing of the TREDISEC technologies by security experts, etc.
- Define the tools to support the evaluation process: online surveys, scripts, documentation, demos, webinars, etc.

Regarding the process to decide how to evaluate the TREDISEC outcomes, several points will be considered:

- Compare execution of UCs without TREDISEC vs. with TREDISEC (2 different sessions)
- Compare with other existing solutions (if any)
- Assessment of the technology solutions provided by TREDISEC by security and IT experts

2.2.1 Evaluation of the overall project success

Project success can be assessed by concluding whether the objectives identified in the previous section have been met or not. Also, compliance to general project objectives (as defined in the DoA) is paramount to conclude that the project has succeeded in achieving its original goals. In order to assess that, these objectives are linked to the evaluation criteria defined in Section 3. The level of achievement can be measured because those criteria are mapped to a set of indicators used to evaluate TREDISEC technological outcomes in the context of the UCs.

It is worth mentioning that the project is also assessed in terms of its innovative component along 3 dimensions (organizational, scientific/technical and market). This assessment also serves to evaluate the project success and is done in the context of Task 1.3. Deliverable D1.5[6] “Innovation Strategy Plan” details the framework for the continuous assessment of the project innovations.

2.2.2 Evaluation of the TREDISEC technological outcomes

We conduct the evaluation of the technological outcomes as follows: we deploy the TREDISEC Framework and the security primitives to the target cloud infrastructure and instantiate the use cases (as defined in WP2). Following, we execute a series of evaluation cases and use the corresponding indicators to perform measurements.

Here, two different types of domain-specific indicators are defined to evaluate the TREDISEC technologies:

- ***UC Process Indicators*** (focusing on the **process** described in the use case)
  - Purpose: Measure process performance improvements
  - Scale: Numeric values or categories
  - Measurement: Analysis of log files, manual assessment of the performance of the supported process, interviews, observation studies with potential end-users.
- ***Technology-related indicators*** *(*focusing on functional and non-functional characteristics of the **technologies developed***)*
  - Purpose: Measure the degree of goal attainment of the tools regarding functional or non-functional characteristics
  - Scale: Categories or numeric values
  - Measurement: Manual test and assessment of the technologies by means of interviews, observation studies with potential end-users or performance tests.

2.3 Success criteria

In order to measure the success of the evaluation, with regards to the objectives listed in Section 0, a set of success criteria can be established. Table 1 summarizes the objectives and the success criteria.

Objective	Contributes to	Success Criteria
O.1 Assessing the maturity level of the TREDISEC technological outcomes that is the TREDISEC Framework and the security primitives		TRL 6: demonstrating technology in a relevant environment (industrially relevant environment in the case of key enabling technologies)
O.2 Gather end-user satisfaction and first-hand feedback from experts with regards to the use of the TREDISEC technological outcomes		
O1.1 Develop and instantiate an evaluation environment which represent a set of industrially relevant scenarios (i.e. the use cases described in D2.1).	O.1	100% of the technical tasks will include at least one primitive for each of the use cases 90% of the technological outcomes of the project can be evaluated at least in one use case instantiation.
O1.2 Deploy and evaluate the TREDISEC Framework in the context of the use cases	O.1	90% of the evaluation cases related to the TREDISEC Framework are executed from start to end. 80% of the indicators associated to each evaluation case have been assessed.
O1.3 Deploy and evaluate all the primitives developed in TREDISEC in the context of the use cases.	O.1	90% of the evaluation cases related to the TREDISEC security primitives are executed from start to end. 80% of the indicators associated to each evaluation case have been assessed.
O1.2.1 Assess compliance of the TREDISEC security primitives to the requirements defined in D2.2	O1.2	100% of the mandatory requirements are assessed (i.e. the corresponding evaluation case is executed) 90% of the mandatory requirements are fulfilled 25% of the optional requirements are fulfilled
O1.3.1 Assess compliance of the TREDISEC framework to the requirements defined in D2.2	O1.3	100% of the mandatory requirements are assessed (i.e. the corresponding evaluation case is executed) 90% of the mandatory requirements are fulfilled 25% of the optional requirements are fulfilled
O1.2.2 Assess enhancement/hindrance of the UC process by using the TREDISEC	O1.2	100% of the related UC process criteria evaluated (i.e. the corresponding evaluation cases is executed)

security primitives		
O1.3.2 Assess enhancement/hindrance of the UC process by using the TREDISEC security primitives	O1.3	100% of the related UC process criteria evaluated (i.e. the corresponding evaluation cases is executed)

Table 1: Objectives and success criteria

2.4 Measurement methodologies

In this section we describe the measurement methodologies we defined according to the different types of techniques we will use to measure all results.

Code	Typology	Description	Example
Q	**Q**uantitative report	This means clear quantitative indicators with a numerical target.	% time saved
I	**I**nterviews and user **I**nteraction analysis	For all indicators, including the user interaction and satisfaction, it is impossible to evaluate the success status without an analysis of real user behaviour in managing the system. For this reason this class of indicators will be used where the users interaction is needed	User interface satisfaction

Table 2: Measurement methodologies

3 Evaluation criteria

In this section we describe the evaluation criteria we defined according to the focus areas of application and the table templates we use for each of the use cases described in WP2.

3.1 Focus areas

The different technical areas for the evaluation of the TREDISEC results and the fulfilment of the requirements are identified in this section.

3.1.1 Impact in the UC process

In order to evaluate the impact of the TREDISEC technologies on the normal practice described in the use cases a set of evaluation criteria are defined focusing in the following areas:

Areas	**Focus**	**Goals**
Quality	Output of a process/activity	an increase in output quality (results) of a process/activity
Performance	Execution time of an activity and its latency. Throughput of a platform/service Memory Consumption Storage Consumption	minimum objective is not to reduce the previous performance KPIs (latencies, consumption and throughput)
Coverage	the breadth/depth of input processed	an increase in breadth/depth of input processed
Simplification	Resources (personnel, technological assets) needed to execute a process/activity	a decrease in resources needed to execute a process/activity
Security	Integrity, protection, availability and confidentiality of data	Data integrity, protection, availability and confidentiality are guaranteed
Usability	Usability of a user-interface/service	to keep a highly and friendly usability of a service

Table 3: Evaluation criteria

3.1.2 Fulfilment of the requirements

In order to evaluate whether the TREDISEC technologies fulfil the requirements and to what extent, a series of evaluation criteria are defined.

3.1.2.1 TREDISEC security primitives

Each security primitive deployed in a use case must assess its compliance to at least one requirement in the table below. The combination of all the security primitives deployed in a use case must cover all the mandatory requirements.

		Functional Requirements Mandatory(M)/Optional(O)						
	Use-Cases	Multi-tenancy	Storage efficiency	Computation efficiency	Data Access	Data Processing	Dynamicity	Availability
File Sharing Services	UC1	O	M		M		M	M
	UC2	M	M		M		M	M

	UC3	M	M		M		M	M
Big Data & Secure Processing Services	UC4			M		M		O
	UC5		O	M		M	O	O
	UC6	O	M	M		M	O	O

Table 4: Functional Requirements

		Security Requirements Mandatory(M)/Optional(O)			
	Use cases	Storage integrity	Computation integrity	Storage privacy	Computation privacy
File Sharing Services	UC1	M		M	
	UC2	M		M	
	UC3	M		M	
Big Data Storage and Secure Processing Services	UC4		M	O	O
	UC5	O	O	M	M
	UC6			M	M

Table 5: Security Requirements

3.1.2.2 TREDISEC Framework

Regarding the evaluation of the TREDISEC Framework we must define a list of evaluation criteria aiming to assess the degree of compliance to the requirements in the table below. Criteria must be defined for both mandatory and optional requirements.

Type	**Requirement**	**Mandatory or Optional**
Architectural	**WP2A1 Measurable framework**	O
	WP2A2 Configurable framework	M
	WP2A3 Flexible deployment model	M
	WP2A4 Semi-automated recovery from failure	O
	WP2A5 Semi-automated build, configuration and deployment processes	M
	WP2A6 Visibility and reporting	O
	WP2A7 Provide User Interfaces	M
	WP2A8 Scalability	M
	WP2A9 Interoperability	M
	WP2A10 Modular design	M
Quality	**WP2Q1 System Availability**	M
	WP2Q2 Elasticity	O
	WP2Q3 Security	M
	WP2Q4 Adaptability	M

	WP2Q5 Performance	M
	WP2Q6 Usability	O
	WP2Q7 Maintainability	O
Business	**WP2B1Quality for business**	M
	WP2B2 Market share	O
	WP2B3 Flexibility	M
	WP2B4 Stakeholder satisfaction	M
	WP2B5 Compliance	M

Table 6: Mandatory and optional requirements

3.2 Template of the evaluation criteria definition

We use the following templates for the definition of the evaluation criteria. The content of each field is explained in *blue colour and italic font*, and it will be adapted for each use case in the following section.

3.2.1 UC Process Evaluation

ID	*Unique identifier*	Use Case	*ID – Name*
Type	UC Process		
Focus Area	Time / Quality / Simplification / Coverage / ….		
Evaluation Criteria	*Which aspects are captured? What are the evaluation criteria?*		
Evaluation Objective	*General description of the goal to achieve. (Ref. D2.1 UC goals)*		
Other comments and considerations	*Does this evaluation depend on others to be executed? Is this evaluation related to others? Do we have special needs to evaluate this criterion (e.g. need to have deployed a Biometric Service, need to record the expert interacting with the tool, etc.)?*		

3.2.2 Technology-related Evaluation

ID	*Unique identifier*	Use Case	*ID – Name*
Type	Technology-related		
Focus Area	Functional / Non-functional requirements		
Evaluation Criteria	*Which aspects are captured? What are the evaluation criteria?*		
Evaluation Objective	*Functional/Non-functional: Related UC requirement (D2.2) evaluated with this criteria*		
Evaluation Objects	*Which objects do we evaluate? (Security primitives, TREDISEC Recipes, TREDISEC Framework)*		
Evaluation measurement	*How do we measure (methodology)? **Q**uantitative **r**eports / **I**nterviews or User Interaction*	Evaluation Scale	*Numeric values / Categories*
Evaluation Team	*Who measures? Who belongs to the evaluation team? Roles*		
Other comments	*Does this evaluation depend on others to be executed? Is this evaluation*		

and considerations	*related to others? Do we have special needs to evaluate this criterion (e.g. need to have deployed a Biometric Service, need to record the expert interacting with the tool, etc.)?*

3.2.3 Examples

3.2.3.1 UC process example

ID	UC3-P-01	Use Case	UC3
Type	Process		
Focus Area	Simplification (technological assets required)		
Evaluation Criteria	Impact on performance of the AC decisions taken over resources shared between tenants		
Evaluation Objective	UC3_BG.1 Provide multi-tenancy and access control, to an E2E encrypted data, with no impact in service efficiency and performance		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

3.2.3.2 Technology (security primitive) example

ID	UC3-T-01	Use Case	UC3
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Support for multiple tenants		
Evaluation Objective	Correct functioning of the AC module with multi-tenancy		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

3.2.3.3 Technology (TREDISEC Framework) example

ID	F- 01	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	All functionalities can be accessed by the end-user via user interface		
Evaluation Objective	WP2A7 Provide User Interfaces		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews or User Interaction	Evaluation Scale	Categories (YES/NO)

Evaluation Team	Tool-owner UC-owner (admin, end-user)
Other comments and considerations	This criterion focuses on the fact that the framework offers user interfaces to access all functionalities, and not by editing configuration files, running scripts, etc. Measurement can be captured via interview/questionnaire.

3.3 List of Evaluation Criteria

3.3.1 UC1: Storage efficiency with security (GRNET)

3.3.1.1 Impact on the UC process

ID	**UC1-P-01**	Use Case	**UC1**
Type	UC Process		
Focus Area	Quality, Simplification, Security		
Evaluation Criteria	The process should not change from the users' perspective. Security should not affect storage efficiency.		
Evaluation Objective	WP33-R2, WP33-R4: Verifiable ownership with data confidentiality and data reduction.		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the users and the tenant admin.		

3.3.1.2 Fulfillment of requirements

ID	**UC1-T-01**	Use Case	**UC1**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Should not require significant changes to the existing client infrastructure. Achieve efficient resource utilization		
Evaluation Objective	Correct functioning of the storage module with multi-tenancy		
Evaluation Objects	Security primitive: Storage efficiency (EURECOM recipe)		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	**UC1-T-02**	Use Case	**UC1**
Type	Technology-related		
Focus Area	Functional requirements: Security		
Evaluation Criteria	A file owner cannot take advantage of the deduplication feature to breach privacy.		
Evaluation Objective	Correct functioning of the Proof of Ownership (PoW) module.		
Evaluation	Security primitive: Proof of Ownership (IBM recipe)		

Objects			
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	**UC1-T-03**	Use Case	**UC1**
Type	Technology-related		
Focus Area	Functional requirements: Dynamicity		
Evaluation Criteria	The storage overhead for updates of various sizes compared to the whole file		
Evaluation Objective	Deduplication is transparent to the user apart from the time savings		
Evaluation Objects	Security primitive: Storage efficiency (EURECOM recipe)		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	**UC1-T-04**	Use Case	**UC1**
Type	Technology-related		
Focus Area	Security requirements: Storage efficiency, Storage Privacy		
Evaluation Criteria	Examine and compare apparent and real size consumption.		
Evaluation Objective	Deduplication is transparent to the user apart from the time savings.		
Evaluation Objects	Security primitive: Storage efficiency (EURECOM recipe)		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	**UC1-T-05**	Use Case	**UC1**
Type	Technology-related		
Focus Area	Functional requirements: Availability, Storage integrity		

Evaluation Criteria	Overhead of proofs should be within acceptable limits.		
Evaluation Objective	Correct functioning of the Proof of Ownership (PoW) module and proof checking.		
Evaluation Objects	Security primitive: Proof of Ownership (IBM recipe)		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

3.3.2 UC2: Multi-tenancy and access control (GRNET)

ID	**UC2-P-01**	Use Case	**UC2**
Type	UC Process		
Focus Area	Quality, Security, Simplification, Usability		
Evaluation Criteria	Users can protect their containers from other users and tenants.		
Evaluation Objective	*WP42-R1: Improved resource isolation.* *WP42-R2: Secure storage per tenant.*		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the users and the tenant admin.		

ID	**UC2-T-01**	Use Case	**UC2**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Users can securely migrate their containers inside a cloud infrastructure.		
Evaluation Objective	Secure data storage for each cloud tenant.		
Evaluation Objects	Security Primitive: Container Isolation (GRNET).		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	**UC2-T-02**	Use Case	**UC2**
Type	Technology-related		
Focus Area	Functional requirements: Security		

Evaluation Criteria	Users should be able to encrypt their containers.		
Evaluation Objective	Effective resource isolation.		
Evaluation Objects	Security Primitive: Container Isolation (GRNET).		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

ID	UC2-T-03	Use Case	UC3
Type	Technology-related		
Focus Area	Functional requirements: Data Access		
Evaluation Criteria	Attackers should not be able to access resources.		
Evaluation Objective	Effective access control.		
Evaluation Objects	Security Primitive: Container Isolation (GRNET).		
Evaluation measurement	Expert Review	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (end-user, admin)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin.		

3.3.3 UC3: Optimised WebDav service for confidential storage (ARSYS)

3.3.3.1 Impact on the UC3 process

ID	UC3-P-01	Use Case	UC3
Type	Process		
Focus Area	Quality, performance, coverage, usability and security (technological assets required)		
Evaluation Criteria	Resources shared between tenants work according to rules and permissions. Integrity, availability and confidentiality of user’s data. Protection of loss data. Data storage space optimization. Current quality and usability when browsing and current performance is not negatively impacted in a significant way. Optional: secure deletion (no access to deleted files or folders)		
Evaluation Objective	UC3_BG.1 Provide multi-tenancy and access control to an E2E encrypted and de-duplicated data, with no significant impact in service performance		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin, together with the metrics to be measured and evaluated (figures to be defined).		

3.3.3.2 1.1.1.2 Fulfillment of requirements

ID	**UC3-T-01**	Use Case	**UC3**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Support for multiple tenants. No tenant can access to other tenant contents if they are not authorized (positive and negative cases).		
Evaluation Objective	Correct functioning of the AC module with multi-tenancy. Tenants content isolation.		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin. Performance of the service will be compared with current platform values (access time, latency and throughput) Related to UC3-P-01		

ID	**UC3-T-02**	Use Case	**UC3**
Type	Technology-related		
Focus Area	Nonfunctional requirements: Performance		
Evaluation Criteria	Performance of the service got no significant impact with regards to access times, latencies and throughput while conducting the multi-tenancy access.		
Evaluation Objective	Correct functioning of the platform and services running on it, with no significant impact with regards to access times, latencies and throughput.		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin. Performance of the service will be compared with current platform values (access time, latency and throughput) Related to UC3-P-01		

ID	**UC3-T-03**	Use Case	**UC3**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Support for multiple user within each tenant. A user or a group of users from Tenant A cannot access to other users' data from tenant A if there is no granted permission.		
Evaluation	Isolation of different user's data within each tenant.		

Objective			
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin. Performance of the service will be compared with current platform values (access time, latency and throughput) Related to UC3-P-01		

ID	**UC3-T-04**	Use Case	**UC3**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Support for multiple user within each tenant. A user or a group of users from Tenant A can access to other users data from tenant B according to granted permissions.		
Evaluation Objective	Data sharing among different users within each tenant.		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin. Performance of the service will be compared with current platform values (access time, latency and throughput) Related to UC3-P-01		

ID	**UC3-T-05**	Use Case	**UC3**
Type	Technology-related		
Focus Area	Functional requirements: Multi-tenancy		
Evaluation Criteria	Support for multiple user within each tenant. A user or a group of users from Tenant A can access to other users data from tenant B according to granted permissions.		
Evaluation Objective	Data sharing among different users within each tenant.		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire to the tenant admin. Performance of the service will be compared with current platform values		

	(access time, latency and throughput) Related to UC3-P-01

ID	UC3-T-06	Use Case	UC3
Type	Technology-related		
Focus Area	Functional requirements: Availability		
Evaluation Criteria	Overall performance of the cloud service is not negatively affected in a significant way, when the primitive is deployed in the cloud infrastructure with a load balancing schema in place		
Evaluation Objective	Correct functioning of the AC module with a high performance/availability deployment.		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Quantitative Report	Evaluation Scale	% performance increase/decrease
Evaluation Team	Technology-owner UC-owner (admin) Customers (end users)		
Other comments and considerations	Measurement can be captured by preparing a battery of requests and testing against the regular deployment and the high performance deployment. Related to UC3-P-01		

ID	UC3-T-07	Use Case	UC3
Type	Technology-related		
Focus Area	Security requirements: Storage Privacy		
Evaluation Criteria	Ensure privacy respectful storage of authorization policies and exchange of user information		
Evaluation Objective	WP41-R2: Privacy-respectful policy enforcement		
Evaluation Objects	Security primitive: AC for Multitenancy (ARSYS recipe)		
Evaluation measurement	Interview/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low (satisfaction with respect to tenant privacy concerns)
Evaluation Team	Technology-owner UC-owner (admin) Customers (admin)		
Other comments and considerations	This criterion can be refined into: - Ensure isolation of authorization policies, according to tenant privacy requirements (distributed policy stores) - Ensure only necessary attributes are present in the access request, according to tenant privacy requirements (the rest of required attributes are obtained in a privacy-respectful manner, in our case using a PIP component (see D4.4 for details) Related to UC3-P-01		

ID	UC3-T-08	Use Case	UC3
Type	Technology-related		
Focus Area	Performance and security.		

Evaluation Criteria	No access to any data (file, folder) if it is taken out of the storage system, as the data is encrypted. Deduplication factors are bigger than 1 while data is encrypted, hence same file or group of files size is smaller than in original source. E2E encrypted data and de-duplicated storage, with balanced impact in service efficiency and performance. User access time remains the same, and latencies and throughput changes within acceptable thresholds.		
Evaluation Objective	Secure data and save storage space		
Evaluation Objects	Security primitive: Data encryption and deduplication (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end users)		
Other comments and considerations	Measurement can be captured via storage monitors and encryption logs. Values for acceptance criteria will be obtained using current latency, throughput and access time values and a % of overhead. Related to UC3-P-01		

ID	UC3-T-09	Use Case	UC3
Type	Technology-related		
Focus Area	Security. Deleted files are not accessible any more. Performance of the service remains with same access times, latencies and throughput.		
Evaluation Criteria	No data (file, folder) can be recovered after secure deletion. Correct functioning of the platform and services running on it, with no significant impact with regards to access times, latencies and throughput.		
Evaluation Objective	Secure data		
Evaluation Objects	Secure deletion primitive: secure data deletion (ARSYS recipe)		
Evaluation measurement	Interview	Evaluation Scale	Yes/No
Evaluation Team	Technology-owner UC-owner (admin) Customers (end users)		
Other comments and considerations	Measurement can be captured via storage monitors and encryption logs. And performance of the service will be compared with current platform values (access time, latency and throughput) Related to UC3-P-01		

3.3.4 UC4: Enforcement of biometric-based access control (MPH)

3.3.4.1 Impact on the UC4 process

ID	UC4-P-01	Use Case	UC4
Type	Process		
Focus Area	Quality		
Evaluation Criteria	Cloud server supplies a proof that biometric matching was correctly performed. Each authentication result is associated with a proof.		

Evaluation Objective	UC4_BG.2: enforce the trust in the outsourced authentication service by providing a publicly verifiable proof that Cloud Authentication Server did its job correctly. WP32-R1: Computation integrity WP32-R2: Public verifiability
Other comments and considerations	Assume that the authentication process contains a biometric comparison which is delegated to a cloud server.

ID	**UC4-P-02**	Use Case	**UC4**
Type	Process		
Focus Area	Performance		
Evaluation Criteria	Verifying the proof to audit the Cloud Server can be done efficiently. Producing the proof does not degrade the Cloud Server performance.		
Evaluation Objective	UC4_BG.2: enforce the trust in the outsourced authentication service by providing a publicly verifiable proof that Cloud Authentication Server did its job correctly. WP32-R6: Verifiable computation with efficiency at the cloud. WP32-R7: Verifiable computation with efficiency at the client.		
Other comments and considerations	Assume that the authentication process contains a biometric comparison which is delegated to a cloud server.		

3.3.4.2 Fulfillment of requirements

ID	**UC4-T-01**	Use Case	**UC4**
Type	Technology-related		
Focus Area	Quality		
Evaluation Criteria	Proofs of biometric authentication are verifiable with a simple process.		
Evaluation Objective	WP32-R2: Public verifiability		
Evaluation Objects	Security primitive: Verifiable matching of biometric templates		
Evaluation measurement	User interaction reports	Evaluation Scale	Difficulty scale
Evaluation Team	UC-owner		
Other comments and considerations	Related to UC4-P-01		

ID	**UC4-T-02**	Use Case	**UC4**
Type	Technology-related		
Focus Area	Quality		
Evaluation Criteria	Computation integrity is guaranteed.		
Evaluation Objective	WP32-R1: Computation integrity		

Evaluation Objects	Security primitive: Verifiable matching of biometric templates		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Security analysis of the parameters. Reaction of the system when supplied with a false proof.
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC4-P-01		

ID	UC4-T-03	Use Case	UC4
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Generate and store a proof for each biometric matching is feasible.		
Evaluation Objective	WP32-R6: Verifiable computation with efficiency at the cloud.		
Evaluation Objects	Security primitive: Verifiable matching of biometric templates		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Time to generate the proof. Size of the proof to be archived.
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC4-P-02		

ID	UC4-T-04	Use Case	UC4
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Verification of the biometric matching proof is efficient.		
Evaluation Objective	WP32-R7: Verifiable computation with efficiency at the client.		
Evaluation Objects	Security primitive: Verifiable matching of biometric templates		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Time to verify the proof.
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC4-P-02		

3.3.5 UC5: Secure upgrade of biometric systems

3.3.5.1 Impact on the UC5 process

ID	UC5-P-01	Use Case	UC5
Type	Process		
Focus Area	Security		
Evaluation Criteria	Outsourced biometric data are encrypted. Encryption enables signal processing operations.		
Evaluation Objective	WP5-R1: Data confidentiality. WP53-R1: Privacy preserving data processing.		
Other comments and considerations	The biometric system will preferably implement face recognition (but could be limited to hand-written digits if the solution for face recognition is not effective).		

ID	UC5-P-02	Use Case	UC5
Type	Process		
Focus Area	Performance		
Evaluation Criteria	Accuracy and scalability of the biometric system over encrypted data.		
Evaluation Objective	UC5_BG.1: decrease the overall time and cost of biometric systems upgrading. WP53-R4: Performance/ Efficiency at the client. WP53-R6: Privacy preserving data processing with Big Data.		
Other comments and considerations	The biometric system will preferably implement face recognition (but could be limited to hand-written digits if the solution for face recognition is not effective).		

3.3.5.2 Fulfillment of requirements

ID	UC5-T-01	Use Case	UC5
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Keep the accuracy of the system acceptable while processing over encrypted data.		
Evaluation Objective	WP53-R6: Privacy preserving data processing with Big Data.		
Evaluation Objects	Security primitive: Biometric features extraction in the encrypted domain.		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Numeric values (false acceptance rate, false rejection rate)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Evaluation criterion linked to UC5-P-02.		

ID	**UC5-T-02**	Use Case	**UC5**
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Evaluate the throughput of the biometric system over encrypted data.		
Evaluation Objective	WP53-R4: Performance/ Efficiency at the client.		
Evaluation Objects	Security primitive: Biometric features extraction in the encrypted domain.		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Numeric values (time to extract features from one encrypted image, throughput: number of processed images per hours, communication needed, memory consumption and storage consumption).
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Evaluation criterion linked to UC5-P-02.		

ID	**UC5-T-03**	Use Case	**UC5**
Type	Technology-related		
Focus Area	Security		
Evaluation Criteria	Make sure that no private information leaks from the processing over encrypted data.		
Evaluation Objective	WP5-R1: Data confidentiality. WP53-R1: Privacy preserving data processing.		
Evaluation Objects	Security primitive: Biometric features extraction in the encrypted domain.		
Evaluation measurement	Quantitative Reports	Evaluation Scale	Security analysis of the encryption scheme parameters.
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Evaluation criterion linked to UC5-P-01.		

3.3.6 UC6: Database migration into a secure cloud (SAP)

3.3.6.1 Impact on the UC6 process

ID	**UC6-P-01**	Use Case	**UC6**
Type	Process		
Focus Area	Usability		
Evaluation Criteria	Whether or not the capability to execute SQL queries on data is preserved.		

Evaluation Objective	UC6_BG.1 Data migration into a secure cloud utilizing a parallelized encryption cluster while preserving the capability to execute SQL queries on the data
Evaluation Team	Technology-owner UC-owner
Other comments and considerations	Here we evaluate usability aspects of UC6_BG.1.

ID	UC6-P-02	Use Case	UC6
Type	Process		
Focus Area	Security		
Evaluation Criteria	Whether or not the data migration process fulfils security requirements.		
Evaluation Objective	UC6_BG.1 Data migration into a secure cloud utilizing a parallelized encryption cluster while preserving the capability to execute SQL queries on the data		
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Here we evaluate security aspects of UC6_BG.1.		

3.3.6.2 Fulfillment of requirements

ID	UC6-T-01	Use Case	UC6
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Overhead of storing data in encrypted form.		
Evaluation Objective	Functional requirement: Storage Efficiency		
Evaluation Objects	Security primitive: Secure Data Migration Service		
Evaluation measurement	**Q**uantitative report	Evaluation Scale	Numeric (Expansion Factor)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC6-P-01		

ID	UC6-T-02	Use Case	UC6
Type	Technology-related		
Focus Area	Performance		
Evaluation Criteria	Scalability of parallelized encryption cluster with regards to number of worker nodes		
Evaluation Objective	Functional requirement: Computation Efficiency UC6_FR.4: A method capable of encrypting multiple gigabytes of data.		
Evaluation Objects	Security primitive: Secure Data Migration Service		
Evaluation measurement	**Q**uantitative report	Evaluation Scale	Numeric (e.g. Speedup Factor by Number of Worker nodes)

Evaluation Team	Technology-owner UC-owner
Other comments and considerations	Related to UC6-P-01

ID	UC6-T-03	Use Case	UC6
Type	Technology-related		
Focus Area	Usability		
Evaluation Criteria	Whether an interface is provided for submitting SQL queries against a relational database.		
Evaluation Objective	Functional requirement: Data Processing UC6_FR.1 Clear text data can be queried from a relational database.		
Evaluation Objects	Security primitive: Secure Data Migration Service		
Evaluation measurement	**I**nterview	Evaluation Scale	Yes/No (Expert Analysis)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC6-P-01		

ID	UC6-T-04	Use Case	UC6
Type	Technology-related		
Focus Area	Usability		
Evaluation Criteria	How much of the data held in the source database is available from the target database after migration.		
Evaluation Objective	Functional requirement: Availability UC6_FR.1 Clear text data can be queried from a relational database.		
Evaluation Objects	Security primitive: Secure Data Migration Service		
Evaluation measurement	**Q**uantitative report	Evaluation Scale	Numeric (Percentage)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC6-P-01		

ID	UC6-T-05	Use Case	UC6
Type	Technology-related		
Focus Area	Security		
Evaluation Criteria	Whether or not key lengths used by encryption schemes are state-of-the-art.		
Evaluation Objective	Security requirement: Storage Privacy Security requirement: Computation Privacy UC6_NFR.1 Target database is enabled to store and process encrypted data. UC6_NFR.4 The cloud provider should not have access to the clear text of user data which was classified as sensitive by the data owner.		
Evaluation Objects	Security primitive: Secure Data Migration Service		

Evaluation measurement	Interview	Evaluation Scale	Yes/No (Expert Analysis)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC6-P-02		

ID	**UC6-T-06**	Use Case	**UC6**
Type	Technology-related		
Focus Area	Security		
Evaluation Criteria	Whether or not the cloud provider has access to clear text of user data which was classified as sensitive by the data owner.		
Evaluation Objective	Security requirement: Storage Privacy Security requirement: Computation Privacy UC6_NFR.4 The cloud provider should not have access to the clear text of user data which was classified as sensitive by the data owner.		
Evaluation Objects	Security primitive: Secure Data Migration Service		
Evaluation measurement	Interview	Evaluation Scale	Yes/No (Expert Analysis)
Evaluation Team	Technology-owner UC-owner		
Other comments and considerations	Related to UC6-P-02		

3.3.7 TREDISEC Framework

ID	**F- 01**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Transparency and auditability of the framework with regards to the resource usage of the security primitives deployed		
Evaluation Objective	WP2A1 Measurable framework		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	Premise: the security primitives and the target cloud should collaborate with the framework in reporting resource usage Resource usage aspects to monitor: - Storage - Processing - Bandwidth		

ID	**F- 02**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Degree of support offered by the framework to enable deployment of custom instances of the primitive in the target cloud system.		
Evaluation Objective	WP2A2: Configurable framework		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H – high, M- medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	Premise: the security primitives should collaborate with the framework in allowing the customization of the deployed primitive. Customization of primitives for deployment in terms of recipes available. Each recipe allows for customization of the primitive in terms of: - Target cloud platform (e.g. OpenStack, Amazon EC2) - Technical requirements (e.g. JRE 1.7, JRE 1.8) - Other cloud requirements (e.g. file-based deduplication, block-based deduplication) - Primitive alone or combined with other primitives		

ID	**F- 03**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Degree of customization of the framework		
Evaluation Objective	WP2A2: Configurable framework		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H – high, M- medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	Customization of the framework in terms of: - Enable the configuration of the operational components (i.e. testing component for different platforms, deployment component with support for advanced deployment options, etc.) - Enable the configuration of the overall framework characteristics (e.g. headless version to be used as a server repository of solutions via command line) - Enable the communication with external security primitives catalogues -		

ID	**F- 04**	Use Case	**ALL**

Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Degree of support offered by the framework to enable deployment of primitives in different cloud service models (SaaS, PaaS and IaaS), deployment options (hybrid, community, private, public), but also with different architectures offered by cloud service providers.		
Evaluation Objective	WP2A3: Flexible deployment model		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H – high, M- medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	This criterion is subject to the existence of primitives and recipes that can be deployed in the evaluated cloud categories. For example, the testing component should support different cloud service models (SaaS, PaaS and IaaS) as required by the security primitives.		

ID	F- 05	Use Case	ALL
Type	Technology-related		
Focus Area	Non-Functional		
Evaluation Criteria	Capability of the framework to recover from failure		
Evaluation Objective	WP2A4: Semi-automated recovery from failure		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H – high, M- medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	Evaluation in terms of failure recovery during the deployment steps (recipe execution).		

ID	F- 06	Use Case	ALL
Type	Technology-related		
Focus Area	Non-Functional		
Evaluation Criteria	Capability of the framework to provide continuous business operation (i.e. highly resistant to disruption and able to operate in a degraded mode if damaged)		
Evaluation Objective	WP2A4: Semi-automated recovery from failure		
Evaluation Objects	TREDISEC framework		
Evaluation	Interviews/Questionnaire	Evaluation	Scale: H – high, M- medium, L-

measurement		Scale	low
Evaluation Team	Tool-owner: ATOS, GRNET UC-owner (administrator)		
Other comments and considerations			

ID	**F- 07**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Capability of the framework to enable a semi-automated configuration, building and deployment of the selected security primitives over the target cloud system		
Evaluation Objective	WP2A5: Semi-automated build, configuration and deployment processes		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H – high, M- medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	This criterion is subject to the existence of primitives and recipes that can be deployed in a semi-automated mode. This is also related to the packaging of the artefacts.		

ID	**F- 08**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Functional		
Evaluation Criteria	Capability of the framework to report on system performance, security and compliance to enable monitoring customer SLAs and billing		
Evaluation Objective	WP2A6: Visibility and reporting		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	% aspects covered
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	Premise: the security primitives must collaborate with the framework in enabling this reporting Reporting aspects to evaluate: - Resource usage of primitives deployed (Dependencies: F01) - Improvement of the overall security achieved in the target cloud - Compliance - Billing (time of use, number of instances deployed, # times the primitive is invoked, MBs of storage secured, …)		

ID	**F- 9**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Framework functionalities accessible by the end-user via user interface		
Evaluation Objective	WP2A7 Provide User Interfaces		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	% of available functionalities that are offered via UI
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the fact that the framework offers user interfaces to access all functionalities, and not by directly editing configuration files, running scripts, etc. Measurement can be captured via interview/questionnaire.		

ID	**F- 10**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Usability of the framework user interfaces		
Evaluation Objective	WP2A7 Provide User Interfaces		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the quality of the interfaces offered to the end-user		

ID	**F- 11**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-Functional		
Evaluation Criteria	Ability of the framework to scale to meet high demands and workloads		
Evaluation Objective	WP2A8: Scalability		
Evaluation	TREDISEC framework		

Objects			
Evaluation measurement	Interview/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (administrator)		
Other comments and considerations	For example, this criterion can be refined to specific operations/functionalities of the framework: - CRUD operations on recipes/implementations/patterns - Searches - Deployment of recipes - Testing of recipes Evaluate in terms of (e.g.): - Impact in Latency/Throughput on the event of increasing user requests - Impact in latency/throughput when the number of artefacts (i.e. TREDISEC recipes, security primitive patterns, security primitive implementations) increases		

ID	F- 12	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Ability to enable the interoperability among the different security primitives		
Evaluation Objective	WP2A9: Interoperability		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Premise: there should be some security primitives available that can be deployed together in the same testing environment. This criterion focuses on: - the capability of the framework to facilitate an environment where multiple security primitives can be deployed and tested/validated. - the capability of the framework to support handling recipes that combines two or more security primitives		

ID	F- 13	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Degree of interoperability of the framework with other solutions (e.g. cloud management systems, cloud monitoring tools, automated deployment/delivery solutions, continuous integration/delivery tools)		
Evaluation Objective	WP2A9: Interoperability		

Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Premise: in order to evaluate this item, there should be some external tools/solutions available to integrate/interoperate with. As an example, whether the framework offers or not an API to allow integration with other systems (e.g. security solution repositories, corporate applications)		

ID	**F- 14**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Modular design of the security primitives		
Evaluation Objective	WP2A10: Modular design		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on evaluating the primitives design approach in terms of: - well-defined modular interfaces, - reusable modular components, - making use of industry standards for interfaces, This criterion evaluates the following aspects in the packaging of the primitive: - testing information - deployment information - binaries - Documentation (i.e. specification of the functionalities, architecture, etc.)		

ID	**F- 15**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Compliance with the applicable regulations and policies (at company, country and European level)		
Evaluation Objective	WP2B5: Compliance		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC		

	UC-owner (admin)		
Other comments and considerations	The framework should enable compliance checks by external auditors. For example, by providing user activity logs, installation logs, etc. Also to study the possibility for how the framework complies with the General Data Protection Regulation.		

ID	**F- 16**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The framework should be able to manage multiple requests and overload.		
Evaluation Objective	WP2Q1: System Availability		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the correct setup of the framework. The framework must be a stable application that can handle thousands of requests without having any issues.		

ID	**F- 17**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Increase the system's workload on the current and additional (dynamically added on demand) hardware resources (scale out).		
Evaluation Objective	WP2Q2: Elasticity		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the hardware resources that are going to be used for the efficiency of the framework.		
ID	**F- 18**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The framework should be an end-to-end secure system.		
Evaluation Objective	WP2Q3: Security		
Evaluation	TREDISEC framework		

Objects			
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the confidentiality and integrity of the TREDISEC framework. Measurement can be captured via security experts.		

ID	**F- 19**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The framework should be flexible enough to adapt to the user needs		
Evaluation Objective	WP2Q4: Adaptability		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the way that the framework is developed and how developers can make changes easily according to the users' needs.		

ID	**F- 20**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The framework should not have an overhead that will affect the users' experience.		
Evaluation Objective	WP2Q5: Performance		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Measurement can be captured via profiling.		

ID	**F- 21**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		

Evaluation Criteria	The framework should be usable even for non-experts and security engineers.		
Evaluation Objective	WP2Q6: Usability		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire		

ID	**F- 22**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The system should be easily and rapidly restored following a failure,		
Evaluation Objective	WP2Q7: Maintainability		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on how the framework will be maintained and restored in the case of an emergency.		

ID	**F- 23**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The TREDISEC framework should provide an impact on the commercial relation between consumers of cloud services and providers of cloud services.		
Evaluation Objective	WP2B1: Quality for Business		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner UC-owner (admin, end-user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire targeting consumers and cloud providers.		

ID	F- 24	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The TREDISEC framework should be at a TRL 5/6 when released.		
Evaluation Objective	WP2B2: Market Share		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	This criterion focuses on the readiness of the framework when it gets into production. Measurement can be captured via extensive testing, bug report analysis etc.		

ID	F- 25	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The framework should be flexible enough to support different services and deployment models, but also to adapt to different business exploitation strategies and chargeback models.		
Evaluation Objective	WP2B3: Flexibility		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Measurement can be captured via interview/questionnaire		

ID	F- 26	Use Case	ALL
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	Identify the key actors involved in the business ecosystem of cloud system in which the TREDISEC framework is deployed and observe how all these stakeholders get benefit.		
Evaluation Objective	WP2B4: Stakeholder Satisfaction		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low

Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)
Other comments and considerations	Measurement can be captured via interview/questionnaire

ID	**F- 27**	Use Case	**ALL**
Type	Technology-related		
Focus Area	Non-functional		
Evaluation Criteria	The TREDISEC framework should comply to regulations. This applies to the cloud user and owner of the data and applications hosted in the cloud		
Evaluation Objective	WP2B5: Compliance		
Evaluation Objects	TREDISEC framework		
Evaluation measurement	Interviews/Questionnaire	Evaluation Scale	Scale: H-high, M-medium, L-low
Evaluation Team	Tool-owner: ATOS, GRNET, NEC UC-owner (admin, end-user)		
Other comments and considerations	Measurement can be captured by checking the framework against existing regulations.		

4 Conclusions

We have defined in this document the criteria that the evaluation of the TREDISEC outcomes shall be focused. The evaluation results shall give us an indication whether the requirements have been successfully fulfilled.

The main TREDISEC technological outcomes can be categorized as the TREDISEC Framework and the security primitives. For this evaluation, this document explains the approach to evaluate the effectiveness by instantiating the use cases with appropriate security primitives. Additionally, the evaluation process is described in a way to align with the requirements and assess the degree of fulfillment (according to D2.2) of the TREDISEC technological outcomes.

For this purpose, the two types of domain-specific indicators are defined: a) use case process, which focuses on the process described in the use case, and b) technology-related indicators, which focuses on functional and non-functional characteristics of the technologies.

Finally, we have defined the objectives success criteria, together with the measurement methodologies, for all the use cases and the framework.

This document will be one of the main references for partners running the evaluation of the TREDISEC outcomes, and for project reviewers to focus on which areas all results are evaluated along the processes, and how requirements are fulfilled.

5 References

[1] TREDISEC consortium, “D2.1: DESCRIPTION OF THE CONTEXT SCENARIOS AND USE CASES DEFINITION”, September 2015

[2] TREDISEC consortium, “D2.2 REQUIREMENTs ANALYSIS AND CONSOLIDATION”, February 2016

[3] TREDISEC consortium, “D2.3 TREDISEC ARCHITECTURE AND INITIAL FRAMEWORK DESIGN”, March 2016.

[4] TREDISEC consortium, “Annex 1 – Description Of Action (part B).pdf”, December 2014

[5] HORIZON 2020 – WORK PROGRAMME 2014-2015. General Annexes. G. Technology readiness levels (TRL)

[6] TREDISEC consortium, “D1.5: INNOVATION STRATEGY AND PLAN”, June 2015