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.

<table>
<thead>
<tr>
<th>Project Title</th>
<th>Trust-aware, Reliable and Distributed Information Security in the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Acronym</td>
<td>TREDISEC</td>
</tr>
<tr>
<td>Project No</td>
<td>644412</td>
</tr>
<tr>
<td>Instrument</td>
<td>Research and Innovation Action</td>
</tr>
<tr>
<td>Thematic Priority</td>
<td>Cybersecurity, Trustworthy ICT</td>
</tr>
<tr>
<td>Start Date of Project</td>
<td>01.04.2015</td>
</tr>
<tr>
<td>Duration of Project</td>
<td>36 Months</td>
</tr>
<tr>
<td>Project Website</td>
<td><a href="http://www.tredisec.eu">www.tredisec.eu</a></td>
</tr>
</tbody>
</table>

**<D7.8 - EXPLOITATION REPORT AND LONG TERM SUSTAINABILITY STRATEGY>**

<table>
<thead>
<tr>
<th>Work Package</th>
<th>WP 7, Communication, Dissemination and Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Author (Org)</td>
<td>Ghassan Karame (NEC)</td>
</tr>
<tr>
<td>Contributing Author(s) (Org)</td>
<td>Brigitta Lange (NEC), Alessandro Sforzin (NEC), Miguel Angel Perez (ARSYS), Elena Gonzalez (ATOS), Beatriz Gallego-Nicasio Crespo (ATOS), Jose Crespo (ATOS), Melek Onen (EURC), Andreas Kind (IBM), Pierre Gacon (IDEMIA), Benny Fuhr (SAP), Kari Kostiainen (ETHZ), Aris Sotiroopoulos (GRNET)</td>
</tr>
<tr>
<td>Reviewers</td>
<td>IDEMIA, SAP</td>
</tr>
<tr>
<td>Due Date</td>
<td>M36</td>
</tr>
<tr>
<td>Date</td>
<td>15/03/2018</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Dissemination Level
- PU: Public
- CO: Confidential, only for members of the consortium (including the Commission)
Versioning and contribution history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>10.01.2018</td>
<td>Brigitta Lange (NEC)</td>
<td>Initial draft</td>
</tr>
<tr>
<td>0.2</td>
<td>22.02.2018</td>
<td>Ghassan Karame (NEC)</td>
<td>Revised draft</td>
</tr>
<tr>
<td>0.3</td>
<td>23.02.2018</td>
<td>ALL</td>
<td>Integrated partner inputs</td>
</tr>
<tr>
<td>0.4</td>
<td>28.02.2018</td>
<td>Ghassan Karame (NEC)</td>
<td>Final draft</td>
</tr>
<tr>
<td>0.5</td>
<td>08.03.2018</td>
<td>Ghassan Karame (NEC)</td>
<td>Addressing peer review comments</td>
</tr>
<tr>
<td>0.6</td>
<td>13.03.2018</td>
<td>Ghassan Karame (NEC)</td>
<td>Addressing approval comments</td>
</tr>
<tr>
<td>1.0</td>
<td>14.03.2018</td>
<td>Beatriz Gallego-Nicasio (ATOS)</td>
<td>Final version after Quality Check</td>
</tr>
</tbody>
</table>

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

Executive Summary .................................................................................................................. 8
1 Introduction ............................................................................................................................. 10
   1.1 Purpose and Scope ........................................................................................................... 10
   1.2 Relation with other project work ................................................................................... 10
   1.3 Structure of the document ............................................................................................. 10
2 TREDISEC Exploitation Strategy ......................................................................................... 12
   2.1 TREDISEC Key Exploitable Results ............................................................................. 12
      2.1.1 Innovation Points of TREDISEC ....................................................................... 12
      2.1.2 Exploitable TREDISEC Results ......................................................................... 12
   2.2 TREDISEC IPR Management ....................................................................................... 15
   2.3 Overview of Exploitation Strategy and Methodology .................................................... 16
3 Market Analysis ..................................................................................................................... 19
   3.1 Market Need .................................................................................................................... 19
   3.2 Risks & Barriers ............................................................................................................. 27
      3.2.1 Cloud Encryption Market ................................................................................. 27
      3.2.2 Gap between market and research ...................................................................... 27
4 TREDISEC Business Model and Common Exploitation Strategy ............................................. 28
   4.1 TREDISEC Business Model ......................................................................................... 28
      4.1.1 Customer Segments ......................................................................................... 28
      4.1.2 Sales Channels ..................................................................................................... 28
      4.1.3 Go-to-Market Strategy ...................................................................................... 29
   4.2 Exploitation of the TREDISEC Framework ..................................................................... 29
      4.2.1 Exploitation options ......................................................................................... 31
      4.2.2 Joint exploitation .............................................................................................. 32
   4.3 Exploitation Activities towards Target Groups ............................................................... 33
      4.3.1 Cloud Security Providers .................................................................................... 33
      4.3.2 Cloud Technology Providers, Cloud Integrators, and Cloud Service Providers .... 47
      4.3.3 Vertical Sector Large Enterprises ...................................................................... 56
      4.3.4 Vertical Sector Small and Medium Enterprises ................................................... 64
      4.3.5 Summary ............................................................................................................ 68
   4.4 Collaboration/Exchange with other Projects .................................................................... 69
   4.5 Exploitation through Standardization and Industry Forums ............................................. 69
   4.6 Collaboration/Exchange with Policy Committees ............................................................ 70
5 Individual Partners Exploitation Strategies ......................................................................... 71
   5.1 Exploitation by ARSYS ................................................................................................ 71
      5.1.1 Organization Profile ............................................................................................ 71
      5.1.2 Exploitation Plan and Activities .......................................................................... 71
5.1.3 Actions towards Exploitation ........................................................................ 72
5.2 Exploitation by ATOS ...................................................................................... 72
  5.2.1 Organisation Profile .................................................................................. 72
  5.2.2 Exploitation Plans and Activities ............................................................... 73
  5.2.3 Actions towards Exploitation .................................................................... 74
5.3 Exploitation by ETH ....................................................................................... 75
  5.3.1 Organization Profile .................................................................................. 75
  5.3.2 Exploitation Plans and Activities ............................................................... 75
5.4 Exploitation by EURECOM ............................................................................ 76
  5.4.1 Organization Profile .................................................................................. 76
  5.4.2 Exploitation Plans and Activities ............................................................... 76
  5.4.3 Actions towards Exploitation .................................................................... 76
5.5 Exploitation by GRNET .................................................................................. 77
  5.5.1 Organization Profile .................................................................................. 77
  5.5.2 Exploitation Plans and Activities ............................................................... 77
  5.5.3 Actions towards Exploitation .................................................................... 78
5.6 Exploitation by IBM ....................................................................................... 79
  5.6.1 Organization Profile .................................................................................. 79
  5.6.2 Exploitation Plans and Activities ............................................................... 79
  5.6.3 Actions towards Exploitation .................................................................... 80
5.7 Exploitation by IDEMIA .................................................................................. 81
  5.7.1 Organization Profile .................................................................................. 81
  5.7.2 Exploitation Plans and Activities ............................................................... 83
  5.7.3 Actions towards Exploitation .................................................................... 83
5.8 Exploitation by NEC ....................................................................................... 84
  5.8.1 Organization Profile .................................................................................. 84
  5.8.2 Exploitation Plans and Activities ............................................................... 84
  5.8.3 Actions towards Exploitation .................................................................... 85
5.9 Exploitation by SAP ....................................................................................... 86
  5.9.1 Organization Profile .................................................................................. 86
  5.9.2 Exploitation Plans and Activities ............................................................... 87
  5.9.3 Actions towards Exploitation .................................................................... 88
6 TREDISEC Sustainability Strategy and Long Term Sustainability ...................... 89
  6.1 TREDISEC Sustainability Strategy ................................................................. 89
  6.1.1 Exploitation Board and Contacts ............................................................... 91
  6.2 TREDISEC Long Term Sustainability & Impact ............................................ 92
7 Conclusion ........................................................................................................... 97
8 Bibliography ........................................................................................................ 98
Appendix I  Questionnaire for Validation of TREDISEC results ........................................................... 99
  8.1 Professional Profile...................................................................................................................... 99
  8.2 General/Background.................................................................................................................. 100
  8.3 TREDISEC TECHNOLOGIES: SECURITY PRIMITIVES ...................................................... 101
  8.4 TREDISEC TECHNOLOGIES: FRAMEWORK .......................................................................... 104
  8.5 TREDISEC BUSINESS MODEL ............................................................................................... 108
Appendix II  ARSYS’ Questionnaire for Large Companies ............................................................. 110
Appendix III ARSYS’ Questionnaire for SMEs .............................................................................. 116
Appendix IV Definitions and Main Applications ............................................................................... 118
Appendix V Long Term Commitments by Consortium Members .................................................... 121
  8.5.1 Arsys .................................................................................................................................. 121
  8.5.2 ETH .................................................................................................................................... 121
  8.5.3 EURECOM .......................................................................................................................... 122
  8.5.4 GRNET ............................................................................................................................... 122
  8.5.5 IDEMIA ............................................................................................................................. 122
  8.5.6 SAP .................................................................................................................................... 122
  8.5.7 NEC .................................................................................................................................... 122
  8.5.8 ATOS .................................................................................................................................. 123

List of Tables
Table 1: TRL of TREDISEC primitives and their associated innovation pint .................................... 14
Table 2: Summary of Patents Filed in TREDISEC ........................................................................... 15
Table 3: Expected level of benefit vs. estimated years to mainstream adoption (Source [1]) ............. 20
Table 4: Exploitation paths for the various TREDISEC primitives ................................................ 26
Table 5: Targets and questions that address them ........................................................................... 48
Table 6: Assigned weights for responses .......................................................................................... 48
Table 7: Overview of ARSYS Exploitation Activities ..................................................................... 72
Table 8: Overview of ATOS Exploitation Activities ...................................................................... 75
Table 9: Overview of GRNET Exploitation Activities .................................................................... 78
Table 10: Overview of IBM Exploitation Activities ....................................................................... 81
Table 11: Overview of IDEMIA Exploitation Activities ................................................................ 84
Table 12: Overview of NEC Exploitation Activities ....................................................................... 86

List of Figures
Figure 1: TREDISEC exploitation strategy ...................................................................................... 18
Figure 2: TREDISEC framework services ..................................................................................... 30
Figure 3: Complementary services for TREDISEC framework ..................................................... 33
Figure 4: Background of questionnaire respondents ................................................................       34
Figure 5: Questionnaire respondents’ familiar technologies ......................................................... 35
Figure 6: Questionnaire participants’ customer sectors ................................................................. 35
Figure 7: Q1 - Participants’ usage of three major cloud technologies: storage, computing, and services36
Figure 8: Q2 - Participants’ expertise with major cloud technologies: storage, computing, and services36
Figure 9: Q3 - Participants’ feeling about their cloud outsourced data with respect to some major aspect of security37
Figure 10: Q4 - How useful would be a solution addressing the shortcomings shown in Figure 9?…..37
Figure 11: Q6 - Respondents’ perceived support given by TREDISEC’s primitives with regards to major aspects of security and software………………………………………38
Figure 12: Q7 - Importance of TREDISEC extra features, such as deduplication and multitenancy support………………………………………………………………………39
Figure 13: Q8 - TREDISEC primitives’ likelihood of enhancing technologies…………………………39
Figure 14: Q9 - Frequency of integration of TREDISEC’s primitives with existing technologies…40
Figure 15: Q10 - Availability of common software requirements in current market solutions………..41
Figure 16: Q11 - Likelihood of participants using a framework offering the functionalities listed in Figure 15…………………………………………………………………………42
Figure 17: Q12 - Frequency of framework usage ……………………………………………………………….42
Figure 18: Q13 - Productivity enhancement brought by TREDISEC framework …………………43
Figure 19: Q16 - Preferred channels of communications of participants and their companies …..43
Figure 20: Q17 - Perceived importance of TREDISEC’s testing feature……………………………44
Figure 21: Q18 - Likelihood of preferring TREDISEC over existing solutions ……………………44
Figure 22: Q19 - Open-source vs free solution …………………………………………………………………..45
Figure 23: Q20 - Comparison between offered licensed solutions ……………………………………45
Figure 24: Q21 - Participants’ preferences about additional services to be offered with a licensed solution ……………………………………………………………………………………46
Figure 25: Respondents’ willingness of recommending TREDISEC to their peers…………………47
Figure 26: Respondents willingness of recommending TREDISEC to their managers ………47
Figure 27: Sample size of the focus group ……………………………………………………………………49
Figure 28: Section 1: Profile Background ……………………………………………………………………49
Figure 29: Q1 - Use of Cloud technologies …………………………………………………………………50
Figure 30: Q3 - Perception of the lack of security …………………………………………………………50
Figure 31: Analysis of question 4 ………………………………………………………………………………51
Figure 32: Q6c) - Perceived support given by TREDISEC primitives with regards to different aspects51
Figure 33: Q7 - Importance of support cloud functional characteristics …………………………52
Figure 34: Q8 - Intention to use the TREDISEC primitives……………………………………………52
Figure 35: Q10 - Demand for a solution such as the TREDISEC framework ……………………53
Figure 36: Q11 - Willingness to use the framework …………………………………………………………53
Figure 37: Q14 - Rate the framework features – options with best results ………………54
Figure 38: Q16- Channels ………………………………………………………………………………………54
Figure 39: Q18 – Preference for TREDISEC framework over others ……………………………….55
Figure 40: Q20 – Preference for additional features/services for licensed primitives ………55
Figure 41: Q21 – Framework Complementary Services ………………………………………………56
Figure 42: Question 1 - Analysis …………………………………………………………………………………58
Figure 43: Question 2 - Technology type …………………………………………………………………58
Figure 44: Question 5 - Knowledge of the Cloud …………………………………………………………59
Figure 45: Question 6 - Security concerns ……………………………………………………………………60
Figure 46: Question 8 - Perceived relevance of TREDISEC functionalities ………………60
Figure 47: Question 9 - Potential of improving products ……………………………………………61
Figure 48: Question 10 - Ease to obtain, test, and deploy security solutions and retrieve documentation……………………………………………………………………………62
Figure 49: Question 11 - Evaluation of TREDISEC functionalities……………………………………62
Figure 50 Question 13 - Commercialization of TREDISEC functionalities ………………………..63
Figure 51: Question 15 – Likelihood of adopting TREDISEC framework …………………………63
Figure 52: Question 16 - Willingness of purchasing TREDISEC primitives…………………………64
Figure 53: Question 19 - Promoting TREDISEC among sales agents ……………………………64
Figure 54: Question 2 – Knowledge/Experience in IT ……………………………………………………65
Figure 55 Question 4 - Concerns regarding non-compliance with GDPR ……………………66
Figure 56: Question 7 - Familiarity with secure deletion ………………………………………………66
Figure 57: Question 8 - Interest in secure deletion ………………………………………………………67
Figure 58: Question 10 - Implemented IT security measures …………………………………………67
Figure 59: Question 11 - Deployment of verification mechanisms for storage integrity ………68
Figure 60: Barriers to GDPR Compliance (source: [21]). .................................................. 95
Figure 61: Expected timing to fulfil GDPR (source: [21]). .................................................. 95
Figure 62: Expected cost associated to GDPR compliance (source: [20]). ........................ 95
Executive Summary

This document reports on all plans and activities for the exploitation of TREDISEC results by the consortium partners. It focuses on marketing strategies and business opportunities for the deployment of security solutions developed by TREDISEC.

The main purpose of this document is to inspect the technology put forth by TREDISEC from the point of view of exploitation, particularly in terms of business value. As the report shows, the results of the project offer cutting-edge security solutions which have the potential to greatly improve the European cloud businesses and to generate new ones.

The document summarizes the business plan undertaken by the TREDISEC consortium as well as the research and development activities pursued by the partners towards realizing this plan. It includes the Exploitation Strategy agreed upon the partners, which illustrates the exploitation principles and methodology, IPR management, and key exploitable results; a detailed analysis of the current cloud market and how the key exploitable results of TREDISEC could affect it; the business model developed within the consortium and corresponding exploitation strategy pursued by all the partners jointly; the specific exploitation strategies adopted by the partners individually; and a sustainability strategy to ensure long-term impact of the TREDISEC results.

We conclude that the results achieved by TREDISEC promise to positively contribute the European cloud market, and are capable to boost the large-scale adoption of cloud products and outsourced services, possibly generating new business in the cloud services landscape.
Acronyms

**CA:** Consortium Agreement  
**IPR:** Intellectual Property Rights  
**PEDR:** Plan for the Exploitation and Dissemination of Results  
**WP:** Work-Package
1 Introduction

1.1 Purpose and Scope
This document presents the final consolidated report on all plans and activities for exploitation of TREDISEC results by the consortium partners with focus on commercialization concepts and business opportunities, such as development of new innovative products and services. The purpose of this document is to demonstrate how TREDISEC research and innovation activities will impact the market and contribute to increase economic competitiveness. Besides summarizing the business plan undertaken by TREDISEC, this document outlines the concrete roadmap undertaken by the TREDISEC consortium to exploit the various TREDISEC results. More specifically, besides outlining the final exploitation strategies of all involved stakeholders in TREDISEC, this document provides details on the common exploitation strategy, as well as on all paths identified for practical impact creation and long term sustainability strategy.

This document constitutes the final ‘Plan for the Exploitation and Dissemination of Results’ (PEDR).

1.2 Relation with other project work
This deliverable is part of work-package WP7 (Communication, Dissemination and Exploitation) Task 7.4 - Exploitation and Sustainability Analysis.

By definition and nature of the PEDR, the exploitation plan follows the evolution of the TREDISEC project already from the proposal stage until the final project report, and hence it directly relates to all other TREDISEC project work.

In particular, it closely relates to all work-packages and tasks where the TREDISEC research and innovation activities are carried out and key exploitable results have been developed and created, i.e., the TREDISEC framework implemented in WP6 and its services and components as developed in technical work packages WP3, WP4, WP5 and deployed /evaluated in WP6.

Within WP7, this deliverable builds on the results and recommendations of Task 7.3 and deliverable D7.7 - Business Models for TREDISEC [1], is linked to the communication and dissemination plan activities as implemented in Task 7.2 and set out in detail in deliverables D7.2 - Dissemination Plan [2] and D7.3 – Communication Strategy and Plan [3] as well as in the three Dissemination and Communication Activities Reports: D7.4 [4], D7.5 [5] and D7.6 [6].

In order to demonstrate the exploitation of the various innovations, progress, and impact of the TREDISEC exploitable results, this deliverable also leverages the Innovation Management work carried out in WP1, Task 1.3.

1.3 Structure of the document
The Exploitation Report and Long Term Sustainability Strategy Deliverable D7.8 is structured as follows.

Section 2 introduces the objectives and methodology of the TREDISEC exploitation strategy, presents the TREDISEC key exploitable results, and outlines the protection and management of the Intellectual Property Rights (IPR) as a prerequisite for successful exploitation and sustainability.

Section 3 provides an overview and analysis of the target market and key customer segments for the commercial exploitation of the new and innovative TREDISEC products and solutions, including key drivers of demand, competitors, potential risks, as well as important legal and regulatory market requirements/factors.

Section 4 reports on the common (i.e. consortium level) TREDISEC exploitation plan and activities. It describes the business plan and exploitation of the TREDISEC Framework by leveraging a thorough market analysis and validation of our business model through stakeholder involvement and customer
feedback. It presents a comprehensive analysis and evaluation of user queries conducted by the consortium with all major TREDISEC target user groups. Furthermore, it discusses the consortium’s joint exploitation activities aimed at exchanging domain knowledge with other research projects, and the promotion of TREDISEC results in relevant industry forums and policy making groups.

**Section 5** gives a detailed overview on all individual exploitation plans and activities with practical impact creation carried out by each of the individual TREDISEC project partners and their organizations respectively.

**Section 6** is dedicated to the societal dimension, sustainability and long term impact of the TREDISEC exploitable results. It investigates the sustainability of TREDISEC results beyond the project life-time and explains how TREDISEC solutions will impact security and privacy of the future cloud business, the Digital Single Market, the European citizens, and the society as a whole. Moreover, it proposes concrete measures adopted by the consortium for the practical implementation of the common TREDISEC project results’ exploitation beyond the project life-time.
2 TREDISEC Exploitation Strategy

2.1 TREDISEC Key Exploitable Results

In this section, we start by outlining the main exploitable results that have been output by the TREDISEC project throughout its lifetime. Before doing so, we briefly recall the main innovation points that TREDISEC aims to achieve, adapted from Deliverable D1.7.

2.1.1 Innovation Points of TREDISEC

The following list presents the 7 key innovation points of TREDISEC that we identified:

- **Innovation Point 1 - Deduplication on encrypted, multi-tenant data:** TREDISEC aims to leverage existing and novel cryptographic protocols, as well as system security mechanisms, which offer strong data confidentiality guarantees while permitting data deduplication across multiple tenants.

- **Innovation Point 2 - Mechanisms to check the integrity and availability of multi-tenant data in presence of storage efficiency:** TREDISEC will ensure data availability while data is deduplicated and enable the verification of data integrity and availability in multi-tenant settings.

- **Innovation Point 3 - Secure deletion of multi-tenant data in presence of deduplication:** TREDISEC is developing new security protocols, possibly leveraging trusted execution environments and/or novel cryptographic techniques developed by its partners, to enable secure deletion of one tenant’s data on top of cross-tenant deduplication, i.e., ensuring that a tenant’s deduplicated data is securely deleted without disturbing the data access to other tenants.

- **Innovation Point 4 - Storage efficiency in presence of securely outsourced DBMS data:** TREDISEC is devising novel secure data outsourcing DBMS schemes which, by design, can work atop compressed/deduplicated data.

- **Innovation Point 5 - Secure outsourced analytics/processing in a multi-tenant environment:** TREDISEC is investigating new primitives such as delegated privacy-preserving word search schemes supporting revocation with no significant impact on performance, etc.

- **Innovation Point 6 - Trustworthy, consistent and conflict-free access control for multi-tenancy settings:** TREDISEC will provide the mapping between existing ABAC models to enforceable policies (e.g. XACML-based), enabling the definition of policies that can be verified against conflicts, and that effectively govern access to the growing number of cloud transactions when spanning different “circles of trust”. TREDISEC will also develop a service for the evaluation of these policies against distributed attributes, allowing immediate access to services/resources to tenants that belong to different circles of trust.

- **Innovation Point 7 - Distributed enforcement of access control policies:** TREDISEC leverages a novel set of cryptographic primitives, which ensure that access to data can be efficiently and collaboratively achieved while preventing malicious tenants from combining their credentials and escalating their access rights.

2.1.2 Exploitable TREDISEC Results

The key exploitable results from TREDISEC comprise:

- **The TREDISEC framework:** we designed TREDISEC’s unified framework to allow the efficient integration of the security primitives without causing cloud service providers and end-users to incur in additional processing and storage costs. We emphasize that cloud security
solutions currently on the market do not support TREDISEC’s novel functionalities such as
deduplication and proofs of retrievability.

- **The individual TREDISEC primitives:** We have built the TREDISEC framework’s
architecture to allow for various security primitives developed in the context of the technical
work packages WP3, WP4, and WP5 to be defined as an interface specification and
documentation.

- **The TREDISEC recipes:** We integrate a number of compatible primitives within the
TREDISEC framework in the form of recipes. These recipes form another fundamental key
exploitation result from the TREDISEC project as they offer a unified software package and
the corresponding installation requirements for integrating the entire recipe (or collection of
primitives) within the cloud environment of customers.

As discussed later in the deliverable, the framework will be open-source and readily available to all
organisations willing to integrate it within their business lifecycle. This enables an easy and
transparent way to transfer one of the main innovation aspects derived from the TREDISEC project to
the broader community. The framework will come equipped with an open recipe:

- **Recipe 1 - Container Isolation:** which corresponds to GRNET's primitive for isolating
containers in the cloud. This recipe will be available for public and can be directly accessible
from the TREDISEC framework.

In addition to these recipes, we envision a number of additional closed and proprietary recipes that
are protected within the TREDISEC consortium and will form the basis, along with the individual
associated primitives, of future commercial exploitation of TREDISEC results. These recipes are:

- **Recipe 2 - TRAVIS:** which corresponds to Atos primitive for Remote Attestation of Virtual
Systems (closed recipe).

- **Recipe 3 - EPICA:** which corresponds to Atos primitive for Access Control with Multitenancy
(closed recipe).

- **Recipe 4 – Secure storage and deletion:** this corresponds to the combination of the file-
based deduplication ClearBox primitive by NEC, the secure deletion primitive of ETH, and the
EPICA primitive by ATOS. This recipe forms the basis of the Use case lead by Arsys.

- **Recipe 5 – Secure and efficient storage:** this corresponds to the combination of the block-
based deduplication PerfectDedup primitive by EURECOM, the proof of ownership primitive
by IBM. This recipe forms the basis of the Use case lead by GRNET.

- **Recipe 6 – Secure biometric matching:** this corresponds to the combination of the
verifiable biometric matching primitive by IDEMIA and the biometric feature extraction
primitive by IDEMIA. This recipe forms the basis of the Use case lead by IDEMIA.

- **Recipe 7 – Secure storage with proofs of retrievability:** this corresponds to the combination of the file-based
deduplication ClearBox primitive by NEC, the outsourced proofs of retrievability primitive by NEC, the key-resilient advanced encryption Bastion primitive by
NEC, and the SPORT primitive by NEC that allows deduplication of the POR tags. This recipe
forms the basis of the exploitation envisioned by NEC of the project results.

- **Recipe 8 – Robust cloud platform:** this corresponds to the combination of the container
isolation primitive by GRNET, the software hardening primitive by IBM, the attack surface
reduction primitive by IBM, and the vulnerability discovery primitive by IBM.

- **Recipe 9 – Verifiable computations:** this corresponds to the combination of the verifiable
polynomial evaluation primitive by EURECOM, and the verifiable matrix multiplication
primitive by EURECOM.
The various primitives have been organized in self-sufficient modules providing a rich set of APIs together with their detailed documentation. The reliance on modularity is not by chance: we designed the framework to allow prospective users to select only those components that meet their needs.

In the following Table 1 we list TREDISEC’s primitives, their preparedness for exploitation, and the innovation points that they cover.

<table>
<thead>
<tr>
<th>Primitive Name</th>
<th>Owner</th>
<th>Initial TRL</th>
<th>Final TRL</th>
<th>Innovation Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPM-based Remote Attestation (TRAVIS)</td>
<td>Atos</td>
<td>3</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Access Control for Multi-tenancy (EPICA)</td>
<td>Atos</td>
<td>4</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Logical Partitioning Hypervisor</td>
<td>ETH</td>
<td>4</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Secure Deletion</td>
<td>ETH</td>
<td>4</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Shared Ownership (Commune)</td>
<td>ETH+NEC</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Perfect Dedup</td>
<td>Eurecom</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Verifiable Polynomial Evaluation</td>
<td>Eurecom</td>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Verifiable Matrix Multiplication</td>
<td>Eurecom</td>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>MUSE</td>
<td>Eurecom</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>ML-POR with MLKeygen</td>
<td>Eurecom</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Container Isolation Component</td>
<td>GRNET</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Software Hardening (MEMCAT)</td>
<td>IBM</td>
<td>?</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Attack Surface Reduction (KTRIM)</td>
<td>IBM</td>
<td>?</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Vulnerability Discovery/Fuzz Testing</td>
<td>IBM</td>
<td>?</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>IBM’s PoW</td>
<td>IBM</td>
<td>?</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Key Management for Secure Deduplication (OOPRF)</td>
<td>IBM</td>
<td>?</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Verifiable Matching of Biometric Templates</td>
<td>IDEMIA</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Biometric Features Extraction in the Encrypted Domain</td>
<td>IDEMIA</td>
<td>0</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Verifiable Document Redacting</td>
<td>IDEMIA</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Proofs of Retrievability</td>
<td>NEC</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Advanced Encryption Resilient to Key Leakage (Bastion)</td>
<td>NEC</td>
<td>2</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Secure Deduplication (ClearBox)</td>
<td>NEC</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>SPORT</td>
<td>NEC</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>MIRROR</td>
<td>NEC</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Authenticated Encryption</td>
<td>NEC</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Secure Data Migration Service</td>
<td>SAP</td>
<td>0</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Multi-Tenancy Enable Encrypted Database</td>
<td>SAP</td>
<td>0</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 1: TRL of TREDISEC primitives and their associated innovation pint
2.2 TREDISEC IPR Management

The management of Intellectual Property Rights (IPR) is a fundamental prerequisite for successful exploitation and maximum impact of the innovative solutions and the protection of key results generated within the TREDISEC collaborative research project. As discussed in Deliverable D1.7, the TREDISEC consortium has filed a total of six patent applications to protect the various primitives devised in technical work packages 3, 4, and 5.

<table>
<thead>
<tr>
<th>Patent</th>
<th>Technology</th>
<th>Partner</th>
<th>Work Package</th>
<th>Innovation Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure and efficient cloud storage with retrievability guarantees</td>
<td>Secure deduplication, Key resilient advanced encryption, outsourced proofs of retrievability, deduplicated POR.</td>
<td>NEC</td>
<td>WP3 and WP4</td>
<td>1 and 2</td>
</tr>
<tr>
<td>A COGNITIVE APPROACH TO MEMORY CATEGORIZATION FOR SEPARATING ATTACKER-CONTROLLED DATA</td>
<td>Memory categorization</td>
<td>IBM</td>
<td>WP4</td>
<td>5</td>
</tr>
<tr>
<td>CRYPTOGRAPHIC KEY-GENERATION WITH APPLICATION TO DATA DEDUPLICATION</td>
<td>Key management for secure deduplication</td>
<td>IBM</td>
<td>WP3</td>
<td>1 and 2</td>
</tr>
<tr>
<td>Practical and Secure Substring Search</td>
<td>Secure Migration related encryption scheme</td>
<td>SAP</td>
<td>WP5</td>
<td>4 and 5</td>
</tr>
<tr>
<td>Encrypted Database Joins with Fine Granular Security</td>
<td>Secure Migration related encryption scheme</td>
<td>SAP</td>
<td>WP5</td>
<td>4 and 5</td>
</tr>
<tr>
<td>Optimized Distributed SQL Executions for Encrypted Databases</td>
<td>Secure Migration related encryption scheme</td>
<td>SAP</td>
<td>WP5</td>
<td>4 and 5</td>
</tr>
</tbody>
</table>

Table 2: Summary of Patents Filed in TREDISEC

The TREDISEC project partners therefore established and agreed upon a plan how results arising within the project, which are expected to be capable of commercial or industrial exploitation, will be managed and protected through Intellectual Property Rights. This has been set out in the TREDISEC Consortium Agreement (CA) [7]. In the following, the relevant sections of the TREDISEC CA are summarized, including the provisions related to the management of IPR involving ownership and transfer of results as well as access rights for exploitation:

- **Ownership of Results (Section 8.0 of the CA):**
  - There are rules in place that handle the ownership of results; in short: results are owned by the party (i.e. the TREDISEC beneficiary and TREDISEC CA contractor) that generates them.

- **Joint Ownership of Results (Section 8.1 of the CA):**
In the case of joint ownership of results there are regulations that manage the legal aspects of the exploitation and protection of the IPR.

- **Transfer of Results (Section 8.2 of the CA):**
  - Each party may transfer ownership of its own results to any of its affiliated entities without notification to any other party. In case of such a transfer the rights and obligations of the other parties are regulated within the CA.

- **Access Rights to Results for Exploitation (Section 9.4 of the CA):**
  - Access rights to results for other parties shall be granted on fair and reasonable conditions, if needed for exploitation of a party's own results; there is no such access right without an explicit agreement.
  - Access rights to results for exploitation in research, demonstration, and for non-commercial, educational purposes are granted in accordance with the requirements of the Grant Agreement (GA) [8].

More details about these and other IPR regulations that are not covered in this abstract can be found in the TREDISEC CA.

Under these IPR management regulations, the consortium has produced an impressive set of results which shall be briefly outlined here.

Throughout the project, the TREDISEC partners have identified and managed their intellectual property rights by making use of internal as well as external IPR specialists. The results of these efforts and investments made by the individual project partners into effective exploitation and protection of intellectual property rights becomes visible by the impressive number of patents filed within TREDISEC (see Table 2).

Management of IPR Protection and jointly generated foreground in connection with commercial exploitation of the project results has also been an integral part of the Common Exploitation Booster\(^1\) support service given to the consortium by the market strategy expert and business plan consultant Peter Moran in 2016.

For the practical implementation and management of IPR in the context of the exploitation of common TREDISEC results beyond the project life-time the consortium has agreed to establish and make use of an exploitation board. The composition, objectives and functions of this board are outlined in Section 6.1.1 of this document. For further details on the results of TREDISEC IPR Management see section 4 and section 5.

### 2.3 Overview of Exploitation Strategy and Methodology

TREDISEC promotes a holistic approach to exploitation and recognizes the latter not as an isolated task but rather as an interconnected and collaborative activity constantly reflecting the progress and objectives of all other project activities. Particularly, the exploitation effort has been highly synergized with the projects' dissemination and communication strategies, as well as with the TREDISEC innovation management activities. Based on the key exploitable results and their TRL, the project identified several routes for exploitation, which will be outlined in the remainder of this document. We stress that while TREDISEC solutions offer a solid basis to foster further research projects in the context of cloud security, they are also capable to be integrated into products and services for the current market. Indeed, the exploitation strategy chosen by the project includes (but is not limited to) establishing cooperation agreements, licensing or selling intellectual property rights, and selling cloud products that incorporate the project innovations.

---

\(^1\) Common Exploitation Booster is a common support service which helps former ongoing R&I projects under FP7 and H2020 programs to bridge the gap between creating research outputs and ensuring their exploitation by providing a series of tailored services. More information at [http://exploitation.meta-group.com/Pagine/About-Us.aspx](http://exploitation.meta-group.com/Pagine/About-Us.aspx)
Broadly speaking, the core elements of the TREDISEC Exploitation Strategy are:

- the enforcement of an intellectual property policy to protect the TREDISEC inventions (see Section 2.2);
- a meticulous analysis of the current cloud market in respect of the project innovations (see Section 3);
- the development of appropriate business models to turn these innovations into profitable commercial products (see Section 4.1);
- a collaboration and synergy plan with stakeholders to obtain early and regular feedbacks from potential end-users (see Section 4.3);
- a sustainability roadmap to ensure long-term impact of products and solutions designed within TREDISEC as well as value creation and technology transfer in compliance with the European regulations and long-term agenda (see Section 6).

Following these principles and methodology, the project established a smooth path to include innovative research results into products and services, to feed them into further research or development activities, and to employ them for the creation of new business.

More specifically, based on the key exploitable results and their TRL the project has identified the following categories that suggest the paths for exploitation/utilization of the individual primitives:

- Category 1: Use for further research
- Category 2: Developing and selling own products
- Category 3: Developing and providing services
- Category 4: Cooperation agreement
- Category 5: Selling IP rights/Selling the (IP based business)
- Category 6: Licensing IP-rights (out-licensing)

More specifically, TREDISEC applies the above-mentioned methodology to all individual key exploitable results summarized in Section 2.1, seeking for each of them the best way to bring it to the market (e.g. as standalone product, as a service, or through support activities). Clearly, this requires a proper management of intellectual property rights as a prerequisite, as already explained in detail in Section 2.2, coupled with a thorough analysis of the current cloud security market, a solid understanding of existing cloud security solutions and, more importantly, of their technological limitations.

In fact, a significant component of the TREDISEC Exploitation Strategy consists of a detailed analysis of the cloud market, which is presented in Section 0 and includes the drivers of demand for TREDISEC solutions, pricing models, potential competitors, risk analysis, regulations, and policies. As the market analysis highlights, the rapidly increasing adoption of cloud services on the one hand, and the promotion of added security features for those services on the other hand, are witnesses of an ever growing demand for cloud security. We stress, however, that existing security solutions for the cloud do not support novel TREDISEC functionalities that reconcile the functional requirements such as deduplication with security requirements such as proofs of retrievability. Thus, the technological innovations developed within the projects not only can be safely deployed, but also promise high commercial potential as outlined in the individual exploitation plans and the common TREDISEC exploitation plan.

Following and complementing the analysis of the current cloud market, Section 0 presents suitable business models for all of the exploitable TREDISEC technologies, which illustrate typical applications and use cases and allows for a rigorous approach towards exploitation. Another key element of the exploitation strategy chosen by TREDISEC is the early and continuous involvement of stakeholders and end-users, which gives a mean to account for user requirements throughout the entire technology
design and development process. Specifically, the TREDISEC consortium distributed a series of questionnaires among the top candidate target groups for the developed technology to identify advantages, shortcomings, and ultimately improve products and solutions generated by TREDISEC. The questionnaire results are then directly fed into TREDISEC’s common exploitation strategy to ensure that various TREDISEC recipes and primitives find their way in the market in the coming few years.

On this basis, TREDISEC pursues an attentive and pragmatic exploitation plan sketched in Figure 1, anticipating technical and societal developments of the market as well as legal and regulatory conditions, and also taking into account the necessity for recurrent iterations and potential corrective actions. Having identified the driving forces of the current cloud market, the final step of exploitation is to create the conditions for a profitable deployment of the project’s innovation. Concretely, the exploitation strategy leverages the TREDISEC unified framework to promote the novel functionalities developed within the project, such as deduplication and proofs of retrievability, and corresponding recipes to combine them. The TREDISEC framework, which is specifically designed for the sound and efficient integration of the novel security primitives within existing cloud infrastructures, will be open source and hence available to the broader community. Together with the framework also some of the novel primitives and recipes will be made available. This will foster a large-scale dissemination of the TREDISEC key innovations, revealing security and efficiency advantages over existing solutions. The most appealing TREDISEC primitives and corresponding recipes, however, are proprietary and in fact represent the major asset of exploitation. Thus, the TREDISEC Exploitation Strategy effectively consists in promoting an innovative open-source product while monetizing highly valuable adds-on for it.

Figure 1: TREDISEC exploitation strategy
3 Market Analysis

In D7.7 – Business models for TREDISEC a wide market analysis was developed, encompassing the following items: Cloud Security Service Providers Market Overview, Competitor’s Overview, TREDISEC Framework, TREDISEC Primitives, SWOT.

3.1 Market Need

Security is progressively becoming a priority among enterprises, but no full consensus exists on what form it should take, as a main consequence most product offerings aimed at this market are still in evolution regarding its scope and functionalities.

When planning to make an update of the market research for the current deliverable, it was decided to focus on the most promising cloud security technologies, which reflect the market response to the main challenges of the industry based on these technologies.

According to the Gartner report: Hype Cycle for Cloud Security 2017 [9] there are 30 technologies focused on Cloud Security which are most promising in terms of the added value given to the customers and have been classified regarding the estimated period to mainstream adoption, this means when these technologies will be in regular use.

The technologies that are attracting the highest interest are those associated with control over identity and the tools that can reliably improve the security of cloud-based applications.

The technologies stressed in blue are those ones which have been identified as belonging to the same challenge than TREDISEC primitives.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Years to mainstream adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than 2 years</td>
</tr>
<tr>
<td></td>
<td>Digital Security</td>
</tr>
<tr>
<td>high</td>
<td>Application Security as a Service</td>
</tr>
<tr>
<td></td>
<td>Identity-Proofing Services</td>
</tr>
<tr>
<td></td>
<td>Private Cloud Computing</td>
</tr>
<tr>
<td></td>
<td>Cloud Access Security Brokers</td>
</tr>
<tr>
<td></td>
<td>Cloud Security Assessments</td>
</tr>
<tr>
<td></td>
<td>Cloud Service Brokerage</td>
</tr>
<tr>
<td></td>
<td>Cloud-Testing Tools and Services</td>
</tr>
<tr>
<td></td>
<td>Secure Web Gateways</td>
</tr>
<tr>
<td></td>
<td>Virtual Machine Backup and Recovery</td>
</tr>
<tr>
<td></td>
<td>Cloud Data Backup</td>
</tr>
<tr>
<td></td>
<td>Cloud Data Protection Gateways</td>
</tr>
<tr>
<td>moderate</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Disastre Recovery as a Service (DRaaS)</td>
</tr>
<tr>
<td></td>
<td>High-Assurance Hypervisors</td>
</tr>
<tr>
<td></td>
<td>IaaS Container Encryption</td>
</tr>
<tr>
<td></td>
<td>Tokenization</td>
</tr>
<tr>
<td></td>
<td>Cloud Application Discovery</td>
</tr>
<tr>
<td></td>
<td>Cloud Infrastructure Security Posture Assessment</td>
</tr>
<tr>
<td></td>
<td>Cloud Management Platforms</td>
</tr>
<tr>
<td></td>
<td>Cloud Workload Protection Platforms</td>
</tr>
<tr>
<td></td>
<td>DLP for Mobile Services</td>
</tr>
<tr>
<td></td>
<td>Immutable Infrastructure</td>
</tr>
<tr>
<td></td>
<td>KMaaS</td>
</tr>
<tr>
<td></td>
<td>OpenID Connect</td>
</tr>
<tr>
<td></td>
<td>Software-Defined Perimeter</td>
</tr>
</tbody>
</table>
In the table above, each TREDISEC primitive has been positioned according to the previous table (Table 3) to identify how the results of the project are aligned with the main cloud security technologies of the current market. Please check the appendix for the exact definition of those categories.

It has been found that TREDISEC results could be classified within a wide scope of these emerging technologies, confirming the relevance of the challenges addressed for the research along the 3-years duration of the project.

We can point out the following technologies being the closest to the TREDISEC research primitives:

Cloud Data Backup refers to those tools that can back up and restore production data generated natively in the cloud. Several TREDISEC primitives pursue similar tools, such as ML-POR, ML-Keygen, Proofs of Retrievability, SPORT or MIRROR primitives.

The estimated period to mainstream adoption is still far, between 5 to 10 years.

Cloud Access Security Brokers consolidates multiple types of security policy enforcement. Examples of primitives are EPICA, which provides Attribute-Based Access Control with specific support for multi-tenancy in cloud environments; Bastion, which prevents data breaches even when the adversary has control of the key, or Authenticated Encryption which ensures data confidentiality and integrity.

In this case, the estimated period of adoption is between 2 to 5 years.

Cloud-Testing Tools and Services are aligned with the TREDISEC Framework, focused on the development stage of cloud services, it primarily adds value by allowing architects to not only review, study, and experiment with technologies, but also do MEMCAT or Vulnerability Discovery/Fuzz Testing. The forecasted period for mainstream adoption is between 2 to 5 years.

Cloud Management Platforms enable organizations to manage private, public and multi-cloud services and resources. Perfect Dedup, IBM’s PoW, and the TREDISEC Framework share similar goals. Estimated period for adoption is between 2 to 5 years.

Digital security, understood as the practice of assuring trust, safety and reliability to digital ecosystems, including operational technology (OT), cyber-physical system security (CPSS) and the Internet of Things (IoT) fits also with a high number of primitives: MUSE, Secure Data Migration Service or Multi-tenancy Enable Encrypted Database. The adoption of this technology is still far, from 5 to 10 years, but the expected impact is one of the highest.

Other relevant technologies that fit with TREDISEC challenges research are:

- Private Cloud Computing, that is a form of cloud computing used by only one organization (Logical Partitioning Hypervisor, or Verifiable Matching of Biometric Templates),
- Container Security, the application of security processes, testing and controls to Linux container-based environments (Container Isolation Component),
- Cloud Data Protection Gateways, technology focused on protecting sensitive data stored in SaaS applications (Shared Ownership or MUSE), or...
- *Data Loss Prevention*, a promising market that continues to experience consistent growth, with estimated total gross revenue of approximately 1.000€ in 2017 [1] (*Secure Deletion*).

In general, we can say that TREDISEC addresses the core topics of the cloud security industry, especially some of the most promising and cutting-edge ones with the major expected benefits for the customer’s needs.

Most of the TREDISEC results will be ready to go to market between 2-5 years, period of time which coincides with the technologies on which they are based.

### Primitives vs Market Alignment

<table>
<thead>
<tr>
<th>Primitive/Market Alignment</th>
<th>Expected period for adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TPM-based Remote Attestation (TRAVIS)</strong></td>
<td></td>
</tr>
<tr>
<td>Cloud Workload Protection Platforms (CWPP)</td>
<td>Estimated 4 years</td>
</tr>
<tr>
<td>Cloud Infrastructure Security Posture Assessments</td>
<td></td>
</tr>
<tr>
<td>TRAVIS primitive permits continuous end-to-end verification of the integrity of the virtual infrastructure, as well as the underlying software-hardware stack, where the outsourced business services and applications are running. With TRAVIS, users do not need to fully rely on the provider of the virtual resources to assess integrity properties, but these can be verified by themselves at any point in time. The integrity verification reports generated by TRAVIS on-demand, can be used as an evidence for the internal auditors too, contributing towards standardized and automated ways for Cloud Security Assessments. TRAVIS can also be used by the virtual services provider for continuous monitoring and verification of the integrity of the VMs and the hypervisor, as CWPP solution.</td>
<td></td>
</tr>
</tbody>
</table>

| **Access Control for Multi-tenancy (EPICA)** | |
| Cloud Access Security Brokers (CASB) | Estimated 2 years |
| EPICA is a primitive that provides Attribute-Based Access Control with specific support for multi-tenancy in cloud environments. EPICA implements the complete XACML architecture, and in particular offers a XACML Policy Enforcement Point that can be deployed as an HTTP gateway between cloud users and the cloud provider environment (services and infrastructure), and thus it belongs to the category of CASB. EPICA's XACML Policy Decision Point can be run as a service and is able to handle access to cloud resources based on policies which include context-based constraints and privacy-aware rules. As an example, in TREDISEC UC03, EPICA is controlling access to the multi-tenant cloud storage service of partner ARSYS, which is accessible to cloud users using WebDAV protocol. EPICA’s PEP has been deployed as a gateway in the Apache server of ARSYS, handling WebDAV http requests to access resources with no interference in the cloud storage service or infrastructure. |

| **Logical Partitioning Hypervisor** | |
| Private Cloud Computing, Container Security and High-Assurance Hypervisors, Micro-segmentation | 2-5 years, because the many-core hardware architectures used for logical partitioning are not yet widely deployed. |
| Usage of hardware-assisted Logical Partitioning enabled strong isolation for multi-tenancy, and thus it enables Private Cloud Computing environments for customers with shared resources. Hardware-assisted partitioning can also be seen as a way to enhance the OS-enforced Container Security. Logical Partitioning enables isolated software components, such as VMs, and thus it can also be used to realize High-Assurance Hypervisors with minimal trusted computing base (TCB). |

| **Secure Deletion** | |
| Data Loss Prevention | < 2 years, as Secure Deletion can be deployed as a relatively simple software update. |
| Secure Deletion as a technology can be seen as the inverse of Data Loss Prevention that addresses the risks of accidental or malicious data loss. Secure Deletion provides a closely related but different technology primitive: it allows data owners to have better control over removal and deletion of data. In particular, Secure Deletion ensures that deleted data truly is made inaccessible to the cloud platform provider that previously hosted it. Thus, Secure Deletion complements Data Loss Prevention. Together they provide cloud customers and data |
owners the best control and assurance over their data.

**Shared Ownership (Commune)**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Data Protection Gateways</td>
<td>Shared Ownership can be deployed as a software update, thus its adoption can be in less than 2 years.</td>
</tr>
</tbody>
</table>

Shared Ownership is related to Cloud Data Protection Gateways as both technologies control access to cloud-hosted data and prevent unauthorized access. Cloud Data Protection Gateways, and other similar technologies, typically assume a single entity as the data owner. Shared Ownership technology extends this model to usage scenarios where data records can have multiple owners that jointly define and maintain access control policies.

**Perfect Dedup**

Cloud management platforms  
Estimated 2-5 years

It can be considered related to the Cloud management platforms as it enables to optimize storage savings while keeping data encrypted.

**Verifiable Polynomial Evaluation/ Verifiable Matrix Multiplication**

Cloud infrastructure security posture assessment (CISPA)  
Digital security  
Estimated 2-5 years

It may be considered related to CISPA as the goal is to provide some means to prove the correct execution of the outsourced operations in the cloud. This can also be related to Digital Security, as thanks to these cryptographic primitives, trust towards the cloud services has increased.

**MUSE**

Cloud Data Protection Gateways  
Digital Security  
Estimated 5-10 years

It can be considered as closely related to cloud data protection gateways as the solution does protect the cloud before its outsourcing to the cloud and users can further query this data with the help of the gateway. It can also be related to Digital Security as the main goal is to encrypt customer's data and enable the execution of search even when the data is encrypted.

**ML-POR with MLKeygen**

Cloud Data Backup  
Key management as a service (KMaaS)  
Estimated 5-10 years

It can be considered as closely related to cloud data backup. This service will ensure that backed-up data is stored correctly. It can also be considered related to Digital Security as proofs of retrievability guarantees the correct storage of the data and hence increases trust.

ML-KeyGen can also be considered as key management service especially for secure deduplication applications.

**Container Isolation Component**

Container Security  
IaaS container encryption technology  
Estimated 2 years

The Container Isolation Component is part of the Container Security technology and share very similar goals with the IaaS container encryption technology, since both attempts to enforce encryption to a container's storage. On top of that, the Container Isolation Component implements an on-the-move encryption mechanism that encrypts sensitive parts of a container's image and guarantees that only authorized key-holders may access them. The expected adoption is in less than 2 years since the popularity of container-based clouds is increasing constantly and magnifies the necessity of providing secure means for transferring container images.

**Attack Surface Reduction (KTRIM) and Software Hardening (MEMCAT)**

Cloud Testing Tools and Services  
Estimated 3 years
Attack Surface Reduction includes a wide set of tools that ensures that an attacker has the smallest amount of resources at its disposal to attack a system. The expected adoption is in 3 years.

### Vulnerability Discovery/Fuzz Testing

<table>
<thead>
<tr>
<th>Tool and Services</th>
<th>Estimated Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Testing Tools and Services</td>
<td>4 years</td>
</tr>
</tbody>
</table>

Fuzz Testing behaves like a classic fuzz tester, by supplying mutated input to a program and observing its behaviour. Often, mutated input leads to crashes, and the crashes reveal ways of exploiting the program. Standard fuzzers however do not take into account the distributed nature of some of the software that powers the cloud. The distributed fuzzer will be optimized for distributed programs and components. The output is a series of crash reports including back-traces and the developer/tester can manually intervene to fix the bug and harden the code. The expected adoption is in 4 years.

### IBM’s PoW

<table>
<thead>
<tr>
<th>Platform</th>
<th>Estimated Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss Prevention</td>
<td>3 years</td>
</tr>
</tbody>
</table>

Proof of Ownership refers to a cryptographic protocol that regulates the interactions between a prover and a verifier. The protocol is usually executed in the context of a storage outsourcing scenario, where the prover is the client and the verifier is the (storage) service provider. The correctness property of Proof-of-ownership schemes require that the owner of a file will succeed in convincing the verifier of this fact. The expected adoption is in about 3 years.

### Key Management for Secure Deduplication (OOPRF)

<table>
<thead>
<tr>
<th>Service</th>
<th>Estimated Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Proofing Service</td>
<td>4 years</td>
</tr>
</tbody>
</table>

Key Management for secure deduplication is intended to be used in a scenario where multiple users are using a storage system to store data with these requirements: deduplication is required, the storage system is not fully trusted, users are not expected to share mutual trust, and users want to store data in encrypted form. The expected adoption is in less than 2 years since the popularity of container-based clouds is increasing constantly and this magnifies the necessity of providing secure means for transferring container images.

### Verifiable Matching of Biometric Templates

<table>
<thead>
<tr>
<th>Technology</th>
<th>Estimated Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth 2 Protocol</td>
<td>2 to 5 years</td>
</tr>
</tbody>
</table>

The Verifiable Matching of Biometric Templates primitive is related to both private Cloud Computing and to the OAuth2 protocol. The primitive fits the following use-case: a service provider proposes its users to authenticate using biometric matching. To rationalize the deploying costs, the service provider delegates the biometric matching to a Cloud Authentication Server. Since the storage of biometric data raises legal issues, the help of a private Cloud perfectly fits the use-case. Indeed, biometric templates can be stored as long as the Cloud provides guarantees that no one except the Service Provider and the biometric authentication service can access these sensitive data.

The Verifiable Matching of Biometric templates therefore can enhance the confidence in the work performed by the private Cloud, enabling the Service Provider to efficiently audit the private Cloud.

The expected adoption is 2 to 5 years to align with the rise of OAuth 2, in which the biometric authentication use case could fit.

### Biometric Features Extraction in the Encrypted Domain

- More than 10 years

The biometric feature extraction in the encrypted domain primitive, when mature, could give corporations handling biometric data the possibility to switch from using a private Cloud to a classical Cloud infrastructure. Indeed, for legal reasons, biometric data should be encrypted before being outsourced. Therefore, an actor of the biometric industry would need to outsource his biometric data and to be able to perform computations on
these encrypted values without leaking information to the Cloud owner.

The expected adoption is more than ten years because the primitive relies on fully homomorphic encryption (FHE), which is not a cryptographic primitive mature enough yet. The main bottleneck is efficiency of the actual primitive, which would prevent adoption from the industry. Significant performance improvement in FHE would result in improvement of the primitive and get it closer to practicality. Note that any breakthrough in FHE would decrease the adoption time.

**Verifiable Document Redacting**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Adoption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifiable Document Redacting</td>
<td>2 to 5 years</td>
</tr>
</tbody>
</table>

The Verifiable Document Redacting primitive is related to Identity Proofing Service. This primitive helps a user to hide some parts of an authenticated document while the resulting redacted document can still be authenticated. A user has thus the control over the amount of information disclosed from the original document. The expected benefits of the primitive are high because people are frequently asked to provide documents to justify their source of income or their place of living to get identity documents from the administration. The expected adoption time is 2 to 5 years in order to first let the identity proofing service to be adopted and then to insert inside the service.

**Proofs of Retrievability**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Adoption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Data Backup</td>
<td>Around 2 years</td>
</tr>
</tbody>
</table>

Outsourced proofs of retrievability is related to Cloud Data Backup as it addresses the risks of accidental or malicious data loss in large archival files. This primitive allows the data owner to check seamlessly the availability and integrity of large data chunks stored on the cloud without the active cooperation of the cloud provider. It is secure against a malicious cloud provider that tries to cheat the system.

**Advanced Encryption Resilient to Key Leakage (Bastion)**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>TRL and Integration Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Access Security Brokers</td>
<td>7 and ready for integration as a software package immediately</td>
</tr>
</tbody>
</table>

This primitive is related to Cloud Access Security Brokers as it prevents data breaches even when the adversary has control of the key.

**Secure Deduplication (ClearBox)**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>TRL and Integration Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Data Protection Gateways</td>
<td>6 and ready for integration as a software package immediately</td>
</tr>
</tbody>
</table>

It prevents data breaches and ensures data confidentiality in spite of file-based data deduplication.

**SPORT**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Adoption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Data Backup</td>
<td>Around 2 years</td>
</tr>
</tbody>
</table>

SPORT is a specific instance of proofs of retrievability that allows deduplication of POR tags. As such, it is also related to Cloud Data Backup as it addresses the same risks as the proofs of retrievability of accidental or malicious data loss in large archival files.

**MIRROR**

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Adoption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Data Backup</td>
<td>Around 2 years</td>
</tr>
</tbody>
</table>

The expected adoption is around 2 years, as this primitive can be deployed as a relatively simple software update.
MIRROR is a specific instance of proofs of retrievability that allows to perform a POR on all file replicas present in the cloud. As such, it is also related to Cloud Data Backup as it addresses the same risks as the proofs of retrievability of accidental or malicious data loss in large archival files.

**Authenticated Encryption**

<table>
<thead>
<tr>
<th>Cloud Access Security brokers</th>
<th>The expected adoption is around 2 years, as this primitive can be deployed as a relatively simple software update.</th>
</tr>
</thead>
</table>

Authenticated encryption is a primitive that ensures data confidentiality and integrity.

**Secure Data Migration Service**

<table>
<thead>
<tr>
<th>Digital Security</th>
<th>Estimated 2-3 years</th>
</tr>
</thead>
</table>

A main aspect of Digital Security is the secure storage of data, which comes from a multitude of sources, e.g., corporate transactions or IoT devices. So far, this data was mainly stored on the premises or in unprotected cloud environments. With SAP's already existing protected database concepts, data can be stored and processed in an encrypted form. However, companies have large amount of unprotected legacy data. The Secure Data Migration Service is a convenient way to bring the old unprotected data into an encrypted on-premises or cloud environment. Thus, this primitive is a main business enabler for Digital Security from the end user perspective.

**Multi-Tenancy Enable Encrypted Database**

<table>
<thead>
<tr>
<th>Digital Security</th>
<th>Estimated 2-3 years</th>
</tr>
</thead>
</table>

A main aspect of Digital Security is the secure storage of data, which comes from a multitude of sources, e.g., corporate transactions or IoT devices. So far, this data was mainly stored on premises or in unprotected cloud environments. For a cloud company, such as SAP, multiple users have to be supported in one cloud environment to save costs. The Multi-Tenancy Enabled Encrypted Database primitive allows multiple tenants to access an environment with encrypted databases. Thus, this primitive is a main business enabler for Digital Security from the cloud provider perspective.

**TREDISEC Framework**

<table>
<thead>
<tr>
<th>Framework vs Market Alignment</th>
<th>Expected period for adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Testing Tools and Services</td>
<td>Estimated 2 years</td>
</tr>
<tr>
<td>Cloud Management Platforms</td>
<td></td>
</tr>
</tbody>
</table>

The TREDISEC Framework provides a lean tool that can be incorporated into technologies such as Cloud Testing Tools and Services, and Cloud Management Platforms. The TREDISEC Framework is especially useful at the development stage of cloud services, allowing architects to review, study, and experiment with technologies. Through the Framework, the integration process can be guided to use ready-made recipes and automated testing environments, facilitating easier technology transfer and enabling better consulting and support from the technology providers. The expected adoption is 2 to 5 years because the workflow and user-friendly environment has to mature through actual use and there has to be time for a library of critical solutions.

Based on the aforementioned market research, we recommend the following exploitation paths for the various TREDISEC primitives (Table 4). As mentioned in Section 2.3, recall that the project has identified the following categories for the paths for exploitation/utilization of the individual primitives:

- **Category 1**: Use for further research
- **Category 2**: Developing and selling own products
- Category 3: Developing and providing services
- Category 4: Cooperation agreement
- Category 5: Selling IP rights/Selling the (IP based business)
- Category 6: Licensing IP-rights (out-licensing)

<table>
<thead>
<tr>
<th>Primitive Name</th>
<th>Owner</th>
<th>Final TRL</th>
<th>Recommendation for Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPM-based Remote Attestation (TRAVIS)</td>
<td>Atos</td>
<td>5</td>
<td>Category 2</td>
</tr>
<tr>
<td>Access Control for Multi-tenancy (EPICA)</td>
<td>Atos</td>
<td>6</td>
<td>Categories 2 and 4</td>
</tr>
<tr>
<td>Logical Partitioning Hypervisor</td>
<td>ETH</td>
<td>6</td>
<td>Category 2 and 5</td>
</tr>
<tr>
<td>Secure Deletion</td>
<td>ETH</td>
<td>6</td>
<td>Category 3 and 4</td>
</tr>
<tr>
<td>Shared Ownership (Commune)</td>
<td>ETH+NEC</td>
<td>5</td>
<td>Category 5 and 6</td>
</tr>
<tr>
<td>Perfect Dedup</td>
<td>Eurecom</td>
<td>4</td>
<td>Category 2 and 5</td>
</tr>
<tr>
<td>Verifiable Polynomial Evaluation</td>
<td>Eurecom</td>
<td>3</td>
<td>Category 1</td>
</tr>
<tr>
<td>Verifiable Matrix Multiplication</td>
<td>Eurecom</td>
<td>3</td>
<td>Category 1</td>
</tr>
<tr>
<td>MUSE</td>
<td>Eurecom</td>
<td>3</td>
<td>Category 1</td>
</tr>
<tr>
<td>ML- POR with MLKeygen</td>
<td>Eurecom</td>
<td>3</td>
<td>Category 2 and 5</td>
</tr>
<tr>
<td>Container Isolation Component</td>
<td>GRNET</td>
<td>7</td>
<td>Categories 2 and 3</td>
</tr>
<tr>
<td>Software Hardening (MEMCAT)</td>
<td>IBM</td>
<td>3</td>
<td>Category 1</td>
</tr>
<tr>
<td>Attack Surface Reduction (KTRIM)</td>
<td>IBM</td>
<td>4</td>
<td>Categories 2, 3, 6</td>
</tr>
<tr>
<td>Vulnerability Discovery/Fuzz Testing</td>
<td>IBM</td>
<td>2</td>
<td>Category 1</td>
</tr>
<tr>
<td>IBM’s PoW</td>
<td>IBM</td>
<td>4</td>
<td>Categories 3, 4, 5</td>
</tr>
<tr>
<td>Key Management for Secure Deduplication (OOPRF)</td>
<td>IBM</td>
<td>2</td>
<td>Category 1</td>
</tr>
<tr>
<td>Verifiable Matching of Biometric Templates</td>
<td>IDEMIA</td>
<td>4</td>
<td>Categories 2, 3, 4, 5</td>
</tr>
<tr>
<td>Biometric Features Extraction in the Encrypted Domain</td>
<td>IDEMIA</td>
<td>2</td>
<td>Category 1</td>
</tr>
<tr>
<td>Verifiable Document Redacting</td>
<td>IDEMIA</td>
<td>4</td>
<td>Categories 2, 3, 4, 5</td>
</tr>
<tr>
<td>Proofs of Retrievability</td>
<td>NEC</td>
<td>3</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>Advanced Encryption Resilient to Key Leakage (Bastion)</td>
<td>NEC</td>
<td>7</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>Secure Deduplication (ClearBox)</td>
<td>NEC</td>
<td>6</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>SPORT</td>
<td>NEC</td>
<td>3</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>MIRROR</td>
<td>NEC</td>
<td>3</td>
<td>Categories 1, 3, 5</td>
</tr>
<tr>
<td>Authenticated Encryption</td>
<td>NEC</td>
<td>1</td>
<td>Category 1</td>
</tr>
<tr>
<td>Secure Data Migration Service</td>
<td>SAP</td>
<td>6</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>Multi-Tenancy Enable Encrypted Database</td>
<td>SAP</td>
<td>5</td>
<td>Categories 2, 3, 4, 5, 6</td>
</tr>
</tbody>
</table>

Table 4: Exploitation paths for the various TREDISEC primitives
3.2 Risks & Barriers

3.2.1 Cloud Encryption Market

The main barriers to go-to-market derive from the still remaining perception of security as a non-priority until there is an incident. This perception is changing due to an increased number of cyber-attacks, some of them with a high impact in terms of social and economic costs, as WannaCry or Petya but enterprises still do not allocate enough human resources or budget to security.

Traditional reluctance to adopt cloud environment from industry, specifically those sectors with high security requirements as Health or Financial, or the effort to entry in an already mature market are barriers that should be taken into account:

- Lack of awareness about cloud encryption and performance concerns among potential customers [10].
- Lack of budget for the adoption of the best cloud encryption solutions among potential customers
- Lack of technical expertise among enterprise workforce
- Users constantly worried about the dangers of cloud environment. Concern about the performance of security among enterprises
- Competitive market in constant evolution with dynamic landscape of cyber-threats that could shift towards new competitors, and products. TREDISEC is an unknown new player in a mature market, with well consolidated players in terms of size, branding and expertise to go-to-market.

3.2.2 Gap between market and research

The main risks associated to TREDISEC are common to most R&D Projects:

- Primitives with different levels of maturity. Some primitives need further development before being ready for production environments. The time-to-market could be high.
- R&D projects with research topics similar to TREDISEC that could also be potential competitors.
- IT Department's Resistance to Change (uncertainty about the effort to introduce TREDISEC to existing infrastructures, new costs associated to the solution)
4  TREDISEC Business Model and Common Exploitation Strategy

We start by summarizing the TREDISEC business model, with special emphasis on the Value Proposition, Customer Segments, Sales Channels and the Go-to-Market Strategy.

4.1 TREDISEC Business Model

Our value proposition is to deliver a set of modular end-to-end security primitives covering the entire spectrum of cloud-relevant security requirements, while guaranteeing that functional and non-functional cloud capabilities remain unaffected.

These security primitives are managed and provisioned by means of a unified framework, which ensures that the primitives adhere to certain technical requirements and specifications, and satisfy relevant quality standards.

By using TREDISEC outcomes, we help businesses and organizations to meet customers’ security requirements, as well as their own, and ultimately to comply with EU General Data Protection Regulation, without significant additional computational or storage costs, and with negligible reduction in performance.

4.1.1 Customer Segments

This section identifies the target segments more susceptible to benefit from the added value of TREDISEC, and potentially willing to pay for the offered security solutions.

Two different segments have been identified according to the following criteria:

- Companies with a core business related to Cloud security.
- IT departments of firms that have a demand for Cloud security mechanisms:
  - Cloud Technology Companies are classified into three different target groups:
    - Technology providers: application, component and/or integration developers.
    - Cloud providers: specialized companies of Cloud services.
    - Integrators: integration of products and services into a unique offering for customers.
  - Other Vertical Sectors:
    - Large enterprises. They usually have IT departments that would be our target. We distinguish two sectors within this section: Financial and Energy, due to the frequency of the attacks they suffer, coupled with the severity of impacts from potential breaches in these sectors.
    - Small and Medium Enterprises (SMEs). As they usually do not have their own IT departments, we have considered SMEs as a separate target segment. SMEs are the key customers in our approach, due to their strategic value in the development of European economy. They also have a demand of security services, and do not always have the financial resources and specific knowledge to face them. That is why it is important to develop affordable security mechanisms for this sector.

4.1.2 Sales Channels

Due to its technical nature, TREDISEC products can be quite complex and its advantages may be easily understood by very specialized profiles: security managers, developers, or system administrators.

In these cases, offering our products through internal influencers inside companies is a powerful way to reach the customers through a B2C2B (Business-to-Consumer-to-Business) strategy. We could try
to reach market first through developers, which are the consumers of the framework, to win them over as loyal users and encouraging proponents. In this way, TREDISEC could sell later to the enterprises they work for, eventually closing larger enterprise licence agreements. For instance, we foresee the organization of pilots/trials based on the closed recipes and primitives that have been devised in the TREDISEC projects.

Offering TREDISEC products through an online channel might be helpful when one of these potential customers is looking for information in a search engine or a marketplace because they are developing a new solution. Our products can be made available online, either through the TREDISEC website or through external marketplaces such as Amazon or Azure.

However, in case a company has already developed a product or service, it might take too much time for the product owner to research, find and decide to test or buy TREDISEC outcomes, following the aforementioned channel. We will try to attract these potential customers through field sales force. The main objective of the sales representatives must be reaching the right decision makers among potential customers, schedule meetings, face-to-face or teleconferencing, trying to understand their needs and then clearly identify how TREDISEC can benefit them, proposing specific use cases for them, and presenting ad hoc solutions.

4.1.3 Go-to-Market Strategy

Being a research and innovation action (RIA), TREDISEC will have a component of research-intensive actions forming the basis for PoCs (Proof of Concept) that show the applicability of the approach and allow the further protection of real Cloud environment systems based on real-world use cases. While the result of the project will be around TRL (Technology Readiness Level) 5/6, i.e., technology validated or demonstrated in relevant industrial environments (see Section 2.1.2), prototypes must be further developed in order to become products themselves, or part of existing products (see Table 3).

Certain individual project components, in particular many of the security primitives developed within the project, are expected to be integrated into the existing product lines, such as the SAP HANA Enterprise Cloud product, IBM SmartCloud and Softlayer’s offerings, IDEMIA Biometric System solutions and other industrial partner’s products, which are already in the market.

An essential factor to be considered in this kind of technological projects is the ‘window of opportunity’, that is, the period of time during which certain actions can be taken to accomplish a wished outcome. As mentioned later, we foresee a window of 4 years where these actions must be accomplished. Once this period is over, the ‘window is closed’, the expected outcome is no longer achievable. TREDISEC wants to be the ‘first mover’, and act before this window is closed.

In order to transform the project outcomes into commercial products, we foresee these next phases:

- Phase I: Software, including framework and primitives, finalization and preparation (TRL 6). Assessment of true maturity of results will be supported by the Evaluation Task (Task 6.3).
- Phase II: Preparation of product bundles and distribution channels to track and cover stakeholder demands. This phase will entail following a technology transfer strategy, highly dependent on each individual partner’s resources and processes (see Section 5).

4.2 Exploitation of the TREDISEC Framework

The TREDISEC framework, as designed in the context of WP2, is a piece of software that facilitates the Cloud Security technology providers to manage the entire lifecycle of the TREDISEC primitives and recipes. The framework also supports consumers of such technologies in locating and identifying them in a simple and effective manner, as well as in testing and deploying those in a specific cloud-based environment, in order to fulfil consumers’ own requirements.
The framework implementation, in itself, does not include primitives or recipes, but provides the necessary infrastructure and services to enable the management, access and use of the artefacts (i.e. primitives, recipes) by the different groups of framework users.

The functionalities offered by the framework implemented in the context of WP6 (Task 6.2) can be grouped as depicted in Figure 2.

**Figure 2: TREDISEC framework services**

- **FS1 - Repository of Cloud Security knowledge**: the framework provides support and features for Cloud Security engineers and experts to manage, store and promote their primitives. It supports and assists users in keeping multiple versions of well-structured documentation of the primitives’ design, which can also be tagged to facilitate effective searches. The corresponding access control system lets primitive owners manage permissions such as viewing, editing and downloading for each primitive by other framework users.

- **FS2 - Repository of solutions**: as described in full detail in D2.3 and D2.4, TREDISEC primitives can be managed by the framework with different levels of abstraction: patterns and implementations. While patterns are high level descriptions of a scheme that solves a specific cloud security problem, implementations go a step further in the design of a solution. Implementations are based on a pattern to design a solution, using a specific technology and focusing on a particular use case (e.g. a specific target cloud technology). While primitive patterns are only designs (i.e. documentation), implementations must include a piece of software/hardware realizing the design. The maturity of such implementations may vary, though. A third level of abstraction is the concept of recipe, which facilitates the installation, configuration and use of TREDISEC primitives in a particular cloud-based environment. The framework provides primitives’ owners functionalities for managing, storing and versioning the TREDISEC implementations and recipes, in terms of software and documentation. In addition to the access control system, the framework provides features to promote solutions and facilitate contact between owners and customers towards commercial exploitation.

- **FS3 - Knowledge sharing & tracking use**: the framework facilitates collaborative design, implementation, testing and refinement of Cloud Security solutions using specific features. The TREDISEC primitives and recipes repository possesses versioning features and includes support for managing permissions to access, edit and download the stored information and software. Owners of the primitives and recipes decide who can see what and to what extent other framework users can contribute to enhancing their own primitives. Some examples of the collaborative work are listed next. Patterns can be implemented by other users other than the owner (if allowed), and the owner can keep track of this activity easily through the framework. Implementations can be tested by other users, either using the framework’s testing features or by their own means. The results of these tests can be uploaded to the framework and be used as a benchmark of the primitive. A framework user may decide to download primitives and build a recipe on their own. At the same time, the primitive owners...
keep track of this activity and the resulting recipe can be uploaded to the framework to enlarge the available catalogue of solutions.

- **FS4 - Development & Testing environments:** the framework supports developers of Cloud Security solutions with functionalities and infrastructure to test TREDISEC primitives, without the need to download, install and configure them by their own means. The use of this feature is two-fold: for primitives under development, the testing environment can be used by developers to test interim versions of their software before making it available for the public; for mature primitives, this feature permits other users of the framework (not necessarily owners) to try the solutions in different cloud conditions and perform their own tests, giving them the opportunity of reporting bugs, enhancing existing capabilities (if allowed) or reporting test results that can be uploaded to the framework too.

- **FS5 - Deployment environment:** to facilitate consumers of TREDISEC, primitives and recipes in the process of installation, configuration and setting-up, the framework provides support for automatic deployment of these artefacts in a cloud-based environment. The target environment is either supported by the framework itself (i.e. Virtual Machines created and managed by the framework administrator) or linked to the environment of the user’s choice (e.g. a corporate’s virtual infrastructure). The framework can be instructed by the user to deploy the primitives/recipes in one or more configured target cloud environments in an automatic manner. This feature is available only for those primitives/recipes that are developed and built with this support.

### 4.2.1 Exploitation options

We identify two main groups of direct users of the framework:

- **Providers of Cloud Security:** this group uses the framework to promote their solutions, in the form of primitives and/or recipes. The group is formed by providers of security solutions and services for the cloud.

- **Consumers of Cloud Security:** this group is formed by providers of other Cloud Technologies and Services, who, nevertheless, have a need of enhancing their technologies in order to offer higher security levels to their customers, while maintaining the efficiency and performance at acceptable terms. The job of enhancing cloud technologies with security solutions can be done by these Cloud providers themselves or through a third party, i.e. an Integrator. Therefore, we include integrators too in this group of consumers. The consumers group uses the framework to get access to Cloud Security solutions that meet their requirements. Depending on the applicable licensing model, the consumers will be able to test and deploy the artefact themselves or get in contact with the provider to reach a commercial agreement.

The TREDISEC framework software is released as Open Source and free of charge [1]. There are two feasible ways to exploit the framework: as a publicly accessible online service or as a private service with access controlled by the framework owners.

- **Public online service (Cloud Security App Store).**

A framework instance is hosted in a public Internet domain and operated by an entity. Providers and consumers can access the framework freely and the framework is the platform to facilitate the interaction between them.

Providers of Cloud Security technologies use the framework to advertise their solutions or services to the rest of users. Providers will benefit from corresponding framework services, depending on the maturity of the solutions offered, the type of provider and the characteristics of the community built around the framework. If the framework is primarily market oriented, targeting a community of professionals with an offering of mature and commercial solutions/services, they should focus mainly on framework services FS2 and FS5. However, if the framework is used as a platform to promote
development of cloud security innovations, to collaboratively validate and enhance primitives under development, then FS1, FS3 and FS4 would be the services to look for.

The operator may charge providers, consumers or both with a fee. This fee can be fixed (i.e. subscription, per year/month) or subject to transactions (i.e. if there is a commercial agreement, the operator claims a percentage). The framework operator may also offer additional services such as training, consulting services, installation and maintenance, etc.

The costs of operating the framework as an online public Cloud Security App Store are derived from the following categories: Infrastructure Operation Costs, Help Desk Service Support, Human Resources and Marketing Activities.

- **Private service (Custom Repository of Solutions)**

The TREDISEC framework, as explained above, is a platform that facilitates management and use of the TREDISEC primitives and recipes, but it is not tightly coupled to them. This permits using the framework with other solutions or services besides TREDISEC artefacts.

Taking advantage of this flexibility, an organization may decide to acquire a copy of the framework software and use their own private instance to manage their software developments and products. The owner of the framework does not obtain any direct monetary benefit. On the other hand, the organization will benefit from the functionalities of the framework that facilitate the storage and management of the lifecycle of software under development on a collaborative manner, which correspond to FS1, FS3 and FS4 mainly. Also, the framework can be used to make accessible mature solutions and services within the organization or to externals. For this purpose, in addition to services FS2 and FS5, the organization will benefit from the framework features that permit establishing different access control schemes per tenant and user roles.

Since the TREDISEC framework is released as Open Source Free software, the costs for running a framework instance as a private service would derive from the following categories: hosting and maintenance/uploads. This model also offers the possibility to an external entity (i.e. third party) to operate and maintain the framework as a service for the owner organization.

### 4.2.2 Joint exploitation

For the following 4 years after the project end, GRNET and ATOS, as owners of the IPR of the TREDISEC framework, commit to jointly exploit it in the following terms:

- **TREDISEC framework source code**

The framework source code is going to be released openly and for free. In particular, Apache 2.0\(^2\) license will apply.

The source code will be hosted at ATOS’ GitLab server\(^3\). The code will also be made available through other means, to support further promotion. In particular, the TREDISEC project website will enable a dedicated space for the framework where the link to the source code will be listed. Additionally, a dedicated space at the Innovation Catalogue of Trust in Digital Life community\(^4\) will also include a link to the source code.

All the documentation that describes the source code, how to install, configure and use the TREDISEC framework, which is already compiled in deliverable D6.1, will be updated and made available also through the same means as described in the previous paragraph.

The maintenance of the source code will be done by ATOS and GRNET on a best-effort basis. A primary contact e-mail and a backup will be advertised together with the link to the source code in every promotional site. In addition to that, any bug or request will be handled by using the Track system, also available through the ATOS’ GitLab server.

\(^2\) [https://www.apache.org/licenses/LICENSE-2.0](https://www.apache.org/licenses/LICENSE-2.0)

\(^3\) [https://gitlab.atosresearch.eu/ari/tredisec-framework-public](https://gitlab.atosresearch.eu/ari/tredisec-framework-public)

\(^4\) [https://trustindigitallife.eu/innovation/](https://trustindigitallife.eu/innovation/)
• **TREDISEC framework public online service**

A running instance of the framework will be available to the public at the following URL:

https://tredisec.dev.grnet.gr/

This running instance of the framework service is going to be hosted and maintained by GRNET, on a best-effort basis.

New versions containing updates to the running framework instance, in order to fix bugs reported using the Track system (see previous paragraphs on the maintenance of the source code), will be deployed by GRNET also on a best-effort basis.

• **TREDISEC framework complementary services**

The following diagram (Figure 3) lists the complementary services that will be offered, in addition to the framework software. These services are subject to commercial agreement with ATOS and/or GRNET and will be discussed on a case-by-case basis.

![Figure 3 Complementary services for TREDISEC framework](image)

The framework will count with a dedicated space in the project official website to support promotion, with the link to the source code, to the online framework service instance and with an updated list of complementary services and contact points.

### 4.3 Exploitation Activities towards Target Groups

In what follows, we show that the aforementioned business model (jotted in Section 4.1) is well aligned with the needs of the target exploitation groups. To this end, we provide results on the validation of the aforementioned business model with respect to four main groups that are targeted for exploitation by the TREDISEC framework: cloud security providers, cloud technology providers (and cloud integrators), vertical sector large enterprises, and vertical sector small and medium enterprises.

#### 4.3.1 Cloud Security Providers
4.3.1.1 Methodology

NEC, ATOS, and SAP organized an internal workshop in which a member of the security group held a presentation about TREDISEC, its technologies, and NEC own primitives.

During the workshop, to collect meaningful feedback about the TREDISEC framework, a questionnaire was presented to subjects of the focus group. The questionnaire was structured in four major sections, each comprised of several questions aimed at various aspects of the framework:

- General Background: these are introductory questions whose purpose is to collect information about the participants’ background and experience with cloud technologies.
- TREDISEC Security Primitives: here we ask the participants to express their opinions on the framework’s primitives and to rate them.
- TREDISEC Framework: these questions ask how well the TREDISEC framework is received by the public. Since the participants are coming from a computer science background, these questions are relevant to understand the value of the framework for experts in the field.
- TREDISEC Business Model: these questions ask for opinions on the preferred method of distribution of TREDISEC’s technologies.

We presented the questionnaire to several individuals whose expertise ranged from software developer to manager. The ratio of the participants’ main background is depicted in Figure 4.

![Figure 4: Background of questionnaire respondents](image)

The group of respondent was mostly composed of software architects, which makes the questionnaire’s results particularly useful, as these are the experts intended to identify and evaluate key technologies to be included in a company’s software stack.

We also asked the target group to list their experience with technologies related to the TREDISEC framework.
Figure 5: Questionnaire respondents' familiar technologies

Figure 5 shows that more than half of the participants are familiar with key technologies directly related to TREDISEC, namely Cloud and Cybersecurity.

Finally, we asked the participants about the area of expertise of their usual customers. This question was important to understand what kind of audience the TREDISEC framework may reach. Figure 6 shows their answers. Clearly the majority of potential customers come from the IT sector, which is the perfect target for TREDISEC.

Figure 6: Questionnaire participants' customer sectors

4.3.1.2 Questionnaire Results

In this section we will present the results of the questionnaire by showing relevant statistics extrapolated from the participants’ answers. As we will see, it’s clear that TREDISEC technologies might have a significant impact on active businesses looking for reliable cloud security solutions to deploy in their premises.

Background on Cloud Security Technologies

The following questions, from 1 to 4, ask the participants about their experience with cloud technologies. Question 1 (Figure 7), shows that all participants are accustomed with at least one major cloud technology, while question 2 (Figure 8) ascertains that all of them have at least a basic understanding of said technologies, with the majority of the participants having very good knowledge. This gives us high confidence in the questionnaire’s outcomes.
Figure 7: Q1 - Participants’ usage of three major cloud technologies: storage, computing, and services

Figure 8: Q2 - Participants’ expertise with major cloud technologies: storage, computing, and services

After measuring the participants’ general level of knowledge about cloud security, the questionnaire asks their opinions about the current status of the cloud. In particular, they are asked how safe they feel whenever they upload data to the cloud.
Figure 9 clearly shows that users feel mostly uncomfortable when it comes to the security, integrity, and confidentiality of their data once it is uploaded to the cloud. In particular, all feel that their data is not secure, more than 60% feels that their data integrity may be compromised, and a high 75% thinks that they are uploading their data to the cloud at the expense of confidentiality. One justification for such results is the recent reveal of extensive governments’ surveillance programs, such as PRISM. It is evident that users are becoming increasingly aware of their privacy rights and, as a consequence, more concerned about what cloud providers might do with customers’ data without their knowledge.

Given this, how would users feel if they were provided with a solution that addresses all the above-mentioned issues (i.e., assuring them that outsourcing data to the cloud could be done without compromising security, integrity, and confidentiality)? This is what question 4 asked. The results are illustrated in Figure 10.

Figure 10: Q4 - How useful would be a solution addressing the shortcomings shown in Figure 9?
As you can see, there is an overwhelming positive response to the idea of having such a solution.

**TREDISEC Security Primitives**

As mentioned above, during the workshop held at NEC labs, participants were exposed to TREDISEC’s security primitives. The novel primitives’ functionalities and roles were explained and compared with the current market offers.

The questionnaire then asked the participants’ opinions about the primitives. In particular, we were interested in what the participants thought about the primitives’ potential to solve the important shortcomings of current cloud technologies mentioned in question 3 (see Figure 9).

![Figure 11: Q6 - Respondents’ perceived support given by TREDISEC's primitives with regards to major aspects of security and software](image)

Figure 11 clearly shows that, in all cases, more than 60% of the participants think that TREDISEC’s primitives would be a great help to make them regain their confidence and trust in cloud technologies. Additionally, we asked their opinion about the additional features of TREDISEC that are currently unavailable in the market. These features include deduplication (even over encrypted data), multitenancy support, and high-performance computation. As Figure 12 shows, about 70% of the participants think that these are (extremely) important features to have, while the remaining 30% think that they are a nice addition over current solutions.
We did not limit our inquiring to rating the primitives. We also asked participants if they consider TREDISEC’s primitives capable to enhance the technologies offered by their companies and, if so, how often they would integrate TREDISEC’s primitives within such technologies. Questions 8 and 9 gathered their answers, as shown in Figure 13 and Figure 14 respectively.

Figure 12: Q7 - Importance of TREDISEC extra features, such as deduplication and multitenancy support

Figure 13: Q8 - TREDISEC primitives’ likelihood of enhancing technologies
The outcomes of question 8 and question 9 show similar results, both very encouraging. In all cases, about 80% of the respondents declared that their technologies would certainly benefit from the use of TREDISEC’s primitives. About the same fraction thinks that they would surely integrate the primitives in their own technologies.

This overwhelmingly positive response confirms that the work conducted within TREDISEC is of the utmost quality. Over the course of the project, the ubiquitous goal was to design reliable primitives in a modular fashion that could be easily integrated with both old and new technologies and yet maintain a high level of security. We can conclude from all the responses gathered so far that this goal was definitely reached.

**TREDISEC Framework**

After asking the workshop’s participants about the primitives, we asked their opinions about the framework as a whole.

To set up a base line to assess the TREDISEC framework we investigated how existing solutions fare in terms of functionalities as well as the level of satisfaction for the average user. To this end, we presented the workshop’s attendees a list of key characteristics of the TREDISEC framework and asked them how frequently these characteristics are met in existing solutions. These key points are common requirements of any reliable software layer. Nevertheless, it seems that they are not commonly found, as Figure 15 shows.
The most common answer for all points is “rarely”. When it comes to good software development, efficiency and testing are imperative. Yet, it seems that these targets are not a priority for most of today’s solutions: about 60% of all respondents said that it is rare to find efficient software, or even one offering some form of testing facilities.

Automatic deployment is also very difficult to find, despite being a highly desired functionality. Software tools such as Docker and Vagrant are widespread and help immensely in speeding up the development cycle. Despite this, almost 60% of the participants said that it is difficult to find support for these tools in the current market.

Software security and the possibility of leveraging multiple cloud providers are core features of the TREDISEC framework. Judging from the questionnaire responses, not many providers will be able to compete with our framework: in both cases almost 100% of the answers indicate that these features are not available in existing solutions.

Having established a base line, we further asked the participants if they would be willing to use a software solution able to address the above mentioned shortcomings. Indeed, the TREDISEC framework offers all the key functionalities listed in Figure 15.
Figure 16: Q11 - Likelihood of participants using a framework offering the functionalities listed in Figure 15

As illustrated in Figure 16, about 95% of the respondents are keen on using the TREDISEC framework, with about 80% answering that they will (extremely) likely use it. Moreover, we not only asked about their willingness to use it, we also asked how much they would.

Figure 17: Q12 - Frequency of framework usage

As Figure 17 shows, about 85% of the participants replied that they would regularly use the framework, with 40% declaring that they would use it very often. These positive responses emphasize the desire for functionalities such as those provided by the TREDISEC primitives, and also suggest that the cloud security community is still looking for a single software able to cater to its needs.

To complete the survey about the framework, the questionnaire asked about the benefits that the TREDISEC framework would bring to its users. In particular, we focused on the potential boost in productivity that we believe the framework would bring as a direct, intended by-product of its functionalities. Figure 18 shows that our hunches were correct: 100% of the responded expressed a positive opinion about the improvement and productivity enhancement driven by the use of TREDISEC’s software. In particular, almost 65% of them reported a potential great boost in productivity brought by the framework.
We kept TREDISEC’s business model as the last set of questions, to make the participants familiar with TREDISEC first. We then tried to get the message across that the framework would greatly enhance the participants’ daily usage of cloud security technology, a message that, according to the received answers, went through very well.

To start, the questionnaire asks what the preferred method to contact each person and corresponding company would be. Here we wanted to validate the two channels that we proposed in D7.7, namely online and sales force. From Figure 19 it appears that the online channel is by far the preferred option for individuals, while companies prefer a mix of both. The answers also suggested alternative options, such as industrial security conferences, proposed by participants.

The questionnaire then moved to inquire about what we consider a very useful feature of the framework: the possibility of testing the technology in a cloud-based testing environment before downloading, installing, and integrating it in the target cloud environment. Figure 20: Q17 - Perceived importance of TREDISEC’s testing feature shows the answers, which confirm the importance of providing such a feature: 95% of the participants answered they consider the feature important to have.
A fundamental goal for the success of the framework is convincing its potential users that the TREDISEC framework outperforms its competitors. After holding our workshop, we felt confident that this goal was achieved among the workshop’s participants. Question 18 asked directly whether they would prefer TREDISEC over existing solutions and, as Figure 21 shows, the results are clear: 100% of the respondents answered affirmatively.

The next couple of questions asked for the participants’ preferences about how to obtain access to the TREDISEC’s primitives. In question 19 open-source and free solutions are evaluated (see Figure 22). The results appear evenly distributed, although there seem to be a slight preference over an open-source solution. This outcome may stem from the fact that IT people are the largest sub-group among the questionnaire’s respondents, and their typical preference for open-source technologies is well known.
Question 20 (see Figure 23) shows that licensed solutions would be well received as long as customizing them to the users’ needs is possible or additional services are provided. The possibility of having a freemium version, that is, having a limited period of time during which users can use the framework’s functionalities free of charge, also rated very high in the minds of the participants.

To complement question 20, we proposed a set of different potential services in question 21 and asked the participants to rate them according to their liking. The trend appearing from Figure 24 is that an initial technical support to get started with the framework would be highly appreciated. Indeed, 100% of the participants expressed a strong preference over having both framework and primitives installed and configured almost automatically. Naturally, all participants also expressed their hope for continuous software updates, as it is always expected in such scenarios. Also worthy of note is their request for primitives’ customization. About 75% of them expressed strong interest in having this feature at launch.
4.3.1.3 Conclusions

The questionnaire results clearly show that the TREDISEC framework is well received from the community.

The TREDISEC framework’s primitives offer a plethora of functionalities that are often unavailable in competitor’s solutions and, above all else, are never packaged in a single solution. Moreover, there seems to be a great confidence in the value added by the TREDISEC functionalities, with the large majority of the respondents expressing their willingness to integrate the primitives in their own products.

The framework providing a single solution to the many shortcomings of today’s cloud security offerings seems to come at the right time. The community has been looking for such a solution for a long time, and the responses that we received demonstrate this. The respondents confirm that current market solutions lack key functionalities, and that they would be very satisfied with a solution providing them. Participants also expressed a strong desire in using the framework in their daily routine. All the more reason to speed up the process of introducing TREDISEC’s software in the market.

Concerning the preferred distribution method of the software, there was no unanimous answer. Some users reported preference over an open-source solution, while other reported that they would not mind paying for a license if it came with additional features such as continuous updates, customization, and technical support in installing and configuring the framework. A deeper investigation on this matter seems necessary.

As a testament of the strong positive feedback received, we report here the results of two additional questions that we asked those present at the workshop. Namely, we asked their willingness to recommend TREDISEC to both their peers and their managers. Figure 25 and Figure 26 show their responses: in both cases well more than 50% of the respondents expressed their willingness to promote TREDISEC.
4.3.2 Cloud Technology Providers, Cloud Integrators, and Cloud Service Providers

4.3.2.1 Methodology

To perform the validation of non-security cloud technology providers, a common questionnaire was developed (see 0) to gather feedback from the members of the focus group on selected topics.

As reflected in Table 5, questions were formulated with the objective of analysing the following aspects:

- **Background/Familiarity**: to estimate the knowledge of the user and possibly to weigh the answers
- **Demand**: targeting the demand for the solution to address an identified problem
- **Experience/Engagement**: to evaluate the perceived experience of the solution w.r.t. certain aspects
- **Value**: to evaluate the perceived value of the solution
- **Differentiator Value/Value Add**: to assess, if other solutions exist, the differentiation component
The questionnaire was organized in five sections: Profile background, TREDISEC background, TREDISEC technologies: Security Primitives, TREDISEC Technologies: Framework, and TREDISEC Business Model. The first two sections aimed at positioning the questionnaire respondents and using their profile to weigh their answers to questions in the rest of the sections. Sections devoted to TREDISEC technologies aimed at evaluating the demand and perceived added value of the primitives and the framework. A complete section is devoted to validate our proposed business model, its appropriateness and alignment to real demands from target groups of end-users.

Taking into account the different backgrounds, weights (see Table 6) were applied giving more importance to the responses of the Software developers and Software architects in the technical questionnaire and more to the IT Consultants with a business and management expertise in the Business Model Section. A second weight was applied for those who had good experience and knowledge in cloud technologies (+0,25).

In the case of concurrence between weights, the second weight was applied.

In a final phase, when the questionnaires were fulfilled, a statistical analysis was performed using frequency, arithmetic mean, mode and median.

There were different approaches implemented by partners in order to present the project, the results and the business model, previous to the distribution of questionnaires.

From the ATOS side, a webinar was developed, where the different features of TREDISEC, its framework and primitives and the business model were explained in detail to the focus group. During the webinar, three members of the TREDISEC project team delivered presentations and technical documentation and support material was distributed to the participants. Additionally, a demonstration was performed, showcasing all the features of the TREDISEC framework, including creation, management, testing and deployment of primitives. The webinar was recorded and made available to the audience offline, as well as all the supporting material and documentation. Credentials to test the framework were provided for those that requested them, in order to get a more subjective and reliable feedback on the technical results of the project. The audience had one week to fill in the questionnaire, after the webinar was conducted.
SAP created a presentation targeting integrators and highlighted the overall goal of the project and the benefits of the security primitives provided by the project. The focus group was physically present during the presentations. Later on, questionnaires were provided and answered during and after the presentation.

In the case of GRNET, the core TREDISEC team did briefings to multiple groups, taking place during the whole project duration. At the end of each presentation, the collaborators were informed that in future they will be asked to fill-in a survey. As a final validation step, questionnaires were fulfilled by the collaborators in a digital format through Google forms.

Figure 27: Sample size of the focus group

Figure 27 shows that the final sample size for this focus group was made up of 19 people with different professional backgrounds: 10 Software architect and analysts, 6 IT Consultants and 3 Software developers.

4.3.2.2 Questionnaire Results

Profile Background

In this first section, we performed a background analysis of the sample, concluding that the heterogeneity achieved is positive for the validation due to the fact that a wide range of answers were collected.

Graph B in Figure 28 shows that 79.95% of the sample uses cloud technologies the most as well as Identity and Privacy (52.63%). The sample's clients are distributed in multiple sectors, highlighting their presence in the IT sector and the Public Sector.

TREDISEC Background

In Q1 and Q2, the average of cloud technologies usage and knowledge was calculated. As the Q1 graphs points out (Figure 29), a majority of the sample use “often” or “very often” cloud technologies, especially cloud storage.
In Q2, the results show that a majority of the sample is an experienced-power user of cloud storage (66.67%), cloud computing (60%) and cloud services (60%).

Attending Q3 responses we can conclude that there is a perception of a crucial lack of security and control when using cloud technologies.
Figure 31: Analysis of question 4

Figure 31 shows that in Q4 responses, 40% of the sample found it very useful to have solutions for the problems outlined in Q3, and 60% would find it extremely useful.

**TREDISEC Technologies: Security Primitives**

Q6 is organized in three different sections. Section C asks about a rating taking into account 5 different features: Making feel more in control of data, Making less worried about security of the data, Making feel the services/apps running in the cloud are protected against security threats, Making feel the data and services/applications are secure without significant impact on performance and usability.

From this section we can conclude that the primitives developed will solve the problems outlined by the sample, due to the fact that a majority of the sample answered “good” or “excellent” in the rating of the technologies in respect to different features, as we can see in the chart below (Figure 32).

![Figure 32: Q6c) - Perceived support given by TREDISEC primitives with regards to different aspects](image)

In Q7 there is an 80% of the sample that finds TREDISEC primitives, providing support for security and cloud functional/non-functional characteristics, “very important” or “extremely important” for the technologies that they produce (see Figure 33). The average in this question is 4.2, ranging from 1 (“don’t care”) to 5 (“extremely important”).
Analysing Q8, we can say that the four primitives presented would have a good reception among the target market in terms of enhancing the technologies that they produce. In particular, regarding Availability & Integrity with Cloud Efficiency, more than a 60% of the sample answered “likely” and “extremely likely”. The other three primitive categories were rated similarly and none of them in a negative way, as it is shown in the graph of Figure 34.

In Q9, the potential frequency of use of the TREDISEC primitives is analysed. Once again, Availability & Integrity with Cloud Efficiency got the best performance with more than 60% of the sample that will use it in the majority of the technologies they produce.

TREDISEC Technologies: Framework

Figure 35 shows a high percentage of the sample has difficulties to find security solutions that also meet cloud requirements (64%). From a business-strategy point of view this is a very positive output for TREDISEC in terms of market competition. There is also a 50% of the sample that “rarely” has access to information on how the different solutions perform in multiple cloud-based environments.
Q11 asks about the willingness of the sample to use the framework. Notable among the statistical results of this question is the average, standing at 4.21, ranging from 1 ("not at all") to 5 ("extremely likely"). Figure 36 shows the results.

Q12 shows the TREDISEC framework usage intent. There is a 78.57% that presented the two highest values of usage (4 and 5), and among those a 45.45% answered that they will use it several times a month. Further, a 78.57% of the responders thinks that the TREDISEC framework would enhance their productivity in a greatly way (Q13).

Q14 asks about the best rated Framework features. The following bar chart shows the most representative features of the framework in terms of quality of the answers and rating (Figure 37).
As shown, the Repository of Cloud Security Solutions and the Support for Searching Cloud Security Solutions are rated as “extremely useful” features by more than 60% of the sample. Support for Testing the Solutions and the Information Provided When Using and Managing the TREDISEC Primitives are also rated as “useful” and “very useful” by the majority of the sample.

**TREDISEC Business Model**

Q16 aimed at validating the two channels proposed in D7.7 to approach our target market: online and sales force. As the bar chart illustrates in Figure 38, the best way to approach individuals is through the Online channel, while companies could be approached through both of them. Some of the respondents proposed other channels such as Industrial Security Conferences to approach companies.

In Q17 we see how important the testing and deploying features of the framework for the respondents are: 55.56% of them rated it as “extremely important”.

Q18 challenges the respondents to indicate whether they would prefer the TREDISEC framework over other comparable solutions in the market. As shown in the chart below (Figure 39), 22.22% of the sample is “extremely likely” to use TREDISEC framework over other solutions and 50% is “likely” to use it.
Q19 and Q20 aimed at assessing the preference of the audience for TREDISEC primitives over competitors with regards to different access modes and licensing options. It can be seen in Q19 that the sample is not clear about the best offer (Open source or Free). Q20 shows that the sample will be more likely to purchase if the licensed primitives are offered together with complementary services, or if the licensed primitives are customized to their own needs. The chart below (Figure 40) shows different answers.

The bar chart below (Figure 41) illustrates the importance that the respondents have given to the complementary services of TREDISEC technologies. It can be seen that all the services should be welcomed in the market and will satisfy real needs of the target market. The best rated services are Consulting and Maintenance.
4.3.2.3 Conclusion

The primary objective of this validation questionnaire were assessing the gain creators and pain relievers of customer target groups as well as getting feedback on value propositions.

There is a clear demand for the TREDISEC technologies to address concerns related to lack of security and control when using cloud services and technologies. Both the framework and the primitives are perceived as solutions for the problems indicated.

One of the most valued features of the framework is the centralized repository of cloud security solutions which provides searching capabilities and detailed information on the primitives in it. The support for testing the offered primitives is also perceived as useful by the majority of the sample, with special interest in having access to information about the primitive’s performance. The most valued group of primitives is the one falling in the category Availability and Integrity with Cloud efficiency, followed by the other categories which are rated similarly among them. The ratings highlights very promising results about the intention of using these primitives integrated in cloud-based developments.

The proposed critical differentiation component of the framework with regards to other existing repositories of security solutions is its testing and deployment capabilities. This premise has been supported by over 55% of the sample considering it as “extremely important” and 77% stating that they would prefer the TREDISEC framework over other options. Based on the feedback received, the framework could be even more attractive for this focus group if offered together with complementary services such as maintenance and consultancy.

The sample does not permit drawing conclusions on whether releasing the TREDISEC primitives with permissive licenses (open source) or free will make them more attractive over other existing options. Nevertheless, it is clear that offering licensed primitive through flexible commercial agreements (freemium, trials, etc.) and with additional services to maintain and customize them will surely be welcomed by the market.

4.3.3 Vertical Sector Large Enterprises
ARSYS carried out an online survey that was distributed among sales agents specialized in Large Companies. Together with the questionnaire, the document 'Catalogue of Security Primitives' was shared with them, which they used as a reference to answer specific questions about the TREDISEC primitives.

The survey was active during January and 7 complete questionnaires were obtained in total. As mentioned in the previous paragraph, the target audience of the survey was the vertical sector of Large Enterprises. Salespeople who participated in the survey represent all the technological areas in which our Professional customers work. Data and main conclusions of the questionnaires are presented below.

The first five questions were focused on the customer's profile. For brevity of presentation, we only focus on discussing the most relevant questions for this target group (see Figure 42, Figure 43 and Figure 44). The vast majority of sales agents indicated that their clients work in technical positions, such as software developer, software architect or testing/deployment engineer. They also indicated that their customers work in technologies related to the Cloud specifically more than 85%, and that more than 40% of them deals with Data Intelligence. According to the results, our customers work mainly in Finance, IT and Industry sectors, followed by Public Administration, Media and Transportation sectors. Regarding how often they use the Cloud, more than 57% said that their customers normally use Cloud services, standing out from Cloud storage or computing. As for their knowledge on the Cloud, the answers are concentrated in Advanced/Average users.
1) How would you describe your customers’ profile?

![Bar chart showing percentages of customer profiles: 57.14% Project Manager, 28.57% Software architect, 14.29% Testing/Deployment Engineer, 42.86% Software developer, 0.00% Work in Sales or Marketing.]

Figure 42: Question 1 - Analysis

2) Which technologies do they usually work in?

![Bar chart showing percentages of technology types: 85.71% Cloud, 42.86% Data Intelligence, 14.29% Cybersecurity, 14.29% Internet of Things (IoT).]

Figure 43: Question 2 - Technology type
The next set of questions (Figure 45, Figure 46 and Figure 47) draws the attention to customers’ concerns regarding data stored on the Cloud and to the advantages offered by the TREDISEC primitives. The vast majority indicated that their main concerns are integrity and confidentiality. The answers to the following question about the knowledge of TREDISEC primitives indicate that only half of the respondents have heard about these IT security solutions. Sales agents stated that more than 66% of their customers would value features such as deduplication, multi-tenancy and high-performance computing as extremely “important” or “important”. In fact, the same percentage indicates that TREDISEC primitives could contribute to the improvement of their customers’ products, particularly in terms of Confidentiality and Data Processing as well as Availability and Integrity with Cloud Efficiency.
6) While using the Cloud, your customers...

- Always: 83.33%
- Often: 83.33%
- Sometimes: 100.00%
- Rarely: 83.33%
- Never: 16.67%

- Do they feel they have control over data stored on the Cloud? 16.67%
- Are they concerned about the security of data stored on the Cloud? 0.00%
- Are they concerned about the integrity of data stored on the Cloud? 0.00%
- Are they concerned about the confidentiality of data stored on the Cloud? 0.00%
- Do they feel that services/applications running on the Cloud are protected against security threats? 0.00%

Figure 45: Question 6 - Security concerns

8) TREDISEC primitives differ from other security solutions by offering features such as deduplication, multi-tenancy and high-performance computing. How important are these functionalities for your customers?

- Extremely important: 50.00%
- Important: 33.33%
- Somehow important: 16.67%

Figure 46: Question 8 - Perceived relevance of TREDISEC functionalities
9) Do you think that TREDISEC primitives could contribute to the improvement of your customers' products?

![Figure 47: Question 9 - Potential of improving products](image)

The following five questions (Figure 48, Figure 49 and Figure 50) delved into the ease of customers to find security solutions, the functionalities of TREDISEC framework, potential sales channels, and the possibility of testing and deploying those solutions in a cloud-based testing environment. Most respondents stated that they rarely or never have access to information about how those solutions work in multi-cloud environments, they usually do not have the opportunity to test solutions on their own platform on the Cloud, and they seldom have the option to (almost) automatically deploy those solutions through scripts, Docker or Vagrant. Among all the features offered by the framework, which largely solve the issues listed previously, the most valued were the Support to look for security solutions on the Cloud and the Support to deploy security solutions in a virtual environment provided through the framework. Regarding the sales channel for the commercialization of TREDISEC, the majority of sales agents indicated that the most suitable are Visits of specialized salespeople and Marketplaces such as Amazon, Azure, Google, FIWARE, etc. Most respondents indicated that the functionality of testing and deploying those solutions in a cloud-based testing environment is "extremely important" or "important" for their customers.
10) Please answer the following questions from your customers’ standpoint.

![Bar chart showing responses to various questions regarding ease of obtaining, testing, deploying security solutions, and retrieving documentation.]

Figure 48: Question 10 - Ease to obtain, test, and deploy security solutions and retrieve documentation

11) TREDISEC is a framework that solves the issues listed in question no. 10. How would your customers evaluate the following framework functionalities?

![Bar chart showing customers' evaluation of TREDISEC functionalities.]

Figure 49: Question 11 - Evaluation of TREDISEC functionalities
13) According to your customers’ profile, which sales channel do you consider most suitable for the commercialization of TREDISEC?

The previous set of questions was focused on the likelihood of using the framework, the willingness of purchasing the primitives, the evaluation of the complementary services, and whether respondents would recommend TREDISEC to other people. After analysing customers’ concerns and presenting the advantages of TREDISEC, more than 83% of the sales agents indicated that “very likely” or “likely” their customers would prefer the TREDISEC framework over other repositories (Figure 51). As for TREDISEC primitives, a large majority of customers would be willing to pay for them if they could be customized according to their own needs, for example, specific Cloud configurations or special features (Figure 52). Customers also valued very highly complementary services such as training, installation/configuration, updates/maintenance, etc. In fact, in the following question most of the respondents confirmed their interest in the installation and configuration of security primitives, the customization of solutions, and the consultancy for new security solutions. Finally, sales agents confirmed that they would recommend TREDISEC to other salespeople as well as to their line managers (Figure 53).

15) How likely is it that your customers would prefer the TREDISEC framework over other repositories or marketplaces?

Figure 50 Question 13 - Commercialization of TREDISEC functionalities

Figure 51: Question 15 – Likelihood of adopting TREDISEC framework
4.3.4 **Vertical Sector Small and Medium Enterprises**

ARSYS conducted an online survey that was published on the [company's blog](https://www.facebook.com/arsys.es/posts/10156032139931575). Likewise, the Marketing and PR department promoted the survey through the following social networks:

- Facebook: [https://www.facebook.com/arsys.es/posts/10156032139931575](https://www.facebook.com/arsys.es/posts/10156032139931575)
- Google+: [https://plus.google.com/b/112991458221364962317/+arsys/posts/5YbWoa9Any6](https://plus.google.com/b/112991458221364962317/+arsys/posts/5YbWoa9Any6)
The survey was active during January and 46 complete questionnaires were collected in total. The target audience of the survey was the vertical sector of Small and Medium Enterprises. Data and main conclusions of the questionnaires are presented below.

Of the 46 questionnaires, more than 60% responded that they work in small or medium companies, are self-employed or work for the Public Administration. The vast majority, more than 80%, indicated that they have knowledge and experience in the IT sector. In fact, almost 35% responded that they are IT technicians: developers, system administrators, network administrators, etc. (Figure 54).

2) What is your knowledge/experience in Information Technology?

![Figure 54: Question 2 – Knowledge/Experience in IT](image)

Regarding the European GDPR (General Data Protection Regulation), more than 65% have heard about this new regulation, however, almost 70% do not know how it affects them. In fact, around 60% expressed an average or high concern regarding the preparation of their organization to comply with the GDPR. A large majority were interested in a webinar on GDPR (Figure 55).
The following questions were focused on the TREDISEC project and some of its primitives (Figure 56 and Figure 57). Most people who answered the questionnaire did not know anything about the project. Regarding the secure deletion, more than 78% indicated that they did know what it is, but more than half of them do not know whether their organization would be interested in implementing this measure (however, more than 32% answered affirmatively). Regarding the possibility of improving the confidentiality of their files by combining encryption and compression, almost 60% responded that this is the responsibility of the IT department, while more than 30% indicated that they could reduce the storage space without sacrificing the privacy of information.

7) Do you know what secure deletion is?

The following questions were focused on the TREDISEC project and some of its primitives (Figure 56 and Figure 57). Most people who answered the questionnaire did not know anything about the project. Regarding the secure deletion, more than 78% indicated that they did know what it is, but more than half of them do not know whether their organization would be interested in implementing this measure (however, more than 32% answered affirmatively). Regarding the possibility of improving the confidentiality of their files by combining encryption and compression, almost 60% responded that this is the responsibility of the IT department, while more than 30% indicated that they could reduce the storage space without sacrificing the privacy of information.
8) Is your organisation interested in the secure deletion?

![Pie chart showing interest in secure deletion]

Figure 57: Question 8 - Interest in secure deletion

Last questions were related to the IT security measures which are or could be implemented in the respondents’ organizations (Figure 58 and Figure 59). It is worth noting that secure deletion of content and management systems for mobile devices (laptops, smartphones, tablets, etc.) are the least implemented measures, with just over 20%. With respect to storage on the cloud, almost 95% indicated that they are not aware of, or have not implemented, any software to guarantee that the recovered data has not been corrupted in the download process. Regarding the possibility of adding different levels of granularity to permissions and user groups for data stored on the Cloud, more than 35% said that it may be interesting.

10) Please indicate below the IT security measures which are implemented in your organisation.

![Bar chart showing implemented IT security measures]

Figure 58: Question 10 - Implemented IT security measures
Figure 59: Question 11 - Deployment of verification mechanisms for storage integrity

When asked about how those solutions were implemented, more than 20% indicated that IT technicians followed recommendations from specialized forums or that the IT Security department implemented solutions from a marketplace (Amazon, Azure, Google, FIWARE, etc.). Around 24% implemented standard solutions. Regarding the contracting, almost 92% indicated their preference for half-yearly or annual payment (29.73%) or pay-per-use (62.16%). Finally, among the people who knew whether their company uses proprietary or open-source solutions, more than 24% indicated that they use both of them.

4.3.5 Summary

The purpose of all exploitation activities conducted during the lifetime of the project was primarily to estimate whether and to which extent the technology created within TREDISEC could satisfy the needs of the current cloud market. To this end, target groups comprising a variegated set of IT experts (all familiar with cloud technologies and products) were informed about the solutions provided by TREDISEC through workshops, webinar, and presentations, and subsequently asked to give their feedback by answering dedicated questionnaires.

Although the questionnaires were distributed among diverse target groups, including software engineers working for small and medium companies as well as sales agents specialized in large companies, the responses show consensus on multiple aspects. First off, concerns about the security of data stored in the cloud (particularly in terms of confidentiality and integrity) are ubiquitous, the general perception being that all currently deployed cloud products lack security to some extent. Not surprisingly, most respondents agree about the usefulness of adopting solutions that overcome the perceived security issues, which evidently are a very rare species in the current cloud market. When presented with the solutions offered by TREDISEC, again a vast majority of the respondents declared that functionalities such as deduplication and support for multi-tenancy are highly desirable. The questionnaire’s outcomes also show that the currently available cloud technology is lacking not only the functionality and security features provided by the TREDISEC primitives but, and more importantly, also a unified framework that allows for easy integration of those features. As it is clear from the participants’ answers, indeed, it is very hard to find all those security properties within a single piece of software.

The highly positive feedback suggests that TREDISEC technology is likely to be largely adopted by the current ICT cloud market. The responses also give a clear indication that the TREDISEC solutions would be preferred over existing ones, and that customers would be willing of purchasing the licensed
primitives, provided that complementary services such as training, installation/configuration, and maintenance, as well as customization of primitives are additionally provided.

All in all, the gathered feedbacks about the TREDISEC solutions provide even more confidence about the potential of these novel technologies, confirming their business value and impact on the cloud market, mostly on those target categories that are essential for TREDISEC common exploitation: cloud security providers, cloud technology providers, large enterprises, and SMEs.

4.4 Collaboration/Exchange with other Projects

Collaboration and exchange between other European projects also help the TREDISEC project identify and approach potential stakeholders more easily. In particular, TREDISEC had close collaboration with the EU H2020 WITDOM project for which ATOS participated to the validation of their framework architecture and EURECOM joined the three advisory board meetings these last three years. Similarly, EURECOM was also a member of the User Advisory Board for the EU H2020 CREDENTIAL project whereby the CREDENTIAL applications cases were presented. Furthermore, TREDISEC members such as ATOS were actively involved in several cloud-related events and in particular, the DPSP cluster events, during which collaborative industrial exhibitions or workshops were organized with other EU projects. These, helped reach potential customers and increase the market potential for TREDISEC members’ in the (secure) cloud computing domain.

For more details on collaboration activities with other projects, we refer the reader to Deliverable 7.6 [6].

4.5 Exploitation through Standardization and Industry Forums

As mentioned in the original TREDISEC proposal, one of the main exploitation of TREDISEC results will be channeled through industry forums, namely through the Trust in Digital Life consortium.

Founded in 2009 as a consortium, Trust in Digital Life (TDL) is a research community committed to pursue joint research and cross-sector development for the establishment of trustworthy digital services and platforms across Europe. In 2014, TDL became a non-profit legal association registered in Belgium. TDL is a community of large corporates, SMEs, and knowledge institutes. Its objective is to provide tools as well as awareness to improve individuals in their daily digital lives based on the unifying principle that trust and trustworthy services are essential for the success of the digital economy.

TDL’s mission is to enable a trustworthy ecosystem that not only protects the rights of citizens but also creates opportunities for businesses to develop novel and secure devices, applications, and services, and to supply them at a convenient price.

The main activities of TDL to achieve such a trusted ecosystem are:

1. Focus on key research areas, such as blockchain, personal data, and Internet-connected devices that are relevant for establishing trustworthy services, with the goal of providing guidelines and recommendations in these areas.
2. Promote innovation by enabling fast and targeted integration projects called Sprints to validate available technology; Sprints have been opened to non-members since 2018.
3. Make results publicly available via white papers, case studies, and validated software, such as the results of EU framework projects to be accessed or downloaded from our web site.
4. Engage experts in multi-disciplinary events to consolidate research and innovation and disseminate this knowledge among stakeholders.

TREDISEC will leverage services from TDL to ensure that TREDISEC results are made accessible beyond the lifetime of the project. It is the intention of TREDISEC to ensure that the results “do not disappear” once the project has ended. As already explained in section 4.2.2, the idea is for TDL to host a pointer of the Atos Gitlab server (See: https://trustindigitallife.eu/innovation/). TDL will store this
pointer indefinitely which allows to disseminate the TREDISEC framework effectively amongst all TDL partners and website visitors. TDL may support PR activities to further promote possible exploitation activities of the TREDISEC framework.

4.6 Collaboration/Exchange with Policy Committees

On 5 July 2016 the European Commission announced the launch of a contractual Public-Private Partnership on cybersecurity. The aim of the partnership is to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance. The EU will invest up to €450 million in this partnership, under its research and innovation program Horizon 2020. Cybersecurity market players, represented by European Cyber Security Organisation (ECSO), are expected to invest three times more.

Atos chairs the ECSO Board of Directors and is a member of ECSO’s partnership board, which is the ECSO body that liaises with the European Commission for the monitoring of the European Cybersecurity contractual PPP and the research & innovation priorities.

Within ECSO there are numerous working groups. Atos is mainly involved with the Sectoral Demand and the Research working groups. The results of TREDISEC are part of the background that Atos brings to discussions within ECSO to define future research agendas in cybersecurity and to align sectoral requirements for cybersecurity with available technologies.

---

5 Individual Partners Exploitation Strategies

We now report on the individual partner exploitation strategy as reported by the individual consortium members.

5.1 Exploitation by ARSYS

5.1.1 Organization Profile

Arsys is the leading Spanish Cloud Service Provider offering Internet solutions for companies and IT professionals. Pioneer in Cloud Hosting in Europe through its commitment to innovation, Arsys provides an easy integration of Information Technology into businesses with a wide range of Web Presence, Cloud Computing, Managed Hosting and Infrastructure as a Service (IaaS) solutions.

With 266,000 customers, Arsys is a wholly owned subsidiary of United Internet Group, a public company with a market cap of more than 10 Billion €. Arsys has a staff of over 300 employees and manages three Data Centres in Spain and Cloud nodes in USA, England and Germany, hosting over 200,000 web pages and 1.5 million email accounts.

In Arsys, there are different segments of customers, from those only interested in website hosting to customers using specific solutions to be configured according to unique requirements, and also customers acting as resellers.

One of the most important lines of business in the company is Advanced Cloud Solutions (ACS), targeting high value customers with requirements above the standard parameters of hosting. Such solutions combine both hosting and Cloud solutions, and also other complementary features as backups, VPNs, SSL, firewalls, security solutions, dedicated servers, etc. TREDISEC fits perfectly as a valuable service to these users. Obviously these customers require consolidated, powerful and easy-to-use products with high levels of reliability. Arsys believes that TREDISEC could be a competitive advantage.

5.1.2 Exploitation Plan and Activities

After testing some of the TREDISEC outcomes, Arsys’ interests in the exploitation of the project results can be summarized into 3 fields, mostly involving the outcomes of the project in the areas of security, multi-tenancy, isolation and deduplication and compression:

1. Improving services currently offered to customers, and developing innovative solutions and services that can be incorporated into Arsys’ product lines and introduced into the market, thus strengthening Arsys’ market position: we are considering the secure deletion and isolation primitives and the multitenancy access control here in order to add extra features to all services that include online storage, like Cloud builder and dedicated servers (normal and managed servers).

2. Arsys will also use the project results internally to improve its own cloud computing developments: further developments in the area of secure deduplication and isolation can be applied in this area, where all platforms supporting hosting and corporate services could save disk space while keeping data encrypted.

3. Consultancy and integration services provided to large accounts and ACS customers in relation to the adoption of multitenancy access control, secure deduplication and secure deletion, so that all our services offered to these customers can include these added value services as an option in the quotations.

According to our experience running tests performed on our platform, the next steps for our individual exploitation plan are:

1. Together with the primitive owners, developing the current packets to integrate all of them in a single platform that can enable the interaction of all the different primitives that Arsys would like to include in all the 3 fields explained above.
2. Deploying the new version of the primitives in the Arsys productive platforms, so that combinations of these primitives can be tested with all the portfolio products described above.

3. After the analysis of the impact of all these TREDISEC outcomes in Arsys portfolio is performed, executives will decide which products and which milestones will be re-defined so all the new services can be incorporated.

All in all, we expect that several products and business units could improve their sales and the number of security requirements that can be satisfied if all these four primitives show that they can be deployed under real Arsys customers’ use cases.

Another option Arsys is considering to extend exploitation of project solutions is to promote TREDISEC outcomes with some of our partners, so that Arsys’ customers could obtain benefits from the owners of the TREDISEC primitives.

5.1.3 Actions towards Exploitation

The following table gives an overview of the exploitation activities ARSYS has carried out towards exploitation of its project results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Madrid and Logroño / Spain</td>
<td>Commercial sessions to identify best ARSYS products and alternatives to implement TREDISEC outcomes</td>
<td>ARSYS business development units and Integrators</td>
<td>Several products were identified as potential beneficiaries of TREDISEC outcomes (apart from the cloud storage of the UC)</td>
</tr>
<tr>
<td>December 2017</td>
<td>Logroño / Spain</td>
<td>Workshop with business and product management units to analyse potential usage of TREDISEC primitives in ARSYS portfolio</td>
<td>ARSYS business development units and Integrators</td>
<td>Status of primitives shows they are not mature enough to be offered to customer. Lack of integration among them is a negative point too.</td>
</tr>
</tbody>
</table>

Table 7: Overview of ARSYS Exploitation Activities

5.2 Exploitation by ATOS

5.2.1 Organisation Profile

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of circa €12 billion and circa 100,000 employees in 72 countries. Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. Atos works in different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Within Atos Research & Innovation (ARI), node of R&D at Atos in Spain, there is technology transfer and business development team that works on transition from research results to Atos global portfolio and service lines. The Cybersecurity lab has a large experience in Research and Innovation projects focused on Security.
5.2.2 Exploitation Plans and Activities

Within the TREDISEC scope, Atos has developed two primitives and participated in the development of the framework. The individual exploitation plans for each of them is detailed next.

- **Multi-Tenancy Access Control (EPICA)** oriented to control access to resources (either services or data) in multi-tenant cloud environments. EPICA fulfills end-to-end security requirements while preserving critical functional requirements of cloud computing, such as scalability, availability, and high performance. EPICA could be presented to the **Innovation Board (IB)** of Atos Research & Innovation (ARI) for its assessment in order to be recognised as a mature software asset, ready to be reused internally or launched into the market as part of a larger solution. This process has been already initiated preparing the required material for the IB members, with actions such as demo preparation, documenting code, etc.

The Innovation Board is a specific ARI initiative to generate new assets based on the results of R&D projects like TREDISEC, and take them into the market using the internal technology transfer lines of Atos. This board is qualified to assess the proposed assets, based on pre-established criteria, and to set priorities among these along the exploitation paths: align with Atos offering – market pilot or PoC – go to market. The selected assets will be promoted to receive resources available for promotion, will be supported to business development, or will participate in proof of concept (PoC) and pilots with Atos customers.

Besides, the approach is applicable to Authentication and Authorization for Constrained Environments (ACE), such as IoT or 5G scenarios, where strong fine-grained mutual authentication and authorization schemes are critical to protect frequency and radio/communication resources, to deliver 5G networks services on demand and comply with different regulation constraints.

Authentication, Authorization and Accounting (AAA) services play a central role in 5G security, at least to protect frequency and radio/communication resources, to deliver 5G networks services on demand and comply with different regulation constraints [11].

This opens a wide and cutting-edge myriad of possibilities for a solution as EPICA, whose feasibility we want to explore for 5G or IoT security use cases.

- **TPM-Based Remote Attestation (TRAVIS):** TRAVIS contributes to increase users’ confidence in an outsourced execution environment by using the TPM technology for the verification of the integrity of a remote virtual environment. This primitive contributes to overcoming some of the main barriers that prevent full cloud adoption such as the lack of proper end-to-end security mechanisms, the need for efficient monitoring of security, and privacy-related aspects in virtual environments that generate proofs and guarantees towards certification of such environments (See D3.3).

In Atos Research & Innovation we have the Next Generation Cloud (NG Cloud) lab³, focused on Cloud Service Integration, the so-called Multi-Cloud, and Edge Computing. The SLA-Framework is an asset, developed by the NG Cloud lab, which provides tools and best practice guidance on the full SLA Lifecycle for Multi-Cloud Providers and Adopters [12].

More specifically, the SLA Framework provides a technical solution that helps materialize SLA contracts and manage the SLA lifecycle providing:

- Standardized SLAs Definition
- Multi-Cloud Independent Monitoring
- SLA Template Definition
- Multi-Cloud SLA Assessment, Enforcement Accounting and Notifications

³ [http://booklet.atosresearch.eu/content/next-generation-cloud](http://booklet.atosresearch.eu/content/next-generation-cloud)
Exploring the Atos offering lines where TRAVIS could add value, we have chosen SLA-Framework because this solution does not have functionalities to verify security aspects such as integrity. TRAVIS could complement the SLA-Framework by contributing to monitor the integrity of virtual environments and dictating the quality of services built on top of them.

We already have presented TRAVIS to the NG Cloud lab and they have expressed interest in the solution. Next steps would be to conduct a feasibility study in technical and operational terms, to determine if the integration of the TRAVIS primitive into the architecture of the SLA-Framework (e.g. a Proof of Concept could be a first step) is viable or not.

- **TREDISEC Framework:** Atos is also interested in supporting the TREDISEC framework as part of the joint exploitation strategy agreed by the consortium as described in Section 4.

### 5.2.2.1 Expected Impacts

Within Atos Research and Innovation, and in particular in the Cybersecurity Lab\(^4\), TREDISEC permitted to further develop two existing proof-of-concept technologies (TPM remote attestation protocol and XACML-based access control proxy and engine) to become mature prototypes validated and demonstrated in relevant environments (TRL 5 and 6 respectively). These two pieces of software contribute to enlarge and enhance ARI's portfolio. Additionally, the know-how acquired in cloud security and particularly in the areas of confidentiality and cloud efficiency and integrity with computation efficiency permit better positioning our company in both the internal (other Atos business units) and external (Atos clients) markets.

Within Atos, the Scientific Community’s mission is to define Atos’ vision for the major trends and future business challenges regarding digital technologies, and considers how these will be addressed by emerging technologies.\(^5\)

The last whitepaper published by this community, Atos Ascent Journey 2018\(^6\), identifies as a relevant digital challenge to guarantee levels of Data Security & Privacy to Cloud services. The knowledge acquired in TREDISEC regarding confidentiality and integrity of data and computations outsourced to the cloud will surely contribute positively to position ARI as a reference in Cloud Security within the Scientific Community.

Another entity where the acquired competences in TREDISEC have contributed to better positioning our Research & Innovation department is the Atos Experts Community. This entity was created with the purpose of identifying innovation topics to drive Atos research and, in particular, the developed work in TREDISEC is of great value for orientating research in cybersecurity.

Gaining relevance in both entities, the Scientific Community and the Atos Experts Community, allows us, to some extent, having some influence in the overall strategy of Atos towards technology related investments in the future.

### 5.2.3 Actions towards Exploitation

The following table gives an overview of the activities ATOS has carried out towards exploitation of its project results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2015</td>
<td>Barcelona/ Spain</td>
<td>Meeting between Canopy and Atos Research &amp; Innovation to present the future research lines on Cloud.</td>
<td>Atos Cloud Security Experts</td>
<td>Good feedback about the solution. However It did not fit in their short term strategy.</td>
</tr>
</tbody>
</table>

\(^4\) [http://booklet.atosresearch.eu/content/trustworthy-systems-services-4](http://booklet.atosresearch.eu/content/trustworthy-systems-services-4)


TREDISEC was presented as cloud security project within state-of-the-art projects.

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event Description</th>
<th>Responsible Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Madrid/ Spain</td>
<td>Meeting with Business Development ARI Manager to value how TRAVIS could transfer technology to other units.</td>
<td>Business Development</td>
</tr>
<tr>
<td>May 2017</td>
<td>Madrid/ Spain</td>
<td>Presentation of TRAVIS to NG Cloud lab</td>
<td>Cloud Security Experts</td>
</tr>
<tr>
<td>November 2017</td>
<td>Madrid/ Spain</td>
<td>Meeting with Business Development manager to talk about EPICA</td>
<td>Business Development</td>
</tr>
<tr>
<td>December 2017</td>
<td>Madrid/ Spain</td>
<td>Webinar+Support material about the complete TREDISEC solution, as well as EPICA and TRAVIS</td>
<td>Atos Security Technology Providers and Integrators</td>
</tr>
</tbody>
</table>

Table 8: Overview of ATOS Exploitation Activities

5.3 Exploitation by ETH

5.3.1 Organization Profile

ETH Zurich (Swiss Federal Institute of Technology in Zurich) is a science, technology, engineering and mathematics university in the city of Zürich, Switzerland. It is an integral part of the Swiss Federal Institutes of Technology Domain (ETH Domain) that is directly subordinate to Switzerland's Federal Department of Economic Affairs, Education and Research. The school was founded by the Swiss Federal Government in 1854 with the stated mission to educate engineers and scientists, serve as a national center of excellence in science and technology and provide a hub for interaction between the scientific community and industry. ETH Zurich is consistently ranked amongst the most prestigious universities in the world for the subjects of engineering and technology.

5.3.2 Exploitation Plans and Activities

ETH individually exploits the TREDISEC projects mostly in the form of student projects and lecture contents. In particular, ETH has completed one semester project and three master theses around the topics of TREDISEC. Also new lectures have been created based on the research results achieved under TREDISEC.

The semester project focused on shared ownership (T4.4) and was supervised together with NEC. One of the master theses focused on secure deletion (T4.4) and studied further extensions to secure deletion and their performance. Another ETH student completed a master thesis on isolation, in particular rollback protections for Intel SGX (T4.2). The third master thesis was focused on side-channels against SGX (T4.2). Further student projects (master’s theses) are currently under investigation.

TREDISEC-related outcomes were also new content for ETH master-level lectures and courses. These lectures (accompanied by matching exercises) discussed current developments in trusted computing (SGX research, T4.2) including its security limitations (side-channel attacks, rollback) and security improvements.
5.4 Exploitation by EURECOM

5.4.1 Organization Profile

EURECOM is a Graduate school and Research Centre in Communication Systems located in the Sophia Antipolis technology park (French Riviera), a major European place for telecommunications activities. EURECOM was founded in 1991 in a consortium form [GIE]. The industrial and academic members of the consortium include Orange, ST Microelectronics, BMW Group Research & Technology, Symantec, Monaco Telecom, SAP, IABG, Institut Mines-Telecom, Aalto University (Helsinki), Chalmers University of Technology, Politecnico di Torino, Technische Universität München (TUM), Norwegian University of Science and Technology (NTNU), Czech Technical University (CTU) in Prague and Principality of Monaco. EURECOM provides graduate and postgraduate courses in communication systems and offers four Master of Sciences fully recognized by the French State and dedicated to foreign students. In 2012, EURECOM opened two Post Master's degrees in booming sectors: Security for Computer Systems and Communication and Communication for Intelligent Transportation Systems. EURECOM undertakes internationally-leading research within three main domains: Communications Systems, Digital Security and Data Science. EURECOM research teams are made up of international experts, recruited at the highest level, whose work is regularly honored and has earned international recognition. EURECOM has participated to several European, national and international research projects.

5.4.2 Exploitation Plans and Activities

One of the main exploitation strategies for EURECOM is to enrich teaching and attract excellent students to the graduate education program and the research activities. TREDISEC findings will be integrated within the newly proposed “Privacy for Big Data and the Cloud” lecture that will be starting in the 2018-2019 academic year. This will improve the knowledge transfer to future engineers. EURECOM also offers on a regular basis dedicated training programmes for its industrial partners' personnel. Future sessions of these programmes will also greatly benefit from the findings of TREDISEC in the field of security and privacy for the cloud.

Moreover, thanks to the TREDISEC research topics and findings, one PhD student has already successfully obtained his doctoral degree (topic: verifiable cloud computing). Two other PhD students are currently finalizing their research work and have started to write their thesis (topics: searchable encryption and verifiable cloud storage). Finally, EURECOM also completed four master projects each of them focusing on the design and/or development of one TREDISEC primitive (multi-user searchable encryption, ML-POR, verifiable computing, secure data deduplication).

Work undertaken in TREDISEC has fed into several research proposals currently in development and in submission to the EU H2020 programme, as well as to work that has recently been accepted for funding from the EU H2020 programme (PAPAYA, “PIAtform for PrivAcY preserving data Analytics” Proposal no: 786767).

Furthermore, participating in TREDISEC allows EURECOM to reinforce its position within the scientific community concerned with cloud security. One of the benefits of developing such expertise is the technology transfer to its consortium of academic and industrial partners. The close association with industrial partners gives all parts of the Digital Security department the opportunity to put research ideas into practice.

5.4.3 Actions towards Exploitation

Regarding the primitives developed by EURECOM in TREDISEC, the support of open-source primitives such as MUSE or ML-POR provides engagement with a broader open-source community, not limited to consortium members. EURECOM will give access to the recipes of all its developed primitives. ML-POR, the verifiable polynomial evaluation and the verifiable matrix multiplication primitives are open-source and therefore will be available to anyone interested. EURECOM may also consider opportunities for patenting.
Furthermore, as previously mentioned, TREDISEC findings will be integrated within the newly proposed “Privacy for Big Data and the Cloud” lecture that will be starting in the 2018-2019 academic year. This will improve the knowledge transfer to future engineers.

5.5 Exploitation by GRNET

5.5.1 Organisation Profile

GRNET S.A. provides Internet connectivity, high-quality e-Infrastructures and advanced services to the Greek Educational, Academic and Research community. GRNET also provides advanced services to the following sectors: Education, Research, Health, Culture. Its backbone interconnects more than 100 institutions including all universities and technological institutions, research centres, public hospitals, museums and libraries, as well as the Greek School Network, with speeds up to 26×10Gbps through its high-speed, high-capacity infrastructure of long-term leased fiber that spans across the entire country.

Its innovative Cloud Computing services are available via the Infrastructure-as-a-Service model, under the brand name ~okeanos. By using ~okeanos, any academic user can create a multi-layer virtual infrastructure and instantiate virtual computing machines, local networks to interconnect them, and a reliable storage space within seconds. Thousands of academic users have already utilized virtual machines in the course of their research, experimental, educational or other activities. The Cloud Computing infrastructure and services of GRNET have been made available to the pan-European R&E community via the “okeanos-global” service. GRNET provides its services towards the Greek Educational, Academic and Research community for free.

GRNET coordinates a series of initiatives aimed at creating e-infrastructures and services that can facilitate organizing, describing, and promoting digital content of educational, research, geospatial, and environmental as well as cultural topics. These actions contribute to the vision of creating a virtual horizontal infrastructure of digital repositories, which is available from universities, research centres, museums, libraries and other institutions and facilitates the preservation, sharing and exploitation of digital content by businesses and the society. The ultimate goal is to enhance the use of digital content and services from researchers, teachers, staff of public bodies and SMEs, as well as other types of communities involved in the production, processing, and use of digital knowledge.

5.5.2 Exploitation Plans and Activities

~okeanos cloud service is the perfect recipient for the novel security schemes and protocols developed by the TREDISEC project. Implementing the proposed methodologies in order to improve security for our clients will be the challenge for us. Through well controlled test cases on our already implemented infrastructure, we will contribute to our continuous effort of improving cloud security for our clients, while at the same time provide the rest of the project teams with the opportunity to measure the overhead imposed by the security mechanism proposed. The work in TREDISEC will enhance GRNET’s capabilities to better identify security risks imposed by cloud services, prioritize those risks and propose new mitigation mechanisms that can adapt to each client’s particular needs for cloud security as an add-on to our products.

Regarding the TREDISEC framework, GRNET’s exploitation plan is to deploy it as a service to internal projects and projects of its clients. A great number of those projects need to build on GRNET’s cloud infrastructure. By using the TREDISEC framework installation as technology portal GRNET helps build a community around common solutions that will enable the creation of more and better technology.

GRNET also plans to utilize the Container Isolation primitive in the next generation of its cloud services (there are at least 2 funded actions), which will support deployment of containers featuring their smart placement and management according to infrastructure conditions, capabilities and user preferences. Container Isolation offers a practical and effective mechanism to meet user preferences for encryption, especially in combination with other infrastructure requirements such as migrating containers for performance or power consumption optimizations.
It should be noted that GRNET’s exploitation strategy also includes all those actions that enable the internal teams to facilitate the beneficial results of TREDISEC, in order to enable them to design advanced cloud services for its users.

The main impact of TREDISEC technology on GRNET involves easier and better security both for GRNET’s cloud infrastructure services and for GRNET clients’ projects. In general, clients will be more willing to use GRNET’s cloud infrastructure because of the enhanced security and feature set. At the same time, resource consumption will be better optimized for GRNET.

More specifically, GRNET has several collaborators that handle sensitive data, including collaborators from the medical sector. Increased security is important for sensitive data, especially since the new European data privacy regulation (GDPR) will be in effect. If GRNET enhances its services with TREDISEC technology, clients can achieve data protection with less cost and more trust than they could handle if they were to implement them by themselves. Even GRNET as a service provider itself will enhance its own security and data privacy regulation conformance. Enhanced security will also allow GRNET to offer a more complete feature set and project more trust and ultimately seek more collaborations and thus broaden its audience and clients, boosting innovation and scientific research in the Greek academic community.

### 5.5.3 Actions towards Exploitation

The following table gives an overview of the activities GRNET has carried out towards exploitation of its project results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2016</td>
<td>GRNET SA HQ</td>
<td>Survey for security features they need for their current and upcoming projects</td>
<td>Blood Donor Registry IT manager</td>
<td>TREDISEC results look promising. Should revisit in the future.</td>
</tr>
<tr>
<td>March 2017</td>
<td>GRNET SA HQ</td>
<td>Security audit of services running on GRNET infrastructure to identify issues that can be addressed with enhanced security measures</td>
<td>Greek Hospital IT Managers, GRNET collaborators</td>
<td>Good feedback about the solution.</td>
</tr>
<tr>
<td>May 2017</td>
<td>GRNET SA HQ</td>
<td>Train project managers and key people from GRNET’s collaborator organizations to technologies TREDISEC offers and can be used to secure existing or new application designs.</td>
<td>GRNET Project Managers</td>
<td>Should definitely use it when completed.</td>
</tr>
<tr>
<td>November 2017</td>
<td>GRNET SA HQ</td>
<td>Create a plan with the operations department for the long-term maintenance of the servers hosting the GRNET TREDISEC framework installation.</td>
<td>Operations department</td>
<td>New meeting is needed to finalize plan.</td>
</tr>
</tbody>
</table>

Table 9: Overview of GRNET Exploitation Activities
5.6 Exploitation by IBM

5.6.1 Organisation Profile

In June 2013, IBM announced to acquire SoftLayer Technologies, Inc., the world’s largest privately held cloud computing infrastructure provider at that time. The acquisition as well as the subsequent formation of a new Cloud Services division strengthened IBM’s position in cloud computing and helped speed business adoption of public and private cloud solutions. Among its many innovative cloud infrastructure services, SoftLayer allowed clients to buy enterprise-class cloud services on dedicated or shared servers, offering clients a choice of where to deploy their applications.

Complementing SoftLayer as an Infrastructure-as-a-Service (IaaS), Bluemix [13] is the IBM open cloud platform that offers mobile and web developers access to IBM software for integration, security, transactions, and other key functions, as well as software from business partners. Built on Cloud Foundry open source technology, Bluemix makes application development easier with Platform-as-a-Service (PaaS). Bluemix also provides prebuilt Mobile-Backend-as-a-Service (MBaaS) capabilities. The goal is to simplify the delivery of an application by providing services that are ready for immediate use and hosting capabilities to enable internal scale development.

Both SoftLayer and Bluemix are today branded as IBM Cloud. IBM Cloud powers AI-intensive workloads that demand data integrity, low-latency and parallel processing. It also offers a broad range of Watson AI and machine learning APIs to build your own applications. IBM Cloud offers the widest array of database options, from relational to NoSQL, while ensuring strong consistency, high integrity, and no delay.

Security is at the core of IBM Cloud, it is not an afterthought. IBM Cloud secures the movement of data on a network of networks. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management. IBM Cloud meets data sovereignty and compliance regulations with nearly 60 locally owned and operated data centers in 19 countries—more than any other cloud provider.

IBM Cloud is available in nearly 60 data centers globally as well as in private data centers. It is possible to consume cloud services over the internet, to deploy cloud services in a company data center, and to integrate multiple cloud infrastructures and traditional IT.

Designed with secure engineering practices, the IBM Cloud platform has layered security controls across network and infrastructure, and provides a group of security services that can be used by application developers to secure their mobile and web apps. It also ensures security readiness by adhering to security policies that are driven by best practices for systems, networking, and secure engineering [14]. These policies include practices such as source code scanning, dynamic scanning, threat modelling, and penetration testing. IBM Cloud follows the IBM Product Security Incident Response Team (PSIRT) process for security incident management [15]. The IBM Cloud environment is compliant with the most restrictive IBM information technology (IT) security standards, ranging across network, data encryption, and access control:

- Application ACLs, permissions, and penetration testing
- Identification, authentication, and authorization
- Information and data protection
- Service integrity and availability
- Vulnerability and fix management
- Denial of service and systematic attacks detection
- Security incident response

5.6.2 Exploitation Plans and Activities
The TREDISEC project produced a range of cloud security techniques that enhance the security of the IBM Cloud.

**Attack Surface Reduction** includes a wide set of tools that ensures that an attacker has the smallest amount of resources at its disposal to attack a system. The IBM Cloud and customer of it benefit from this set of capabilities developed in TREDISEC because several zero-day exploits target unused features of the kernel and the risk can be significantly lowered with a reduced attack surface.

**Fuzz Testing** behaves like a classic fuzz tester, by supplying mutated input to a program and observing its behaviour. Often, mutated input leads to crashes, and the crashes reveal ways of exploiting the program. Standard fuzzers however do not take into account the distributed nature of some of the software that powers the cloud. The distributed fuzzer will be optimized for distributed programs and components. The output is a series of crash reports including back-traces and the developer/tester can manually intervene to fix the bug and harden the code. The TREDISEC capability of Fuzz Testing is, thus, a good extension to source code scanning and dynamic scanning procedures in the IBM Cloud.

**Proof of Ownership** refers to a cryptographic protocol that regulates the interactions between a prover and a verifier. The protocol is usually executed in the context of a storage outsourcing scenario, where the prover is the client and the verifier is the (storage) service provider. The correctness property of Proof-of-ownership schemes require that the owner of a file will succeed in convincing the verifier of this fact. This TREDISEC technology can be deployed as part of a deduplication scheme on encrypted data and therefore has the potential to lead to significant storage reduction and lowered operational costs.

Other TREDISEC capabilities have, too, potential commercial applicability in the context of the IBM Cloud (e.g., **Key Management**). The overall alignment of TREDISEC output with IBM Cloud offerings suggests good opportunities for exploitation. As TREDISEC partner, IBM Research has already approached the respective IBM development organizations in order to discuss the integration of TREDISEC capabilities. Dissemination paths are being planned in the context of the next cloud architecture that IBM will deploy as the foundation of future cloud offerings. As a further action, the integration of the listed cloud security functions should be transferred via the “joint program” that is established on a yearly basis between IBM Research and the IBM Cloud business unit. This highly effective technology transfer mechanisms has been used for exploitation of many similar cloud innovations before.

Cloud represents over 20 percent of total IBM revenue with full-year cloud revenue of $17.0 B, up to 24 percent year to year [16]. We expect a measureable positive impact on IBM’s cloud business, which will be in the form of reducing operational costs (i.e., reduced storage capacity due to deduplication, reduced security incidents due to attack surface reduction and fuzz testing) as well as increased revenue based on competitive advantage and differentiating security (i.e., increased privacy due to key management and a range of other TREDISEC developed capabilities).

### 5.6.3 Actions towards Exploitation

The following table gives an overview of the activities IBM has carried out towards exploitation of its project results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 2017</td>
<td>Internal Meetings</td>
<td>TREDISEC primitives were discussed with various stakeholders in the IBM Systems division. The context of the discussions was the 2018 joint program funding and</td>
<td>IBM Systems division</td>
<td>A new joint project was defined that included various aspects of the</td>
</tr>
</tbody>
</table>
respective technology transfer from IBM Research to the IBM Systems business unit.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2017</td>
<td>Internal Meetings</td>
<td>TREDISEC primitives were discussed with various stakeholders in the IBM Security division. The context of the discussions was the 2018 joint program funding and respective technology transfer from IBM Research to the IBM Security business unit.</td>
</tr>
<tr>
<td>Feb 2018</td>
<td>Internal Meetings</td>
<td>Preparation of the IBM internal Storage Security strategy.</td>
</tr>
</tbody>
</table>

Table 10: Overview of IBM Exploitation Activities

5.7 Exploitation by IDEMIA

5.7.1 Organisation Profile

IDEMIA is the global leader of Augmented Identity – an identity technology that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions for an increasingly digital world. Through its core markets, IDEMIA aims to empower people to enjoy life through trusted identities. Whether in the physical or digital world, for government, civil or commercial usages, IDEMIA combines a wide range of innovative technologies to provide its customers with convenient and user-friendly products and services making our world a safer place.

IDEMIA team is made up of 14,000 employees, gathers more than 80 nationalities, and speaks 32 languages.

IDEMIA addresses the following main markets:
- Financial Institutions: IDEMIA has given birth to offers that help financial institutions take on mobility and digitalization, shaping the future banking and payment customer journey (management of secret keys, reduction of payment fraud – both online and in-store, EMV, NFC and mobile payment migration around the world, digital banking development, secure mobile and IoT/M2M payment solutions).
1. 1,800 financial institutions, including most of the world’s largest banks
2. 1M cards digitalized per month in the 3 major digital wallets
3. Mastering the largest biometric acquisition and verification projects in the world

- **Mobile Operators:** IDEMIA designed tools to link strong authentication with secure elements and service platforms to guarantee simple connectivity and service access to end-users anywhere, anytime. IDEMIA also assists its clients through the disruptive management of subscriptions through dedicated platforms as well as embedded or removable SIM cards and optimized chips. IDEMIA services are optimized, connecting many more objects to enable vertical services. From supporting connectivity through SIM cards, to using mobile devices as biometric entry points to authenticate themselves, and to developing digital wallet services, individuals can have full and worry-free usage of their mobile phones while safeguarding their mobile identities with the highest level of protection.

  1. 500 mobile operators around the world, including leading mobile operators worldwide
  2. 20+ subscription Manager solutions delivered
  3. 100+ OTA platforms deployed around the world

- **Connected Objects:** IDEMIA’s solutions combine security and convenience to enable OEMs and IoT service providers to manage the connectivity and safety of a wide range of devices across the world and to deploy and maintain critical value-added services during a device’s full lifecycle.

  1. Major industrial OEMs, including premium mobile and car makers and leading IoT players
  2. Leader Front-runner on eSIM & remote subscription management in the consumer device and IoT spaces
  3. 250M embedded Secure Elements (eSE) sold in the world

- **Citizen Identity:** IDEMIA provides services to protect citizens’ identities on the move. Citizens travel more than ever before, are more connected and digital than ever but also more aware of privacy and security concerns. IDEMIA’s solutions ensure citizens and governments alike that each delivered identity is unique and can be trusted, whenever and wherever. IDEMIA is the unique one-stop-shop that can effectively manage and secure the entire value chain for its customers – governments, from registration and verification of citizens’ identities, to issuing personalized IDs that resist fraud – in the form of traditional ID documents or digital IDs – to managing those identities securely both in the physical and digital world.

  1. #1 in civil identity solutions & engaged in the world’s largest biometric deployment (Aadhaar, India)
  2. 3bn+ identity documents issued
  3. 135+ active citizen identity programs

- **Public Security:** As the world leader in biometric solutions, IDEMIA’s fully integrated solutions and innovations focus on the user experience, allowing its customers to do more with less budgets: risks and threats identification, and crime solving in less time than ever; efficient and transparent identity verification for citizens, which creates a safer world, yet has very little impact on their daily life. IDEMIA’s services now combine digital and cloud expertise to bring unparalleled efficiency and next-generation user experiences to our customers.

  1. #1 in police biometric systems & world largest supplier of biometric terminals
  2. 150+ million passenger crossings managed
  3. 169 AFIS (Automated Fingerprint Identification) systems deployed around the world
As most of IDEMIA’s customers need to focus on their core business, they have plan the outsourcing of some of their major IT functions, as well as some of their digitalized business processes. Therefore, one of IDEMIA’s strategic business development lines aims to build a set of solutions and services that combine data hosting and Cloud computing, including its biometric solutions. TREDISEC’s framework offers an opportunity to build a competitive offer, by providing end-to-end security solutions that take care of privacy, data availability and integrity, and ensure customers’ processes isolation.

5.7.2 Exploitation Plans and Activities

The innovative technologies produced within the project are expected to be combined with IDEMIA’s biometric system solutions, enabling the company to generate intellectual property and to provide a wide range of new products and services in the trendy and competitive market of Security Services Out-Sourcing. TREDISEC’s framework offers a perfect opportunity to test the privacy preserving biometric matching primitive (prototyped through WP3) within a realistic cloud environment. Thus:

- IDEMIA intends to use the processing of encrypted biometric data capability on the one hand, for private identification over encrypted biometric database, and on the other hand, for processing encrypted biometric images, even though at the time of this writing, current innovations achieved within the project belong to the TRL 2-3 level.
- IDEMIA intends to deploy the developed prototype for a privacy preserving biometric matching primitive via its offer MorphoCloud, an Automated Fingerprint Identification System in the cloud implementing IDEMIA’s flagship Biometric Identification Solution.
- Within its activity of the outsourcing of major updates on its customers’ biometric databases, IDEMIA intends to improve the quality of service provided to its customers, by applying update algorithms over encrypted biometric data, and thus address privacy issues. (Outsourcing Service of major updates on biometric databases: A major accuracy update of biometric systems requires reprocessing the raw images to enable the new algorithms. This process usually takes time (e.g., several months) and requires in-house hardware. Thus, the perspective to delegate such computations to the cloud seems appealing. However, for privacy reasons, outsourced biometric data should be encrypted.)

Moreover, the technologies about the verifiability of computation produced by the project could enhance IDEMIA’s technologies for secure computation over encrypted biometric data. Thus:

- IDEMIA intends to use the efficient and strong authentication means (biometric authentication based on verifiable computing techniques) within the FIDO alliance for supplying strong online authentication.
- IDEMIA intends to use verifiable computation technologies to enhance its solutions at airport gates. In particular, they might be used to accelerate the throughput at the boarding gates.

5.7.3 Actions towards Exploitation

The following table gives an overview of the activities IDEMIA has carried out towards exploitation of its project results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2017</td>
<td>Paris / France</td>
<td>Workshop with Product management unit of the Strategy-</td>
<td>IDEMIA Strategy-Market&amp;Offer-Innovation Unit</td>
<td>Several services (based on the processing of encrypted biometric data capability) were identified as potential beneficiaries of TREDISEC outcomes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management unit of the Strategy-Market&amp;Offer-Innovation to identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>best IDEMIA products and strategies to implement TREDISEC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 11: Overview of IDEMIA Exploitation Activities

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Description</th>
<th>IDEMIA Unit</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2018</td>
<td>Paris/France</td>
<td>Workshop with Strategy, Business and Product management unit of the Citizen Identity BU to analyse potential usage of TREDISEC primitives in Citizen Identity BU portfolio</td>
<td>Citizen Identity Business Unit</td>
<td>As the current innovations achieved within the project belong to the TRL 2-3 level, potential TREDISEC outcomes benefits are expected in the middle term</td>
</tr>
<tr>
<td>January 2018</td>
<td>Paris/France</td>
<td>Workshop with Sales and Marketing unit of the Public Security BU to analyse potential usage of TREDISEC primitives in Public Security BU portfolio</td>
<td>Public Security Business Unit</td>
<td>Additional development and integration are necessary to implement the privacy preserving biometric matching primitive within a realistic cloud environment. It is also the case for the Outsourcing Service of major updates on biometric databases</td>
</tr>
</tbody>
</table>

### 5.8 Exploitation by NEC

#### 5.8.1 Organisation Profile

NEC Corporation is a leader in the integration of IT and network technologies that benefit businesses and people around the world. By providing a combination of products and solutions that cross utilize the company's experience and global resources, NEC's advanced technologies meet the complex and ever-changing needs of its customers. NEC brings more than 100 years of expertise in technological innovation to empower people, businesses and society.

NEC Laboratories Europe GmbH is a research laboratory and is located in Heidelberg, Germany. NEC Labs Europe conducts leading research and development across IT and communications, including Future Internet, next generation fixed and mobile networks, security and privacy technologies, the Internet-of-Things, multimedia and smart energy services. NEC Laboratories Europe has provided solutions for Identity and Access Management, processing of encrypted data, and mobile device security.

#### 5.8.2 Exploitation Plans and Activities

Over the course of TREDISEC, NEC has focused on the definition, implementation, and assessment of a number of security primitives related to Proofs of Retrievability (PoR), secure deduplication, and encryption.

A proven track record of successful publications in well-respected conferences presenting the research results carried out within TREDISEC, and patents filed to protect these innovative results, speak for NEC’s commitment to the project and its outcomes.

NEC is in constant discussion with Business Units and intends to use TREDISEC’s results in future NEC products. NEC plans to use the project’s outcomes to enhance its products, such as its SaaS and IaaS solutions. More specifically, NEC cloud services and storage solutions can greatly benefit from TREDISEC research. Indeed, thanks to TREDISEC, NEC will be able to provide a complete cloud storage solution that offers advanced encryption, efficient data verification and repair, and costs reduction through deduplication. Namely, we argue that our technologies motivate a novel business model in which customers and external auditors establish a contract by which customers can rest
assured about the security of their files. By doing so, our technologies increase the users’ trust in the cloud, while incurring minimal user interaction. We therefore argue that our work lays basic foundations for realizing secure external auditing of cloud services; we believe that such auditor-based schemes will provide a stepping stone for establishing a cyber-insurance market for cloud services and could considerably strengthen NEC storage solutions in the area.

### 5.8.3 Actions towards Exploitation

The following table gives an overview of the activities NEC has carried out towards exploitation of its project results with special focus on promotion of results towards target groups (users, business partners etc.).

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Location</th>
<th>Activity</th>
<th>Target Group</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 22-25, 2016</td>
<td>GSMA Mobile World Congress 2016, Barcelona, Spain</td>
<td>Demonstration and showcasing of secure deduplication technology ClearBox at NEC Booth</td>
<td>GSMA Mobile World Congress Visitors</td>
<td>Assess Market conditions for ClearBox, potential user/customer feedback and contacts.</td>
</tr>
<tr>
<td>April 2016</td>
<td>NEC Headquarters, Japan</td>
<td>Meeting with NEC Business Units for Cloud Manager</td>
<td>NEC Business/Marketing Units</td>
<td>Discussion on enhancing NEC products by secure and efficient ClearBox cloud storage technology</td>
</tr>
<tr>
<td>October 2016</td>
<td>NEC Headquarters, Japan</td>
<td>Meeting with NEC Business Units for VDC and Storage solutions</td>
<td>NEC Business/Marketing Units</td>
<td>Follow up discussion on suitability of PoR and ClearBox for NEC storage products</td>
</tr>
<tr>
<td>June 2016</td>
<td>EEMA TDL (Trust in Digital Life), Industrial Forum; The Hague, Netherlands</td>
<td>NEC as member of TDL chaired the TDL Cloud Security Panel and demonstrated the “secure de-duplicated multi-cloud storage” at EEMA TDL</td>
<td>Industry, Public Sector and Governments</td>
<td>Awareness and promotion of TREDISEC Research Results in relevant Industry Forum; links created to potential partners for future exploitation</td>
</tr>
<tr>
<td>August 2016</td>
<td>SECODIC 2016; Workshop on Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud; ARES Conference,</td>
<td>Presentation of TREDISEC Research Results at Research Conference and Collaboration with H2020 Project WITDOM</td>
<td>Scientific, Research Community</td>
<td>Promotion of TREDISEC research activities and links created to potential partners for future exploitation</td>
</tr>
<tr>
<td>Date Range</td>
<td>Event Description</td>
<td>Session Purpose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 19, 2017</td>
<td>Internal Meeting with the chairman of NEC, CeBIT Hannover, Germany</td>
<td>Introduction of Project Result</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Management of NEC Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Raising awareness with Top Management to promote project activity/results in NEC Group and beyond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 20-24, 2017</td>
<td>CeBIT 2017, Global Exhibition for Digital Business; Hannover, Germany</td>
<td>Exhibition, demonstration and promotion of secure and efficient cloud storage solution ClearBox at NEC booth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CeBIT Visitors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEC secure and efficient cloud storage solution ClearBox promoted, potential customer contacts and feedback</td>
<td></td>
<td></td>
</tr>
<tr>
<td>April 2017 – December 2017</td>
<td>Internal Meetings with relevant NEC Business Units</td>
<td>In the course of the following months this feedback has been evaluated and discussions involving the various NEC business units on how to exploit the information obtained to adjust the business plans accordingly have been intensified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEC Business Units</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Development of business plan for ClearBox based on CeBit customer feedback /integration into future /expansion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 21, 2017</td>
<td>NetCracker Innovation Day; Brussels, Belgium</td>
<td>Presentation and showcasing of secure and efficient cloud storage solution ClearBox</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEC secure and efficient cloud storage solution ClearBox promoted, potential customer contacts and feedback</td>
<td></td>
<td></td>
</tr>
<tr>
<td>January 8, 2018</td>
<td>TREDISEC Evaluation Workshop, NEC Laboratories Heidelberg, Germany</td>
<td>Presentation of TREDISEC Project Results and Feedback/Evaluation by Target Group Feedback - Questionnaire</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud Security Providers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Feedback &amp; Target Group Questionnaires collected for analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12: Overview of NEC Exploitation Activities

5.9 Exploitation by SAP

5.9.1 Organisation Profile

SAP has grown to become the world’s leading provider of business software solutions. With 12 million users, 96,400 installations, and more than 1,500 partners, SAP is the world’s largest inter-enterprise
software company and the world’s third-largest independent software supplier, overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP industry solutions support the unique business processes of more than 25 industry segments, including high tech, retail, manufacturing and financial services.

Via Horizon 2020 projects SAP bridges the gap between open, collaborative research with external partners and exploitation into new or existing SAP product lines through SAP’s development groups. More than 35 researchers of the Product Security Research unit focus on security and privacy in the software development process and products. Recent results include, among many others, a searchable encrypted cloud database, an attack monitoring framework for ERP systems, and cloud-based secure multi-party computation schemes for optimization problems in distributed supply chains. The Product Security Research team has a long history of leading European collaborative research projects to success (15+ projects in FP7) and is actively contributing to shaping the security research agenda.

As the world’s leading provider of business software solutions, SAP is interested in becoming a major company in the Cloud market, moving its on-premise software delivery to the Cloud. Since customers are reluctant to outsource their data into the Cloud due to risk of losing control, research on technologies that allow customers to maintain data ownership of their data is a cornerstone of the company’s Cloud strategy. SAP’s Chief Security Officer Justin Somaini announced Zero Knowledge Systems as a business enabler, consequently putting security into the strategic focus of SAP for the near future. SAP Security Research is working on Zero Knowledge Systems that allow our customers to upload their business data to our Cloud infrastructure while remaining in full control. These systems can directly benefit from TREDISEC results.

5.9.2 Exploitation Plans and Activities

As part of the TREDISEC project, SAP is primarily working on the definition, implementation and assessment of a use case which relates to a company transitioning its data and business operations into the cloud. More particular, as part of this project, SAP’s efforts are twofold: First, as part of WP5, SAP is working with the project consortium on a concept to prepare (i.e. encrypt) data as well as seamlessly outsourcing the actual (encrypted) data into a cloud environment. Second, as part of WP4, SAP is researching and evaluating new designs for privacy-preserving scalable multi-tenant cloud systems that allow resource sharing (and by doing so optimizing the operating costs) without weakening data security.

The results of these research efforts will directly feed into an already existing research project on a searchable yet encrypted database. Thus, the novel techniques developed within the TREDISEC project will support SAP to deliver an industrial-strength solution to its customers as part of SAP’s overall cloud strategy. The SAP Product Security Research group has a full HANA (SAP’s in-memory, column-store database) development environment available within which project results are deployed and evaluated.

Any IP generated within TREDISEC will be either used following a passive (publication) or active (patent filing) strategy. So far, SAP already published five papers and filed three patents that where funded by TREDISEC. This shows the commitment of SAP to utilize the outcomes of TREDISEC in the future. Furthermore, SAP had a direct impact by the importance of the topic worked on in the TREDISEC project. Specifically, it led to the creation of additional resources in SAP’s security research department. A temporary position was transformed to a permanent position underpinning the commitment to follow up on TREDISEC’s results in the future.

SAP’s Product Security Research runs internal projects, such as the SEEED project that are fed by a number of EU projects, such as TREDISEC, ESCUDO-CLOUD or PRACTICE. This enables SAP to focus on a few core inventions and innovations we deliver to SAP. The SEEED project is highly regarded within (and outside of) SAP and strongly benefits from the TREDISEC project. Significant previous development effort has already been spent on SEEED. Apparently, zero downtime migration
from plain on premise data to encrypted outsourced data (WP 5) as well as multi-tenancy support (WP 4) is crucial for customer’s acceptance of the SEEED project.

With the support of TREDISEC, SAP aims to offer a complete cloud transition lifecycle solution that covers (1) analysis of data structures before outsourcing them, (2) efficient data preparation for provisioning, (3) support for an encrypted, yet multi-tenant database with all benefits provided by SAP HANA.

This fits perfectly into SAP’s strategy as S4/HANA has been announced as new core product replacing ERP at the New York stock exchange. This move puts the HANA platform at the center of the SAP product portfolio. Furthermore, it enables products to be deployed seamlessly on premise, in the cloud or as a hybrid. This makes data security even more crucial paving the road for projects like TREDISEC. The security department of SAP, including its research division, consults development in order to ensure safe and secure software services and products. It is placed under Bernd Leukert’s Products & Innovation organization and hence the development groups are the main stakeholders for transferring and exploiting the research results. It is of main importance to create visibility, determine the product roadmap and involve the developers and development managers in the exploitation process. One prime example of these efforts is that the recent SAP HANA 2, which was introduced in the beginning of 2017, already supports data at rest encryption, backup encryption, and application encryption.

5.9.3 Actions towards Exploitation

As part of our exploitation strategy to create awareness, we participated in internal developer conferences, held meetings with internal stakeholders, and ran in internal entrepreneurial competitions. Overall the actions we took are as follows:

- We held successive meetings with several internal stakeholder groups and agreed on a follow-up with the SAP HANA product management.
- We presented at a highly coveted spot at SAP DKOM in Palo Alto to the entire product development organization.
- We presented our encryption technology as a means to secure personal data in the cloud to representatives of the EU parliament and commission.
- We presented our prototype to selected high-profile customers (CISO level) in SAP’s security advisory board.
- We won the 2nd place in the software development organization (P&I headed by Bernd Leukert) in the Hasso Plattner Founders’ Award – the most prestigious SAP internal award with 100.000 EUR prize money. The selection among the 5 highest ranked contestants was made by Bernd Leukert himself.
- We presented TREDISEC technologies at SAP’s Security Expert Summit. This event brings top security experts from academia, the security research community, and SAP’s internal security experts together.
- We showed our TREDISEC use case at the ISSE to a broad audience of industry experts, commercial end-users and government policy-makers.
- We actively attended several direct SAP customer events to give presentations on SAP Security Research results in general and the topic of processing of encrypted data with databases in particular.
- We introduced TREDISEC to multiple internal security experts and technology providers and asked for their feedback through questionnaires. With this effort, we extended the circle of potential consumers of TREDISEC results and got valuable insights for further improvements regarding technical details and business opportunities.
6 TREDISEC Sustainability Strategy and Long Term Sustainability

6.1 TREDISEC Sustainability Strategy

The project results of TREDISEC are key building blocks for a secure and efficient cloud infrastructure. Security and privacy are key for the acceptance of the Cloud as an infrastructure and for protecting human rights worldwide. Setting up a global Cloud infrastructure is beneficial due to the better utilization and therefore the saving of resources that can be achieved. A resilient global IT-Infrastructure such as the TREDISEC framework furthermore enables IT-services and storage for all, even without a powerful local infrastructure and will foster economic growth.

With the sustainability strategy, the TREDISEC consortium aims to ensure that the project outcomes will be widely used and remain available to all stakeholders. The sustainability strategy goes therefore hand in hand with the exploitation plan to aim for a wide use of TREDISEC technology.

The actions will be planned and coordinated by the specifically crafted board that comprises representatives from the consortium members and that will assume control right after the end of the project. In a consortium made of different research institutions, this means pre-emptively ensuring that each organization is in a position of tackling the challenge of market-oriented exploitation and sustainability of its own as well as common project results.

In TREDISEC, the consortium's institutions planned for this challenge by agreeing on establishing an exploitation board (see the individual commitment of partners in the Appendix) that will manage and coordinate the exploitation and IPR of TREDISEC common results, i.e. the framework and the various TREDISEC Recipes, beyond the project life-time.

The goals of the board are manyfold:

- Establishment of an effective and successful long-term impact, exploitation and sustainability strategy for the TREDISEC project results.
- Providing recommendations for the exploitation of common results beyond project life-time.
- Agreeing to and authorizing the terms and conditions for the exploitation of common results.
- Discussing terms and conditions of the partners’ individual interests and plans for exploitation of the TREDISEC common results if necessary.
- Ensuring that board meetings are planned and scheduled when necessary (e.g. upon customer interests in using project results, and or an individual organizations plan to exploit a common result).
- Appointing the respective contacts/agents for response to customer request, and follow-up actions.

The key activities targeting sustainability are:

a) **Activity 1**: providing technology developed in TREDISEC to be further shared, used and built upon;

b) **Activity 2**: increasing the scope of the outcomes beyond the pilot use cases and promote the take up of TREDISEC innovations;

c) **Activity 3**: education, training and influencing the academic community;

d) **Activity 4**: coordinating communication to sustain the benefits of the created partnerships in the consortium.

**Activity 1**
The TREDISEC website (tredisec.eu) that is hosted by ATOS provides access to all public deliverables and further public brochures created by the project. The website will be available beyond the project’s lifetime for at least 4 years and as long the information is still up-to-date.

The TREDISEC consortium releases its framework as a common open source project under the Apache 2.0 License. The long-term availability of this framework is ensured by hosting it in the infrastructure of the TDL association (trust in digital life). TDL was founded by leading industry partners and knowledge institutes within the European Union and is already hosting the results of many EU projects (see Section 4.5 for further details on sharing results via TDL).

**Activity 2**

On top of the TREDISEC framework, the partners have developed several primitives that are exploited by the respective technology owners individually.

Activities to encourage further development of innovation on top of the framework by former consortium members but also by external stakeholders will be discussed and planned by the board.

To facilitate the pick-up of technology the board will work towards eliminating technical and legal obstacles.

This includes a strategy towards standardization of the TREDISEC platform. In IT-Services many standards come as de facto standards set by the key partners in the industry. For this to be successful the TREDISEC platform and further developments will be discussed within the board. A key role will also be the wider TDL community involving leading European stakeholders, where the TREDISEC partners bring the TREDISEC platform to discussions and presentations in the working groups. But also the standardization activities of established standardization organizations in the area, e.g. IETF, ETSI, is monitored and when suitable joined. Several partners are active in the organisations in various areas already. Besides standardization of the platform and innovations, it is a goal of the partners that solutions based on TREDISEC stand out, e.g. by obtaining a suitable certification.

The board will decide on the terms and conditions for the exploitation of the common TREDISEC results. The board will furthermore coordinate technical support and intellectual property within the consortium in a timely manner and also when interest of external customers or organizations interesting in exploiting results arises.

**Activity 3**

TREDISEC shows innovative ways to raise the security of the cloud infrastructure. The project results also aim at application developers that can utilize the developed API to provide a security-by-design approach for the development of secure distributed applications.

Unfortunately, still security and privacy are commonly only of secondary concern for both the developers of products and services and also for their consumers. Therefore education and training plays an important role in the sustainability strategy.

The new European GDPR comes in time to support the awareness and increase the importance of technical security measures for IT products and services. The industrial partners use the pilots developed in the project for internal education and awareness but also for a wider education of the community at industrial exhibitions and events.

The academic partners of the consortium use project results and experience gained through the project for the education of the next generation of developers, a wider academic community and the public. The board is used to discuss and share experiences and approaches among the partners.

TREDISEC has already achieved high visibility within the security and privacy academic community by publications and presentations in top-tier journals and conferences. This facilitates further development of the fundamental technology and consideration by a wider security research community worldwide.
**Activity 4**

The partnerships built during the project life time would remain active after the end of the project through meetings called on demand. Many of the partners of the consortium are also active in the TDL association.

Further collaboration beyond the life-time of the project may lead to industrial and commercial cooperation or further cooperation in internally or externally funded R&D projects that pick up technology from TREDISEC and develop it further for future needs, therefore contributing to the impact of TREDISEC.

### 6.1.1 Exploitation Board and Contacts

The following table shows the contact points corresponding to each of the project consortium partners. The Exploitation Board will use a distribution mailing list as unique contact point to externals where all members of the board are members: tredisec-eb@lists.atosresearch.eu

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Contact (Name)</th>
<th>Role</th>
<th>Responsibilities</th>
<th>Email</th>
<th>Telephone Number</th>
<th>Address</th>
<th>Backup Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arsys Internet, S.L.U.</td>
<td>David Vallejo</td>
<td>Head of PMO</td>
<td>Leading a group of project managers in charge of international projects</td>
<td><a href="mailto:dvallejo@arsys.es">dvallejo@arsys.es</a></td>
<td>+34902261 526</td>
<td>C/Chile 54, Logroño, 26007, Spain</td>
<td>Miguel Ángel Pérez</td>
</tr>
<tr>
<td>Atos</td>
<td>Pedro Soria-Rodriguez</td>
<td>Head of Market</td>
<td>Management of R&amp;I operations and Bid Manager</td>
<td><a href="mailto:pedro.soria@atos.net">pedro.soria@atos.net</a></td>
<td>-</td>
<td>C/Albarracín 25 Madrid</td>
<td>Rodrigo Díaz</td>
</tr>
<tr>
<td>ETH</td>
<td>Kari Kostiainen</td>
<td>Senior Scientist</td>
<td>Management of TREDISEC primitives. Development of TREDISEC primitives.</td>
<td><a href="mailto:kari.kostiainen@inf.ethz.ch">kari.kostiainen@inf.ethz.ch</a></td>
<td>+41446328 384</td>
<td>Universitätstrasse 6 8092 Zürich Switzerland</td>
<td>Srdjan Capkun</td>
</tr>
<tr>
<td>EURECOM</td>
<td>Refik Molva</td>
<td>Profesor &amp; Head of the Digital Security Department</td>
<td></td>
<td><a href="mailto:refik.molva@eurecom.m.fr">refik.molva@eurecom.m.fr</a></td>
<td>+33493008 112</td>
<td>EURECOM, Campus SophiaTech, 450, Route des Chappes, CS 50193, 06904 Biot Sophia-Antipolis, Cedex, France</td>
<td>Melek Önen</td>
</tr>
<tr>
<td>GRNET SA</td>
<td>Georgios Tsoukalas</td>
<td>TREDISEC GRNET Lead, Design and Develop</td>
<td>Handle requests on TREDISEC framework</td>
<td><a href="mailto:gtsouk@admin.grnet.gr">gtsouk@admin.grnet.gr</a></td>
<td>+30210747 4464</td>
<td>Kifissias Ave 7, Athens, Greece</td>
<td>Aristeidis Sotiropoulos</td>
</tr>
</tbody>
</table>
6.2 TREDISEC Long Term Sustainability & Impact

At a high level, TREDISEC intended to tackle three of the main barriers limiting the widespread adoption of cloud services: Security & Data Protection, Trust, and Data Access & Portability. To overcome these barriers, TREDISEC specifically aimed to improve the reliability of two fundamental aspects of cloud computing environments, namely storage and computation, while supporting highly desired features such as multi-tenancy and deduplication. A major challenge in the context of cloud security stems from the fact that, in a cloud environment, resources like storage, computation, and even the network itself, are inherently shared. This peculiarity of the cloud setting opens the door to new vulnerabilities and security issues.

Mindful of the obstacles and challenges to the widespread adoption of cloud services, TREDISEC envisioned the opportunity to pioneer the development of security and privacy solutions for the cloud. In order to reach this ambitious goal, the TREDISEC consortium conducted a synergetic activity encompassing research, development, and deployment of cloud technology and embracing the whole process of design, validation, and dissemination of security innovations.

Broadly, the technology and products developed within TREDISEC have been conceived to positively shift the public’s perception of outsourced services as well as to enhance the security (and hence the competitiveness) of European businesses. More specifically, the results targeted by TREDISEC were
meant to have particular impact in the following dimensions (where IP stands for Impact Point), as implicitly indicated in the original project proposal of TREDISEC:

**IP1.** Design solutions compliant with European Security and Privacy regulation.

**IP2.** Empower users to take control over their data and trust relations.

**IP3.** Improve the protection of users’ privacy.

**IP4.** Increase users’ trust in ICT and online services.

**IP5.** Strengthen the security and privacy of European products.

**IP6.** Bring technology to practice via pre-product development and testing with end-users.

**IP7.** Devise security primitives that require minimum modifications to existing paradigms.

**IP8.** Increase the level of security and/or privacy at marginal additional cost.

**IP9.** Create technology that will impact existing businesses and will generate new ones.

As we elaborate in the rest of this section, the innovations created in the course of the project successfully achieved all of the above objectives. The TREDISEC primitives provide novel functionalities which enable/enhance security while preserving efficiency, thus offering the best trade-off between security and availability.

As a first step towards achieving the above goals, the consortium invested particular effort in identifying the conditions and prerequisites for the large-scale adoption of cloud services and developing adequate solutions.

One such prerequisite is concerned with protecting the data of customers. We pointed out already in previous sections of this document that concerns about data loss/exposure are one of the main obstacles to the adoption of outsourced services. In fact, currently deployed security solutions for the cloud are not able to support both strong security and resource-efficient features (such as deduplication and multi-tenancy) simultaneously. TREDISEC addresses this problem with dedicated solutions offering security-by-design without compromising the unique efficiency properties of cloud environments.

The novel TREDISEC functionalities such as deduplication over encrypted data and proofs of retrievability (just to mention a few) do offer a cutting edge over existing solutions. These functionalities pave the ground for commercial products and services which not only are compliant with the European security and privacy regulations (IP1) but also improve the user’s privacy and data security in a verifiable matter (IP2 and IP3). This has been demonstrated by the numerous end-user feedbacks that were acquired from questionnaires and through the various exploitations activities carried out by consortium members.

We argue that the dissemination of TREDISEC’s privacy-preserving and verifiable solutions for the cloud will undoubtedly increase the user’s trust in cloud providers (IP4), positively affecting the public’s perception of outsourced services, and consequently support the cloud business as well as technological innovation.

Protecting the privacy of users has always been a primary goal of the consortium. The strong focus on privacy is even more evident from the end-to-end security achieved by the TREDISEC solutions which empower users of cloud services to take control over their data as well as their metadata. We emphasize that enhancing security and privacy for users is part of the Digital Single Market (DSM) strategy, identified as one of the ten political priorities of the European Commission [17]. The DSM regulates the conditions for individual and businesses to access online services and targets specifically data protection of users. Thus, the technology created by TREDISEC is capable to strengthening the security and privacy of European enterprises (IP5), to positively impact their businesses, and to sustain new and prosperous business directions in cloud security.
The successful outcome of the project was contributed by leading researchers with proven track record in recognized conferences and journals as well as renowned ICT companies and specialized enterprises with established markets and successful history of product business.

As demonstrated by the strong focus on industry, TREDISEC intended to offer beyond research innovations also a pragmatic approach to turn research results into practice and bring them to the market through the evaluation and feedback of real end-users. The involvement of leading cloud providers in the market such as GRNET, ARYSYS, NEC, ATOS, IBM, and SAP, was not by chance but rather a meditated choice. One of the project activities that proved to be extremely successful for the actual development and deployment of the TREDISEC solutions was indeed the active collaboration with industry, which allowed the partners to test products and prototypes, to obtain early feedbacks from end-users, and hence to greatly improve the solutions (IP6).

The immediate consequence of such collaborative effort is a technology truly capable to strengthen the security and privacy of European cloud services. All in all, the technology brought by TREDISEC offers security-by-design in a strong and realistic adversarial model, thus providing European enterprises with techniques and tools to protect themselves from surveillance, but also loss or exposure of sensitive data.

Another important aspect of cloud computing, and a prerequisite for the large-scale adoption of this technology, is that it offers a concrete opportunity to save energy and resources. Cloud services are typically purchased on a pay-as-you-go basis which incentivizes users to consume no more than what is actually needed. Further, they also enable multi-tenancy letting different individuals and/or enterprises to share the same cloud infrastructure, which again leads to remarkably decreasing the use of physical resources (in particular energy) and associated costs. The novel functionalities developed by TREDISEC contribute a fortiori to the saving of resources and costs by preserving the above-mentioned features of cloud computing and additionally enabling storage-efficient solutions on top of them. Given this, we argue that the solutions put forth by TREDISEC, beyond generating business and fostering the adoption of cloud services, also offer a more sustainable technology.

It is worth noting that the adoption of energy-efficient cloud technology is in line with the United Nations 2030 Agenda and corresponding Sustainable Development Goals (SDGs), adopted by the European Union as well, on Affordable and Clean Energy, Industry Innovation and Infrastructure, and Climate Action (SDGs 7, 9, and 13) [18].

Last but not least, TREDISEC dedicated particular effort to devising appropriate security and privacy primitives that only require minimal modifications of deployed cloud services (IP7). All of the TREDISEC security primitives were specifically designed to be integrated into existing cloud infrastructures in a lightweight and cost-efficient manner through the unified TREDISEC framework, making the adoption of the new technology particularly easy for customers. Thus, enterprises will benefit from both increased efficiency and lower costs, and hence will be encouraged to augment their business (IP8). At the same time, customers will be able to use cloud services without fearing to lose their data or sacrifice privacy (IP2-IP4). All these factors will contribute to expand the cloud security market, leading to a platform for technology development and job creation.

It is also worth noting that all the technologies developed in Tasks 4.3 and 5.1 are compliant with the upcoming GDPR regulations that are expected to be enforced in May 2018. The latter appears to be an appealing feature given the evident difficulties faced (and perceived) by enterprises to modernize their IT infrastructure in this regard [19] (see also Figure 60 and Figure 61) as well as the estimated costs for compliance (c.f. [20]). At all times, the Innovation director, the project coordinators and the Scientific director were constantly monitoring the market evolution.
More specifically, the use of primitives such as Bastion, PerfectDedup, Multi-tenant encrypted databases, ClearBox, ensure compliance with the GDPR regulations by enforcing end-to-end security without compromising functional requirements in existing clouds. **This allows existing cloud businesses to easily support the changing regulations in the European market without compromising their profitability.**
The technology created by TREDISEC is capable to positively impact existing businesses, in particular European cloud providers, through the deployment of robust security and privacy features and is likely to foster new business areas even after the termination of the project (IP9). IP9 is further strengthened by the fact that one of the main outputs of the TREDISEC project, which is the framework, will be available as open source for the entire community and will be shared through industry forums, such as TDL, for an indefinite amount of time. This would allow existing businesses and European cloud providers to benefit from TREDISEC by incorporating the TREDISEC platform within their offerings.
7 Conclusion

The present document summarizes the plan and activities undertaken by the consortium for the exploitation of the results achieved by TREDISEC, with particular focus on their business impact and commercial value.

The report includes an overview of the common exploitation strategy, a thorough analysis of the current cloud market, a business model for the exploitation of the TREDISEC innovations, a detailed report on all the exploitation strategies pursued by the individual partners, and a long-term sustainability strategy to ensure the continuous impact of results and innovations long after the termination of the project.

The main goal pursued by TREDISEC is the development of appropriate technology to encourage the adoption of cloud-based products and services among enterprises and individuals. The results of the project provide cutting-edge solutions that offer novel security as well as efficiency features, leading to appealing products for the current and future cloud business.

It is evident from the analysis of the current market that the innovations generated by TREDISEC offer competitive security solutions for the current cloud business. The deployment of products and services supporting the security features and novel functionalities designed within TREDISEC will allow enterprises to offer efficient and secure services at contained costs and, at the same time, will help increasing the customers' trust on outsourced services.

By enabling secure cloud computing and enhancing the privacy of users, the technology created by TREDISEC is truly capable of enriching existing business as well as creating new and prosperous business opportunities.

In addition to the development and dissemination of high-impact solutions for the cloud market, TREDISEC is strongly committed to ensure that the project’s results will generate business impact and be exploitable in the long run.
8 Bibliography

Appendix I Questionnaire for Validation of TREDISEC results

8.1 Professional Profile

1. How would you describe your profile background?
   - [ ] Software developer
   - [ ] Software architect, analyst
   - [ ] IT consultant

2. Which technologies do you work with?
   - [ ] Cloud
   - [ ] Cybersecurity
   - [ ] Data Intelligence
   - [ ] Identity & Privacy
   - [ ] IoT
   - [ ] Others

3. In which sector/field would you place the clients/users of the technologies that you produce?
   - [ ] Financial Services
   - [ ] Public Sector
   - [ ] Telecom
   - [ ] Health
   - [ ] Information Technology
   - [ ] Energy
   - [ ] Environment
   - [ ] Homeland Security & Defence
   - [ ] Manufacturing & Retail
   - [ ] Media
   - [ ] Transport

If you wish to receive the conclusions of the analysis that we will perform over all the questionnaire responses received, please, enter a valid e-mail address here:

[ ] I also wish to receive other regular updates on the project progress and results
8.2 General/Background

Q1. How often do you use Cloud technologies?

<table>
<thead>
<tr>
<th></th>
<th>Very often</th>
<th>Often</th>
<th>Every now and then</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q2. How would you judge your knowledge of Cloud technologies?

<table>
<thead>
<tr>
<th></th>
<th>Global Expert</th>
<th>Power User</th>
<th>Experienced Still learning</th>
<th>Beginner</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q3. When using the Cloud…

<table>
<thead>
<tr>
<th></th>
<th>Always</th>
<th>Frequently</th>
<th>Occasionally</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you feel you have control over the data stored in the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you worried about the security of the data stored in the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you feel the services/applications running in the Cloud are protected against security threats?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q4. Would you find it useful to have solutions that mitigate the issues outlined in Q3?

<table>
<thead>
<tr>
<th>Extremely useful</th>
<th>Very useful</th>
<th>Useful</th>
<th>Somehow useful</th>
<th>Not at all useful</th>
</tr>
</thead>
</table>

Q5. Do you think that such solutions would enhance your business capabilities?

<table>
<thead>
<tr>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
</table>
8.3 TREDISEC TECHNOLOGIES: SECURITY PRIMITIVES

Q6. TREDISEC primitives are a suite of cloud security technologies for the cloud that solves issues outlined in Q3.

a. Have you heard about them?

<table>
<thead>
<tr>
<th>Confidentiality with Storage Efficiency</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with Multitenancy</td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Data Processing</td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Integrity with Cloud Efficiency</td>
<td></td>
</tr>
</tbody>
</table>

b. If Yes to a), have you tried them?

<table>
<thead>
<tr>
<th>Confidentiality with Storage Efficiency</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with Multitenancy</td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Data Processing</td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Integrity with Cloud Efficiency</td>
<td></td>
</tr>
</tbody>
</table>

c. If Yes to a), how would you rate them with respect to?

<table>
<thead>
<tr>
<th>Excellent</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>Very Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making you feel more in control of your data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Making you less worried about the security of your data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Making you feel your services/applications running in the Cloud are protected against security threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Making you feel your data and services/applications are secure without significant impact in performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q7. TREDISEC primitives are a suite of security technologies for the cloud that differ from other solutions in the area by supporting Cloud functional characteristics such as deduplication, multi-tenancy or high performance computation. How important is this feature for the technologies that you produce?

<table>
<thead>
<tr>
<th>Extremely Important</th>
<th>Important</th>
<th>Somewhat important</th>
<th>Nice to have</th>
<th>Don’t care</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q8. Do you think that TREDISEC primitives would enhance the technologies that you produce?

<table>
<thead>
<tr>
<th></th>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with Storage Efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality with Multitenancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Data Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Integrity with Cloud Efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q9. If the TREDISEC primitives were made available how often would you use them in the technologies that you produce?

<table>
<thead>
<tr>
<th></th>
<th>Very often (in every piece of technology that I produce)</th>
<th>Often (in the majority of the technologies)</th>
<th>Regularly (in many of the technologies)</th>
<th>Rarely (only in some with very specific security requirements)</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with Storage Efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality with Multitenancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Data Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Integrity with Cloud Efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.4  TREDISEC TECHNOLOGIES: FRAMEWORK

Q10. Imagine you have an assignment to produce a technology, with security and cloud functional and non-functional requirements to meet.

<table>
<thead>
<tr>
<th></th>
<th>Always</th>
<th>Frequently</th>
<th>Occasionally</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you find it easy to find solutions that meet your security requirements?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you find it easy to find security solutions that also meet cloud functional and non-functional requirements?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have access to information on how the solution performs in multiple cloud-based environments?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have the opportunity to test by yourself the solution (functionalities, performance) in your own configured cloud-based environment?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have the option to automatically (or semi-) deploy the solution in a specific cloud-based environment (e.g. via scripts, docker, vagrant)?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have access to different versions of the same solution pre-configured and/or adapted to work in multiple cloud-based settings (i.e. Recipes)?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q11. If a framework which supports the features listed in Q10, was available, how likely would you use it?

<table>
<thead>
<tr>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
</table>

Q12. How often would you use that framework?

| Very often (several times a month) | Often (once a month) | Regularly (more than 6 times a year) | Rarely (5 or less times a year) | Never |
Q13. Do you think such framework would enhance your productivity?

<table>
<thead>
<tr>
<th>Extremely</th>
<th>Greatly</th>
<th>Moderately</th>
<th>Somewhat</th>
<th>Not at all</th>
</tr>
</thead>
</table>

[Response goes here]
Q14. TREDISEC provides a framework that solves the issues outlined in Q10.

a. Have you heard about it?  
   
   Yes/No

b. If Yes, Have you tried it?  
   
   Yes/No

c. If Yes to b), which features of the framework do you value the most?

<table>
<thead>
<tr>
<th>Framework Feature</th>
<th>Extremely useful</th>
<th>Very useful</th>
<th>Useful</th>
<th>Somehow useful</th>
<th>Not useful at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>The repository of cloud security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for searching cloud security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for testing functional and non-functional aspects of the solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for creating/linking cloud testing environments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for deployment cloud security solutions in a virtual environments offered by the framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for deployment cloud security solutions in a virtual environment linked to the framework but owned by the user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedback received from the use and testing of cloud security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support uploading own recipes in the framework and make them available for the community (for promotion, testing, validation and use)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guidelines for search, test and use of TREDISEC primitives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provided information when using and managing the TREDISEC primitives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for controlling access to different tenants and users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options for configuring the framework (administrative GUI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q15. Which specific features of the TREDISEC framework are you missing that would help you in your daily work? (Open question)
8.5 TREDISEC BUSINESS MODEL

Q16. According to your own profile and what you learnt from the presentation, which channel do you consider more suitable to reach customers of the TREDISEC outcomes?

<table>
<thead>
<tr>
<th>Customers</th>
<th>Online</th>
<th>Field Sales Force</th>
<th>Other (Which one?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To reach you</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To reach your organization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q17. The TREDISEC framework, among other features, is a central repository of security and functional solutions for the Cloud that also permits testing and deploying (in an automatic, semi-automatic or manual way) these solutions in a cloud-based testing environment before actually downloading/installing/integrating those in the target cloud systems. How important is this feature for you?

<table>
<thead>
<tr>
<th>Extremely Important</th>
<th>Important</th>
<th>Somewhat Important</th>
<th>Nice to have</th>
<th>Don’t care</th>
</tr>
</thead>
</table>

Q18. How likely is it that you will prefer looking for cloud security solutions for the cloud in the TREDISEC framework over other repositories or marketplaces?

<table>
<thead>
<tr>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
</table>

Q19. How likely is that you will prefer TREDISEC primitives over other solutions …

<table>
<thead>
<tr>
<th>If offered Open Source?</th>
<th>Extremely Likely</th>
<th>Very Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>If offered for free?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you had to pay for them?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q20. How likely is that you will consider paying for TREDISEC primitives …

<table>
<thead>
<tr>
<th>If you have the chance to try them before purchasing (trial version, freemium version)</th>
<th>Extremely Likely</th>
<th>Very Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are offered a suite of primitives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
where some primitives are free while others are licensed

If the licensed primitives are customized to your own needs (e.g., specific cloud settings, special features)

If the licensed primitives are offered together with complementary services (i.e., training, installation/configuration, updates/maintenance, etc.)

Q21. Which complementary services would you consider more interesting?

<table>
<thead>
<tr>
<th>Options</th>
<th>Extremely interesting</th>
<th>Interesting</th>
<th>Somehow interesting</th>
<th>Nice to have</th>
<th>Don't care</th>
</tr>
</thead>
<tbody>
<tr>
<td>TREDISEC framework installation &amp; configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Primitives installation &amp; configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance: updates &amp; support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customization of solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultancy for new cloud security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Which others would you propose?

Q22. How likely is that you will recommend TREDISEC to your peers

<table>
<thead>
<tr>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q23. How likely is that you will recommend TREDISEC to your upper management

<table>
<thead>
<tr>
<th>Extremely likely</th>
<th>Likely</th>
<th>Probably</th>
<th>Likely not</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix II  

ARSYS’ Questionnaire for Large Companies

Online survey of the European Project TREDISEC on Information Security on the Cloud.

TREDISEC offers a set of end-to-end security modular primitives that cover all the significant technical requirements for the Cloud, ensuring that services provided are not affected. These security primitives are managed and deployed through a unified framework, which ensures that primitives comply with relevant quality standards. TREDISEC solutions will help companies and organizations to meet customer security requirements, as well as with their own, without additional storage or computing costs, and with negligible performance reduction.

1) How would you describe your customers’ profile? (checkbox)
   a) Software developer.
   b) Software architect.
   c) Testing/deployment engineer.
   d) Project Manager.
   e) Work in Sales or Marketing.

2) Which technologies do they usually work in? (checkbox)
   a) Cloud.
   b) Cybersecurity.
   c) Data intelligence.
   d) Internet of Things (IoT).

3) In which sector would you locate technology users in which your customers work? (checkbox)
   a) Finance.
   b) Energy.
   c) Public Administration.
   d) Environment.
   e) Telecommunications.
   f) Defence.
   g) Health.
   h) Industry.
   i) IT.
   j) Media.
   k) Transport.
4) How often do your customers use the Cloud? (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Very often</th>
<th>Often</th>
<th>Every so often</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5) How would you assess your customers’ knowledge on the Cloud? (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Expert</th>
<th>Advanced user</th>
<th>Average user</th>
<th>Beginner</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6) While using the Cloud, your customers… (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Always</th>
<th>Often</th>
<th>Sometimes</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do they feel they have control over data stored on the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are they concerned about the security of data stored on the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are they concerned about the integrity of data stored on the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are they concern about the confidentiality of data stored on the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do they feel that services/applications running on the Cloud are protected against security threats?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7) TREDISEC primitives are a set of security technologies for the Cloud that solve the issues described in question no. 6. Please indicate below whether you have heard about the following primitives. (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with storage efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality with multi-tenancy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality and data processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability and integrity with Cloud efficiency</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8) TREDISEC primitives differ from other security solutions by offering features such as deduplication, multi-tenancy and high-performance computing. How important are these functionalities for your customers? (radio button)
   a) Extremely important.
   b) Important.
   c) Somehow important.
   d) Non-essential.
   e) Not important.
9) Do you think that TREDISEC primitives could contribute to the improvement of your customers’ products? (matrix)

<table>
<thead>
<tr>
<th>Confidentiality with storage efficiency</th>
<th>Very likely</th>
<th>Likely</th>
<th>Unlikely</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality with multi-tenancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality and data processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability and integrity with Cloud efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10) Please answer the following questions from your customers’ standpoint. (matrix)

<table>
<thead>
<tr>
<th>Always</th>
<th>Often</th>
<th>Sometimes</th>
<th>Rarely</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you find it easy to get solutions that meet your security requirements?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you find it easy to get security solutions that also meet the efficiency requirements of the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have access to information about how these solutions work in multi-cloud environments?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have the opportunity to try these solutions on your own platform on the Cloud?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have the option to automatically (or almost) deploy these solutions through scripts, Docker or Vagrant?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11) TREDISEC is a framework that solves the issues listed in question no. 10. How would your customers evaluate the following framework functionalities? (matrix)

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Extremely useful</th>
<th>Very useful</th>
<th>Useful</th>
<th>Little useful</th>
<th>Useless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository of Cloud security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support to look for security solutions on the Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support to test functional and non-functional aspects of security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support to deploy security solutions in a virtual environment provided through the framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support to deploy security solutions in a virtual environment linked to the framework, but owned by the user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12) What other features would you add to TREDISEC that could facilitate your customers’ daily work? (open question)

13) According to your customers’ profile, which sales channel do you consider most suitable for the commercialization of TREDISEC? (checkbox)
   - a) Corporate website and social networks.
   - b) Telesales: telephone calls and/or webinars.
   - c) Visits of specialized sales agents.
   - d) Marketplaces (Amazon, Azure, Google, FIWARE, etc.).

14) TREDISEC framework is a central repository of Cloud security solutions that also allows to test and deploy these solutions beforehand in a cloud-based test environment. How important is this functionality for your customers? (radio button)
   - a) Extremely important.
   - b) Important.
   - c) Somehow important.
   - d) Non-essential.
   - e) Not important.
15) How likely is it that your customers would prefer the TREDISEC framework over other repositories or marketplaces? (radio button)
   a) Very likely.
   b) Likely.
   c) Unlikely.
   d) None.

16) What is the likelihood of that your customers would consider paying for the TREDISEC primitives? (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Very likely</th>
<th>Likely</th>
<th>Unlikely</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>If they would have the opportunity to try them before purchase (trial version, freemium version)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If they would be offered a set of primitives in which some are free and others require a licence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If the licensed primitives would be customizable according to their own needs (for example, specific Cloud settings, special features)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If the licensed primitives would be offered along with complementary services (i.e. training, installation/configuration, updates/maintenance, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17) What complementary services would your customers consider most interesting? (matrix)

<table>
<thead>
<tr>
<th></th>
<th>Very interesting</th>
<th>Interesting</th>
<th>Non-essential</th>
<th>Without interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation and configuration of TREDISEC framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation and configuration of security primitives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance: updates and support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customization of solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultancy for new security solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
18) What other services would your customers like to have? (open question)

19) Would you recommend TREDISEC to other sales agents? (radio button)
   a) Very likely.
   b) Likely.
   c) Unlikely.
   d) No.

20) Would you recommend TREDISEC to your line managers? (radio button)
   a) Very likely.
   b) Likely.
   c) Unlikely.
   d) No.
Appendix III  ARSYS’ Questionnaire for SMEs

Online survey of the European Project TREDISEC on Information Security on the Cloud.

1) What is your main professional activity? (dropdown menu)
   a) I work in a large company.
   b) I work in a medium-sized company.
   c) I work in a small company.
   d) I am self-employed.
   e) I work for the Government.

2) What is your knowledge/experience in Information Technology? (radio button)
   a) I use computers, smartphones and tablets regularly, but my technical knowledge is limited.
   b) I consider myself a mid-level or advanced user, but I don’t work in the IT sector.
   c) General knowledge and experience in the IT sector.
   d) IT Technician: developer, system administrator, network administrator, etc.

3) Have you heard about the GDPR, when will it be launched and what does it entail? (radio button)
   a) No, it is the first time that I read the acronym GDPR.
   b) Yes, I've heard about it, but I don’t know how it affects me.
   c) Yes, I know the regulation, when it starts up and its repercussions.

(to be shown after answering the previous question)

The General Data Protection Regulation (GDPR) aims to create a harmonised legal data protection framework throughout the European Union, with the aim of returning control over citizens' personal data by imposing at the same time strict rules about who will host and process this data, anywhere in the world. The regulation also presents rules concerning the free circulation of personal data inside and outside the European Union. It is expected to enter into force on May 25th, 2018.

4) Please indicate below your degree of concern regarding the preparation of your organisation to comply with the GDPR. (radio button)
   a) Low concern. We have a defined Implementation Plan and it is being executed.
   b) Average concern. We don't have a roadmap, but we are considering hiring the services of a specialised consultancy firm.
   c) High concern. We haven’t yet proposed any action to comply with the regulation.
5) Would you be interested in a webinar about GDPR?  
   a) Yes. 
   b) No.

6) Do you know TREDISEC? (radio button) 
   a) Yes. 
   b) No. 
   (to be shown after answering the previous question) 
   TREDISEC is a European R&D Project, whose ambition is to develop systems and techniques that make the Cloud a secure and efficient place to store data. Based on existing cryptographic protocols and through the development of new algorithms, the consortium aims to create a single framework that harmonises and facilitates the implementation of information security solutions.

7) Do you know what secure deletion is? (radio button) 
   a) No, I hadn't heard it before. 
   b) Yes, it's about the elimination of data stored on the Cloud so that it cannot be recovered in any way.

8) Is your organisation interested in the secure deletion? (radio button) 
   a) Yes. 
   b) No. 
   c) I don't know.

9) One of the improvements offered by TREDISEC is the confidentiality of the files combining encryption and compression. Would you implement this improvement in your organisation? (radio button) 
   a) This is IT department's responsibility. 
   b) This depends on an external company. 
   c) Yes, we could reduce the storage space without sacrificing the privacy of information.

10) Please indicate below the IT security measures which are implemented in your organisation. (checkbox) 
   a) Logical access controls to access IT systems. 
   b) Backup system for the information stored in workstations and/or servers. 
   c) Encryption of internal and/or external storage. 
   d) Cloud storage. 
   e) Secure deletion of content. 
   f) Management systems for mobile devices: laptops, smartphones, tablets, etc. 
   g) Antivirus, firewall or proxy. 
   h) Remote connections through Virtual Private Networks.

11) If your organisation uses storage on the Cloud, do you have any software installed to guarantee that the recovered data has not been corrupted in the download process? (radio button) 
   a) I don't know. 
   b) No. 
   c) Yes.

12) Would your organization be interested in adding different levels of granularity to permissions and user groups for data stored on the Cloud? (radio button) 
   a) I don't know. IT department or external company is responsible for this. 
   b) We don't use Cloud storage. 
   c) No, I don't think so. 
   d) Yes, it may be interesting.
13) How were those solutions implemented? (radio button)
  a) IT technicians followed recommendations from specialised forums.
  b) The IT Security department implemented solutions from a marketplace (Amazon, Azure, Google, FIWARE, etc.).
  c) The IT Security department implemented standard solutions.
  d) They were outsourced to a specialised company.
  e) I don’t know.

14) Regarding the contracting of IT security services, which one do you prefer? (radio button)
  a) Initial single payment.
  b) Half-yearly or annual payment.
  c) Pay per use.

15) Does your organisation use IT security solutions developed in open source? (radio button)
  a) I don’t know.
  b) No, we use proprietary solutions.
  c) Yes, but in a minority way.
  d) We use both proprietary and open source solutions.
  e) Yes, we only use open source solutions.

Appendix IV Definitions and Main Applications

Cloud Access Security Brokers
Cloud access security brokers (CASBs) are on-premises or cloud-based security policy enforcement points, placed between cloud service users and providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, data security (content inspection, encryption, tokenization), logging, alerting, and malware detection/prevention. CASBs are uniquely positioned to enable organizations to achieve consistent security policies and governance across a range of cloud services. Unlike traditional security products, CASBs are designed to protect your data that’s stored in someone else’s systems.

Cloud Data Backup
Cloud data backup refers to policy-based backup tools that can back up and restore production data generated natively in the cloud. As more production workloads migrate to the cloud (either in the form of SaaS or IaaS), it has become critical to protect data generated natively in the cloud. SaaS and IaaS providers typically offer infrastructure resiliency and availability to protect their system from a site failure. However, when data is lost due to their infrastructure failure, the providers are not financially responsible for the value of lost data and only provide limited credit for the period of downtime. When data is lost due to user errors, software corruption or malicious attacks, user organizations are fully responsible themselves. The more critical cloud-generated data is, the more critical it is for users to provide recoverability of such data.

Cloud Data Protection Gateways
Cloud data protection gateways (CDPGs) may deploy a combination of forward or reverse proxy and
API, applying encryption, masking or tokenization to structured or unstructured data as it flows through the gateway to the cloud SaaS provider. CDPG functionality is also provided by several cloud access security broker (CASB) products. It prevents unauthorized access by application users, other cloud tenants, SaaS administrators and bad actors into the cloud service, and helps meet data residency requirements when using SaaS.

Cloud Infrastructure Security Posture Assessment
Cloud infrastructure security posture assessment (CISPA) offerings analyze the correct and secure configuration of the control plane infrastructure of public cloud services, typically for IaaS, but could also be applied to PaaS and SaaS services. For example, CISPA offerings analyze identity and access management (IAM) accounts, privileges, network connectivity, network configuration and storage configuration.
CISPA offerings help information security leaders gain confidence and assurance that the setup and configuration of their cloud services is implemented securely.

Cloud Management Platforms
Cloud management platform (CMP) tools enable organizations to manage private, public and multi-cloud cloud services and resources. Their specific functionality addresses three key management layers: access management, service management and service optimization.
Management services include accessing/requesting cloud services, and provisioning and managing them to defined SLAs. Optimization supports the orchestration and automation of cloud services, as well as the underlying infrastructure resources, in accordance with defined policies. Enterprises will deploy CMPs to increase agility, reduce the cost of providing services and increase the likelihood of meeting service levels.

Cloud Security Assessments
The buyers and sellers of public cloud services need standardized ways to assess provider security and continuity. Formal assessments are performed by authorized independent evaluators, who use published control standards and process guidelines to evaluate service provider security posture, and publicly share their findings.

Container Security
Container security is the application of security processes, testing and controls to Linux container-based environments. Container security starts in development with an assessment of the risk and the trust of the entire contents of the container and should extend into runtime threat protection and access control to containers when in production.
OS containers are not inherently unsecure, but are being deployed insecurely, driven by developers and a need for agility in service development and deployment. Security and risk management leaders must address container security issues around vulnerabilities, visibility, compromise and compliance.

Cloud-Testing Tools and Services
Cloud-testing tools and services involve the use of cloud technology to support testing from or in the cloud. This includes cloud-based lab management, service virtualization, on-demand delivered testing tools and device clouds. This term also covers support for large-scale load and performance tests, strong technology coverage (middleware, message formats, security protocols, etc.) and the ability to work across applications using a mixture of technologies.

Cloud Workload Protection Platforms
The market for cloud workload protection platforms (CWPPs) is defined by host-centric security
Digital Security

Digital security is the practice of assuring trust, safety and reliability to digital ecosystems. The systems addressed includes operational technology (OT), cyber-physical system security (CPSS) and the Internet of Things (IoT). Systems include devices, networks, communications, applications and data in business, government and society that are part of digital business initiatives. Digital security controls create trust and provide safety, reliability, privacy and resiliency for the digital infrastructure supporting those initiatives.

Data Loss Prevention

Data loss prevention (DLP) is the dynamic application of a policy based on the content and context at the time of an operation. DLP addresses the risks of inadvertent or accidental data loss, and the exposure of sensitive data using monitoring, filtering, blocking and remediation features.

IaaS Container Encryption

Infrastructure as a service (IaaS) container encryption is the use of encryption within workloads hosted by IaaS providers (including those using containers) to encrypt data at rest stored by the workload in the IaaS provider's infrastructure in an application-neutral way. By controlling access to the decryption keys, organizations are able to protect the data used and created by IaaS workloads from adjacent tenants, cloud service provider administrators and potential hackers of the IaaS provider.

Identity-Proofing Services

Identity-proofing services validate or corroborate an individual’s identity claim to enable an organization to: issue the person a new account or credentials, allow an individual to conduct a potentially high-risk transaction, or revalidate identity required to address high-risk and anomalous transactions. These services have historically relied on aggregated PII data from public or proprietary sources. More recently, they have encompassed non-PII data sources and include risk analysis based on multiple identifying attributes.

High-Assurance Hypervisors

A high-assurance hypervisor is a hypervisor that establishes a high level of trust that it is hardened, has not been tampered with or compromised. Once high assurance of trust is established, mission-critical workloads and sensitive data are provided a high level of confidence from the platform underneath.

KMaaS

Key management as a service (KMaaS) solutions are deployed within public cloud infrastructure as a service (IaaS). These can be software appliances or hardware security modules (HSM) that provide encryption key management and even bring your own key (BYOK) and enable data access control policies. They may be provided by third parties or natively by the cloud service provider (CSP).
Micro-segmentation (Software-Defined Segmentation)

Micro-segmentation (referred to as software-defined segmentation in previous Hype Cycles) uses policy-driven firewalling (typically software-based) or network cryptography to isolate workloads in data centers and public cloud infrastructure as a service, and into containers, including workloads in hybrid and multi-cloud scenarios spanning all of these.

OAuth 2

The OAuth 2 authorization framework orchestrates approval and accesses interactions between client programs, which may represent a user and an application, thus making it possible to grant third-party applications limited access to resources on behalf of end users. The OAuth 2 authorization framework separates the access request from the resource being requested. This allows an independent authorization service to manage access independently of client programs such as mobile or web apps.

Applications that invoke embedded browsers can use proprietary authentication methods and SAML federation protocols. However, use of standard authentication and authorization capabilities could help enterprises avoid lock-in for any given access method. OAuth will be relevant as a method of supporting authorization for a variety of use cases and applications.

Private Cloud Computing

Private cloud computing is a form of cloud computing used by only one organization or one that ensures an organization is completely isolated from others. As a form of cloud computing, it has full self-service, full automation behind self-service and usage metering. It does not have to be on-premises, or owned or managed by the enterprise.

Appendix V Long Term Commitments by Consortium Members

We now list the long term commitment of the main TREDISEC partners with respect to the long-term sustainability strategy of TREDISEC.

8.5.1 Arsys

After the project end Arsys Internet S.L.U. is further committed to common exploitation of project results under the TREDISEC Framework. In particular Arsys Internet S.L.U. will maintain and update all information related to its TREDISEC primitives and recipes on a regular basis. For any requests or interest in the utilization, business and commercialization of the TREDISEC framework components (i.e. primitives owned by Arsys Internet S.L.U.), Arsys Internet S.L.U. will provide a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.

Furthermore Arsys Internet S.L.U. will continue to promote TREDISEC project results internally and to the relevant business partners.

8.5.2 ETH

After the project end, ETH is further committed to common exploitation of project results under the TREDISEC Framework. In particular, ETH will maintain and update all information related to its TREDISEC primitives and recipes on a regular basis. For any requests or interest in the utilization, business, and commercialization, of the TREDISEC framework components (i.e. primitives owned by ETH), ETH provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.
Furthermore, ETH will continue to promote TREDISEC project results internally and to relevant business partners.

**8.5.3 EURECOM**

After the project end, EURECOM is further committed to common exploitation of project results under the TREDISEC framework. In particular EURECOM will maintain and update all information related to its TREDISEC primitives and recipes whenever needed. For any requests or interest in the utilization, business, and commercialization of the TREDISEC framework components (i.e. primitives owned by EURECOM), EURECOM provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.

Furthermore EURECOM will continue to promote TREDISEC project results internally and to its relevant consortium members.

**8.5.4 GRNET**

After the project end, GRNET is further committed to common exploitation of project results under the TREDISEC Framework. In particular, GRNET will maintain and update all information related to its TREDISEC primitives and recipes on a regular basis. For any requests or interest in the utilization, business, and commercialization, of the TREDISEC framework components (i.e. primitives owned by GRNET), GRNET provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.

Furthermore GRNET will continue to promote TREDISEC project results internally and to relevant business partners.

**8.5.5 IDEMIA**

After the project end IDEMIA is further committed to common exploitation of project results under the TREDISEC Framework. In particular, IDEMIA will maintain and update all information related to its TREDISEC primitives and recipes on a regular basis. For any requests or interest in the utilization, business, and commercialization of the TREDISEC framework components (i.e. primitives by IDEMIA), IDEMIA provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.

Furthermore, IDEMIA will continue to promote TREDISEC project results internally and to relevant business partners.

**8.5.6 SAP**

After the project ends, SAP will provide a contact person for our primitives for at least two years. This person can be contacted for all questions about SAP’s contributions within TREDISEC and in particular with respect to SAP’s delivered primitive. If any entity wants to use the primitives, this contact person may involve corresponding internal departments (such as sales and legal) for further negotiations. Currently, Dr. Mathias Kohler (Research Manager, SAP Security Research) will be the respective contact person. Furthermore, SAP will actively advertise the TREDISEC framework in our internal security portal for at least 4 years.

**8.5.7 NEC**

After the project end NEC is further committed to common exploitation of project results under the TREDISEC Framework. In particular, NEC will maintain and update all information related to its TREDISEC primitives and recipes on a regular basis. For any requests or interest in the utilization, business, and commercialization of the TREDISEC framework components (i.e. primitives by NEC), NEC provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of 4 years.
Furthermore, NEC will continue to promote TREDISEC project results internally and to relevant business partners.

8.5.8 ATOS

After the project end, ATOS is further committed to common exploitation of project results under the TREDISEC Framework. In particular, ATOS will maintain and update on a regular basis all information related to its TREDISEC primitives and recipes. For any requests or interest in the utilization, business, and commercialization, of the TREDISEC Framework components (i.e. primitives owned by ATOS), ATOS provides a dedicated point of contact that will follow-up on the request in a timely and professional manner for a period of ATOS. Furthermore ATOS will continue to promote TREDISEC Project results internally and to relevant business partners for a period of 4 years.