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

D1.6 - INNOVATION MANAGEMENT REPORT

Work Package	WP 1, Management
Lead Author (Org)	Ghassan Karame (NEC)
Contributing Author(s) (Org)	Elena Gonzalez (ATOS), Alessandro Sforzin (NEC)
Reviewers	Rodrigo Diaz (ATOS), Melek Önen (EUR)
Due Date	30.11.2016
Date	28.11.2016
Version	0.7

Dissemination Level

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)

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

Versioning and contribution history

Version	Date	Author	Notes
0.1	29.06.2016	Ghassan Karame (NEC)	Initial outline
0.1	29.06.2016	Alessandro Sforzin (NEC)	Initial outline
0.2	11.10.2016	Ghassan Karame and Alessandro Sforzin (NEC)	First pass
0.3	04.11.2016	Elena Gonzalez (ATOS)	Framework details
0.4	07.11.2016	Ghassan Karame and Alessandro Sforzin (NEC)	Final draft
0.5	10.11.2016	Ghassan Karame and Alessandro Sforzin (NEC)	Comments of peer review integrated
0.6	21.11.2016	Ghassan Karame and Alessandro Sforzin (NEC), Melek Önen (EUR), Elena Gonzalez (ATOS)	Version for approval
0.7	28.11.2016	Jose Fran. Ruiz (ATOS), Rodrigo Diaz (ATOS)	Quality check approval

Disclaimer

Table of Contents

Executive Summary 5
1 Introduction 6
1.1 Goals of Innovation Management 6
1.2 Recap on Innovation Management Approach in TREDISEC 6
1.3 Detailed Activities 7
1.1 Structure of the document 7
2 Overview of Cloud Security Market 8
2.1 Key Innovation Points of TREDISEC 8
2.2 Cloud Security and Storage Market Trends 9
2.3 Cost Reductions Due to Deduplication 10
2.4 Summary 11
3 Overview of Innovation in the Technical WPs in TREDISEC 13
3.1 Innovation within WP2 and WP6 13
3.2 Innovation within WP3 13
3.3 Innovation within WP4 14
3.4 Innovation within WP5 15
4 Minutes of Innovation Management Plenary Meetings 16
4.1 Minutes of Innovation Management Meeting during the GA at Sophia-Antipolis 16
4.1.1 WP2 and WP6 16
4.1.2 WP3 16
4.1.3 WP4 16
4.1.4 WP5 17
4.1.5 Conclusion 17
4.2 Minutes of Innovation Management Meeting during the GA at Heidelberg 17
4.2.1 WP2 and WP6 17
4.2.2 WP3 17
4.2.3 WP4 18
4.2.4 WP5 18
4.2.5 Conclusion 18
4.3 Minutes of Innovation Management Meeting during the GA in Salzburg 19
4.3.1 WP2 and WP6 19
4.3.2 WP3 19
4.3.3 WP4 19
4.3.4 WP5 19
4.3.5 Conclusion 19
5 Quantifying Innovation in TREDISEC 21
5.1 Methodology: Framework for the continuous assessment of project innovation 21
5.2 Scientific Technical Dimension 21

5.2.1 Project R&D Excellence 21
5.2.2 S/T Continuous Alignment 26
5.3 Market Dimension 28
5.3.1 Market Alignment 28
5.3.2 Company´s Strategic Fit 31
5.3.3 Organizational Dimension 33
6 Conclusions 36
7 References 37

List of Tables

Table 1: Summary of risks identified at the GA meeting in Sophia-Antipolis. 17
Table 2: Summary of risks identified at the GA meeting in Heidelberg 18
Table 3: Summary of risks identified at the GA meeting in Salzburg. 20

List of Figures

Figure 1: The main key innovation points of TREDISEC. 8
Figure 2: Cost Reductions due to data deduplication vs. prices of commodity storage providers (adapted from [9]). "ppu" stands for price per user. The x-axis specifies the amount of GB stored. 10
Figure 3: Storage savings due to various deduplication techniques using realistic datasets. 11
Figure 4: Framework dimensions used to assess innovation activities. 21

Executive Summary

The goal of this document is to outline the current progress of the TREDISEC project from the point of view of Innovation Management activities. Recall that the main purpose of innovation management is to ensure that the project research activities, technological developments, and achievements, are kept well connected to outside technology developments. An additional goal of innovation management here is to maintain low risk level for the project and to prevent the project results from losing relevance given the evolving trends in the market.

This report includes an update on the main innovation points that are selected for monitoring in the TREDISEC project. We also report on the various activities conducted by the Innovation Director until the time of writing to monitor the current state of innovation within TREDISEC and outline/measure possible risks to TREDISEC's innovation output. We also include a market analysis summarizing the current advances in the cloud security market, as well as an overview of existing products that promise to offer end-to-end security in the cloud. Additionally, this deliverable includes a detailed innovation management report of two general assembly meetings held in 2016, as well as an up-to-date assessment of the innovation level within each technical work package (WP) in TREDISEC.

We further refine the framework that we previously outlined in deliverable D1.5 to quantitatively measure the innovation level of TREDISEC and we provide first draft measurements of the current innovation level of the project.

Our current assessment shows that the innovation level of TREDISEC is fairly healthy and that the fast progress in achieving some of the milestone goals of the project minimizes the risk that the project goals lose relevance given the evolving trends in the market.

1 Introduction

1.1 Goals of Innovation Management

One of the main objectives of innovation management in TREDISEC is to strongly support the exploitation of the research results of the project. This goes beyond the production and dissemination of novel cloud security techniques, and concerns mainly the innovation impact of TREDISEC. Indeed, innovation often characterizes an activity which does not only consist of dissemination, but also deals with the exploitation of the R&D results of the project.

Studies have shown that one of the best ways to successfully convert research into innovative success stories lies in ensuring that all cooperating research organizations can prepare themselves for the challenges of market-oriented exploitation. The earlier and more organized is this preparation, the more likely it is to reach a success story.

In TREDISEC, this process is organized owing to the installed innovation management scheme which is devised to ensure the successful exploitation of the project results, and the conversion of these results into innovative success stories.

Namely, the main purpose of innovation management activities in TREDISEC is to ensure that the project research activities, technological developments, and achievements, are kept well connected to outside technology developments. An additional goal of innovation management here is to maintain low risk level for the project and to prevent the project results from losing relevance given the evolving trends in the market.

Since the start of the project, the innovation management task is mainly carried out under the lead of the Innovation Director (ID) of TREDISEC, who was constantly supported by the rest of the members of the Executive Board (EB), which includes the Work Package Leaders (WPLs). In what follows, we briefly recapitulate the innovative management approach adopted by TREDISEC.

1.2 Recap on Innovation Management Approach in TREDISEC

The TREDISEC consortium comprises a rich mixture of large industrial players, who have a strong overview of the cloud security market trends. The involvement of these players in the TREDISEC consortium increases the success rate of project innovation. These enterprises can indeed make a strong difference in successful market-oriented exploitation by ensuring that the research outcomes are in line with their expectations, and are consistent with the current demands of the market. This is further strengthened in TREDISEC by integrating the technology into bundles that can be directly used by service providers.

Innovation management in TREDISEC is conducted at the WP1 management level. As mentioned earlier, the communication and management of innovation-related activities are orchestrated by the ID, who will ensure that all the different entities in the consortium can manage the respective innovation-related risks, and in the event that a risk becomes an actual challenge or threat, the ID will follow an emergency management scheme to alleviate such risks.

Our management scheme includes the following milestones:

- Protecting innovation before disseminating the project results. Our innovation strategy plan (see Deliverable D1.5) provides clear and efficient procedures for rapidly protecting new results and agreeing on dissemination, therefore ensuring that no information is published which could be detrimental to the protection of some innovative project results. A formal process is described in D1.1 section 3.3, where the Project Coordinator, the Scientific Director, the Innovation Director, and the WP7 leader, by means of the TREDISEC Press Office, validate any publication or dissemination activity before its actual release to the public.
- Specifying other innovation management activities such as monitoring of innovation, setting up emergency plans, or taking-up activities.

- Defining strategies related to the granting of licences to third parties, or to the identification of potential hurdles for the implementation of the results of the project (e.g., standards or third parties' patents, etc.)
- Refining the innovation management strategy as market trends evolve. That way, the exploitation of the project results becomes more accurate and aligned with relevant tendencies.
- Identifying and acquiring feedback from different entities and communities (e.g., advisory board body, related projects, cloud and security communities, etc.) to better align the project results with users' expectations.

1.3 Detailed Activities

In this deliverable, we include an assessment of the current status of the project's innovation activities. We will use our assessment of the technologies to determine the key innovation points that should be monitored throughout the project.

Concretely, we present the status of the following innovation management activities:

- Monitoring of cloud security and storage market trends to support the definition of the business cases and to plan sustainability activities.
- Monitoring the WPs' progress according to the Innovation Strategy and propose actions to be taken if necessary.
- Assessing the innovation level of the project with regards to a set of innovation-related indicators grouped into framework dimensions.

1.1 Structure of the document

This document is structured into 6 main sections as follows:

Section 2 provides a general background on the current status of cloud storage and security market, and pinpoints limitations in current cloud solutions.

Section 3 identifies the innovation potential of the project, analysing the current status of innovation within the technical work packages (i.e., WP2, WP3, WP4, WP5, and WP6) of TREDISEC.

Section 4 summarizes the minutes of the various plenary innovation management meetings that were held during the GA meetings.

Section 5 outlines the current assessment of innovation in TREDISEC according to the framework described in deliverable D1.5.

Section 6 concludes the deliverable and lays down the various activities and deliverables that will be conducted in the upcoming months, in the context of Innovation Management.

2 Overview of Cloud Security Market

In this section, we overview the current state of the cloud security market with respect to the main innovation points outlined in deliverable D1.5. We start with a brief recap of the key innovation points of TREDISEC.

2.1 Key Innovation Points of TREDISEC

In deliverable D1.5, we have identified 7 key innovation points of TREDISEC (summarized in Figure 1).

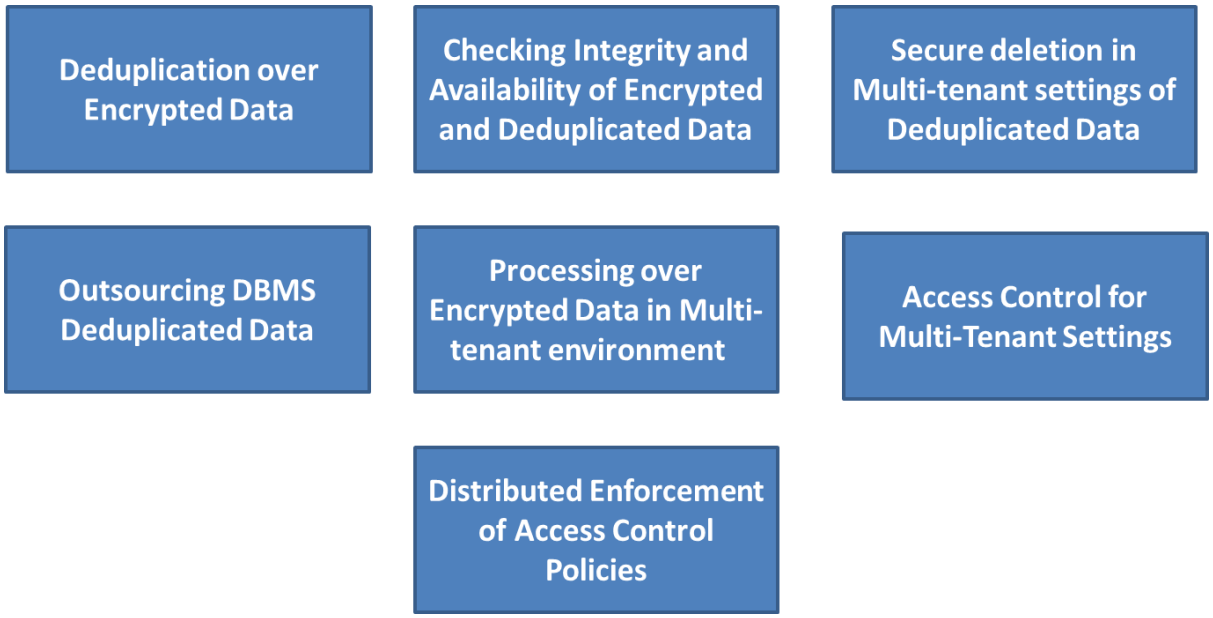

Figure 1: The main key innovation points of TREDISEC.

We now provide a brief recap of those 7 innovation aspects adapted from deliverable D1.5:

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

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

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

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.

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..

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 able to evaluate these policies against distributed attributes, allowing immediate access to services/resources to tenants that belong to different circles of trust.

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.

2.2 Cloud Security and Storage Market Trends

The cloud security market has witnessed considerable growth, particularly after 2010, when a vast number of organizations started adopting cloud services for cost cutting, agility and flexibility of IT infrastructure.

Since 2010, we witnessed the emergence of a large number of cloud specific threats. These threats were mainly resulting from the lack/improper use of security technology in the cloud, but also from configuration errors within the cloud (e.g., by careless or non-expert cloud administrators). This is especially true after the outbreak of the PRISM revelations. These revelations unearthed the details of a massive surveillance program which was neither restricted to one geographical area, nor mitigated by the various security countermeasures already deployed within the targeted services.

Most cloud providers nowadays deploy standard security solutions by which they retain full control over the customers' data in order to ensure that their offerings can leverage the multitude of benefits originating from the adoption of multi-tenancy and storage efficiency techniques. This entails retaining cryptographic keying material, choosing the underlying cryptographic primitives, etc. This strategy does not only increase the profitability of the cloud, but also ensures that cloud providers can offer cheap services to users at relatively small costs. Unfortunately, in this model, customers of cloud services have no means to control and verify how data is processed or stored.

Given this, it is expected that the future growth of cloud security market will have a huge impact on the increasing adoption of cloud computing by the small and medium size enterprises. Overall, it is expected that the cloud security market will be worth $8.71 Billion by 2019 out of an estimated 60-70 Billion dollar cloud storage market [1]. Exemplary key players in this market are Computer Associates (CA) Technologies, Symantec, Fortinet, Symplified, IBM, Trend Micro, Zscaler, Panda Security, Sophos, and McAfee.

Additionally, the market currently contains a number of secure cloud offerings, such as:

- Boxcryptor [2] is a simple interface to the cloud which offers no security besides simple encryption.
- Cleversafe [3] (currently bought by IBM) offers scalable distributed storage. It embeds security mechanisms such as end to end encryption and all-or-nothing transforms, but does not deal with verifiable storage/computations, nor does it attempt to address issues with storage efficiency and compatibility with multi-tenancy solutions.
- Wuala [4] is a Swiss cloud provider which offers only basic encrypted cloud storage.
- Most large telco operators such as Swisscom [5], Telefonica [6], and others, offer their customers personal data stores. These stores are promised to be isolated from other stores

and only contain their individual customers' data. Encryption is typically performed using keys provided by the telco-operators, which opens the door for a large variety of threats.

According to [7], data growth continues at a rapid pace - about 50 percent per year - with an estimated 50 percent to 80 percent of new data being comprised of unstructured and archival data. These factors heavily influence the deployment of security technologies in the cloud; it is clear that security technologies are required to be highly scalable with the size of data to be effective and adopted in practice.

2.3 Cost Reductions Due to Deduplication

Notice that there are a number of envisioned cloud deployments. According to a report [8], the full costs (including IT infrastructure and IT infrastructure administration) for securely storing 1TB/year are:

- $955,500 in a private cloud (hosted by the enterprise itself),
- $251,600 in existing public clouds,
- $716,000 when using hybrid solutions that comprise a deployment of public and private clouds.

Our analysis, based on pure storage prices per month in existing public clouds, shows further cost reduction potential through deduplication. This is depicted in Figure 2.

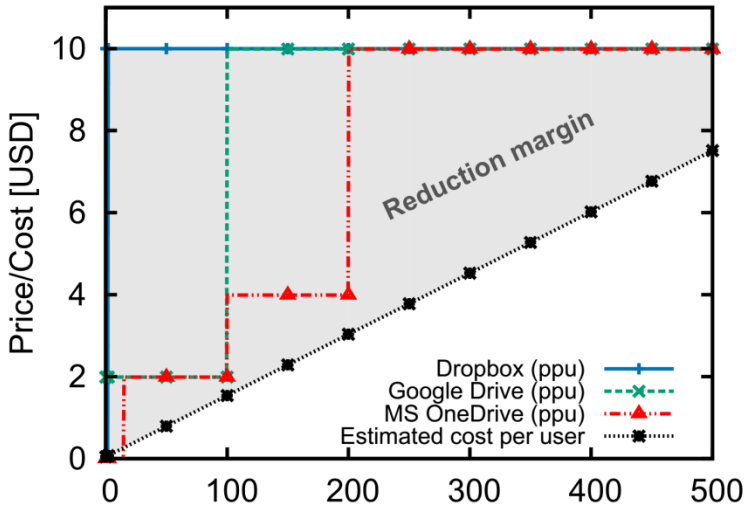

Figure 2: Cost Reductions due to data deduplication vs. prices of commodity storage providers (adapted from [9]). "ppu" stands for price per user. The x-axis specifies the amount of GB stored.

In Figure 2, the blue, green, and red curves show the price currently charged by Dropbox, Google Drive, and MS OneDrive respectively. The dotted black line depicts the estimated cost of storage per user in Amazon S3 after data undergoes deduplication. Assuming that 50% of the data stored by clients is deduplicated with the data pertaining to two other cloud users, and that clients download 0.96% of the data stored in their accounts per day. The "reduction margin" refers to the difference between the price borne by the users and the effective cost of users' storage after deduplication.

We start by studying the storage cost savings due to data deduplication. Following [10], we differentiate between two possible data deduplication techniques: file-based deduplication and block-based deduplication.

File-based deduplication only deduplicates identical files. Deciding whether two files are identical is usually achieved by hashing the content of each file and comparing the results. File-based deduplication requires modest computational and indexing overhead. The main drawback of file-based deduplication is that it does not result in any storage savings if two files differ even in a single bit (since the resulting hash would be different).

On the other hand, block-based deduplication chunks a file into blocks and deduplicates any two blocks with identical content. This technique enables fine-grained deduplication and overcomes the drawbacks of file-based deduplication. The simplest chunking algorithm splits a file in blocks of fixed size. Fixed block-size chunking can efficiently deduplicate files that only differ in one or a few blocks. Small block sizes may increase the storage savings (since the probability that two blocks are identical increases)—this however comes at the expense of larger indexes. Previous work has shown that block sizes of 4 to 8 KiB yield the best storage savings taking into account the savings for deduplication and the size of the index. Fixed block-size chunking, however, fails to effectively deduplicate even slightly “shifted” content. This shortcoming can be effectively addressed by content-defined chunking (CDC) algorithms. CDC produces variable-sized blocks by processing files with a sliding window with one-byte steps. At each offset, CDC computes a fingerprint of the content in the window and inserts a block boundary at the end of the window if the fingerprint matches a pre-defined value; if a block boundary is inserted at byte i, the new windows starts at byte i+1. Popular functions for CDC algorithms consist of rolling checksums, e.g., based on Rabin fingerprints. Rolling checksums allow the efficient computation of checksums based on a sliding window, as the checksum of the current window can be efficiently computed using the checksum of the previous window.

In Figure 3, we measure the storage savings that result from data deduplication using realistic datasets obtained from TREDISEC partners, NEC, ETHZ, and EURECOM. We observe that, for all studied datasets, CDC-based schemes using Rabin fingerprints with average block sizes of 4 KiB and 8 KiB exhibit the highest storage reductions (up to 90% in archival scenarios). File-based deduplication techniques achieve lower storage reduction when compared to block-based techniques. We further observe that fixed-sized block deduplication techniques considerably improve storage costs when compared to their file-based counterparts; these techniques however result in lower savings when compared to CDC-based schemes.

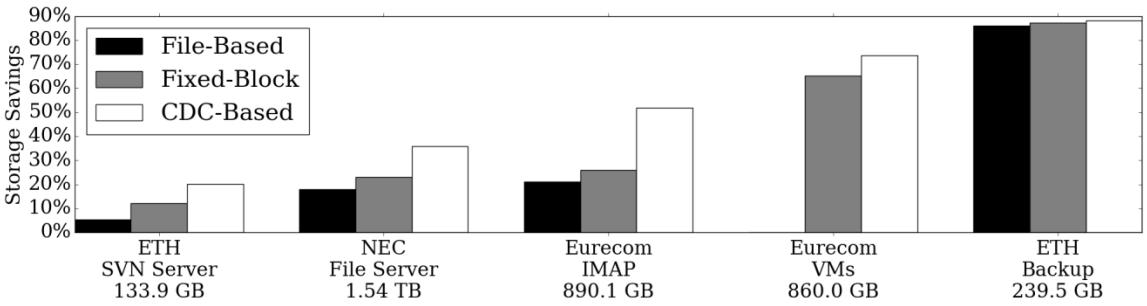

Figure 3: Storage savings due to various deduplication techniques using realistic datasets.

2.4 Summary

In summary, we can safely conclude that our market analysis confirms indeed that TREDISEC is addressing an important problem in the cloud security market, which has immediate applicability in the current market and would increase cloud adoption by industrial players and SMEs.

Our current view of market trends also shows that there are no significant technological changes that threaten the innovation within TREDISEC. As shown in Figure 3, storage efficient techniques indeed result in considerable storage costs savings. We remark that different deduplication techniques (i.e., result in different overhead in terms of storing metadata information (e.g., pointers, URI). To avoid any technological bias in choosing a specific deduplication technique, it is the goal of TREDISEC to devise appropriate technologies that could be applied to the multitude of popular block-based and file-based deduplication techniques.

3 Overview of Innovation in the Technical WPs in TREDISEC

We now proceed to evaluate the current innovation delivered by TREDISEC with respect to the technical work packages, namely with respect to WP2, WP3, WP4, WP5, and WP6. Notice that since WP2 basically orchestrates the requirements and architectural design choices for the TREDISEC framework, which is in turn covered in WP6, we analyse the innovation jointly within both WP2 and WP6.

3.1 Innovation within WP2 and WP6

One important point that should not be overlooked when designing security mechanisms for cloud systems is their integration into a single framework. Typically, a security primitive is devised for a single use-case and/or a specific application. Although such a design approach may reduce the complexity of the solution, it may lead to situations where security primitives are incompatible to the point that they cannot be implemented using the same interface or the same framework. This demonstrates the need for devising a unified framework which efficiently integrates the required security primitives, without incurring extra processing and storage cost at the cloud service providers or end-users.

According to the Deliverable D2.3, the TREDISEC framework makes multiple security primitives and recipes centrally available. Following the initial design of D2.3, we are currently realizing the architecture of the TREDISEC framework, and identifying specific implementation issues.

Specifically, we have provided a concrete architecture plan built upon three pillars:

1. A security primitive is defined as an interface specification and documentation.

2. A security primitive implementation should be considered as a unified software package within a recipe.

3. Integration among primitives and cloud environments is expressed as installation instructions within a recipe.

In the context of (1) we have implemented a primitive API documentation guide to be used by all TREDISEC partners. Our plan is to provide a concrete implementation of the framework based on (2) and (3). As far as we are aware, this is the first realization of a unified framework that combines a number of security primitives, which are compatible with existing cloud functional requirements.

3.2 Innovation within WP3

Cloud service providers offer an unlimited storage capacity with high reliability/availability guarantees at affordable prices. Nevertheless, many individuals and companies do not fully trust cloud service providers to handle their data correctly. To win clients' trust, cloud service providers are encouraged to put in place mechanisms that allow for transparent data storage/processing practices.

In Task 3.1, project partners aim at designing primitives that ensure an efficient verification of the correctness of the storage operation at the cloud. One prominent technique to achieve such a goal is Proof of Retrievability (PoR). Although there exist many proposals for PoR in the literature, most of these solutions overlook cloud servers' functional requirements and therefore cannot be immediately deployed. One of the new TREDISEC PoR primitives, dubbed ML-PoR [11] is inherently compatible with functional requirements, such as deduplication, and security requirements, namely data confidentiality. Another innovative approach to enforce storage correctness in TREDISEC is taken with the *MIRROR* [12] primitive which in addition to the verification of the correct storage of the data, also ensures the efficient verification of the data replication operation frequently used by cloud service providers.

To save bandwidth, cloud providers may opt for client-side deduplication whereby clients only upload documents that do not exist in the cloud server. This however leads to serious vulnerabilities: for instance, a client can easily claim ownership of any data and therewith retrieve a document without being authorized. In Task 3.3, partners address this problem by investigating new proof of ownership solutions that, compared with related work, are more efficient and provide better security guarantees. Furthermore, a secure deduplication operation raises a new problem whereby a client wishes to pay for the actual storage cost only. A newly designed TREDISEC primitive [9] helps the cloud to provide a proof on the deduplication ratio to the clients, and hence define an appropriate billing policy.

In addition to storage services, cloud servers are asked to perform computationally demanding operations on behalf of their clients. This gives rise to the need for verifying the integrity of the output of such delegated operations. Existing verifiable computation solutions are mostly theoretical that draw upon probabilistically checkable proofs or quadratic arithmetic programs and hence are not efficient. In Task 3.2, partners already proposed three different primitives focusing on three widely used operations, namely polynomial evaluation, matrix multiplication [13], and biometric matching [14]. These primitives are more efficient when compared to previously proposed techniques. These innovative results are highlighted in deliverable D3.2.

3.3 Innovation within WP4

Achieving end-to-end security in existing cloud services is not straightforward. Notably, end-to-end security aims at ensuring that end-users are the only entities able to decrypt their encrypted data outsourced to the cloud. This implies that cloud service providers may neither be able to offer standard APIs to efficiently process customers' data, nor to take full advantage of cost-effective storage solutions which rely on existing deduplication and compression mechanisms. In addition to data confidentiality, users also call for resource isolation solutions that enable tenants to have a secure and isolated environment. Although implementing resource isolation in the cloud would indeed deter threats originating from unknown vulnerabilities and the subsequent loss of data governance, these measures typically come at odds with multi-tenancy and resource sharing, which would in turn prevent a successful and cost-effective instantiation of the current multi-tenant cloud model.

Existing state of the art solutions completely give up one requirement for the other. That is, they either rely on standard solutions at the expense of end-to-end security and governance, or provide end-to-end security but renounce any form of resource sharing or storage efficiency techniques.
One way is to ensure that the code that performs access control is secure, as vulnerabilities in this code would allow for access control checks to be bypassed and resource isolation to be breached. There are three steps to securing code: reducing the amount of bugs, reducing the attack surface, and hardening. While testing is typically associated with the functional aspects of a program, vulnerability-targeted testing aims at revealing security-critical bugs. A popular approach is fuzz testing, feeding random input to the program to trigger memory corruption bugs. At the moment, Driller [15] is one of the state-of-the-art approaches in this area, combining fuzz testing with symbolic execution to explore and test critical parts of application code. However, cloud software stacks might be well beyond what application-level fuzz testing tools are capable of. For instance, native distributed systems code that runs in a privileged mode is less than straightforward to instrument, and binary non-standard communication protocols often do not come with extensive test suites that would be required for efficient testing. In Task 4.2, partners are investigating these challenges along with the suitability of fuzz testing techniques to ensure that the code that performs access control is secure. Another technique would be to rely on trusted computing technologies, such as Intel SGX to protect the reference monitors from being compromised. Recently published research by TREDISEC partners shows that Intel's SGX, while being an enabler for private computation in the cloud, is prone to exploitation of synchronisation bugs in enclave code. The reason is that SGX's threat model allows for an attacker to be in control over enclave code scheduling by triggering page faults in enclave code. Control over stopping and resuming enclave code enables an attacker to exploit synchronisation bugs in multithreaded code, such as use-after-free bugs, in a reliable manner. Research results by TREDISEC partners have however shown that TPM-based technology can be successfully applied to many-core systems in order to solve such challenges.

On the other hand, a number of solutions for secure data deduplication in the cloud [9] [16] [17] [18] recently emerged with the goal of enhancing the provisions of message-locked encryption schemes. Most of these solutions rely on the existence of an additional party that assists in the key generation phase, or even performs data encryption. Recall that the use of semantically secure encryption effectively prevents the detection of duplicate copies and hence restrains the deduplication ratio. To reconcile data deduplication with block-based data encryption, TREDISEC partners have proposed PerfectDedup [17] which assists the user in discovering the popularity of the data prior to choosing the appropriate encryption mechanism. To counter dictionary attacks on the lookup process, PerfectDedup leverages a privacy-preserving popularity detection mechanism that relies on perfect hashing which yields well-distributed collisions for unpopular data. Thanks to this primitive, the user can decide which encryption solution to use to protect her data prior to its upload, without leaking any meaningful information to the untrusted cloud server. Compared to existing work, PerfectDedup significantly reduces the storage and communication overhead by storing a single copy of each data segment when popular; the computational overhead is also optimized due to the use of symmetric encryption instead of a threshold encryption. Moreover, to deal with file-based deduplication, TREDISEC partners have additionally proposed ClearBox, a primitive which relies on server-assisted key generation in order to allow different clients that store the same file to devise the same encryption key, thus effectively enforcing file-based deduplication. ClearBox implements an OPRF based on blind BLS signatures. The rationale here is that BLS signatures are considerably shorter than RSA signatures (which are used in earlier solutions), and are faster to compute by the key server when compared to state of the art solutions. This, in turn, improves the scalability of the key server (w.r.t. the number of keys generated per second). In addition, ClearBox leverages novel cryptographic accumulators in order to allow a storage service provider to transparently attest to its customers the deduplication patterns of the (encrypted) data that it is storing. By doing so, ClearBox enables cloud users to verify the effective storage space that their data is occupying in the cloud, and consequently to check whether they qualify for benefits such as price reductions, etc.

3.4 Innovation within WP5

WP5 performs research on multiple outsourcing mechanisms and technologies. This work package comprises research on the design of a provisioning framework, concepts on secure outsourced data processing, and methods and algorithms to optimize data queries over encrypted data by outsourcing its processing into a hosted environment with more computing power.

WP5 already presents a set of innovative ways in preparing data, as well as SQL statements specifically for a migration from an on-premise solution to a cloud solution. Our optimizations for storing encrypted data aim at optimizing the data storage on three dimensions: data owners are enabled to select the sensitivity of their data, SQL queries are analysed for an optimized performance experience when they will be executed within a cloud environment, and the storage space for encrypted data is optimized in multiple ways while preserving the security sensitivity levels the data owner initially selected.

WP5 advances in outsourcing data into an encrypted cloud with a new solution for outsourcing data with the help of a cluster [19]. The outsourcing process is possible as live migration with nearly zero down time such that, even if the encryption of data requires a significant amount of time, operations can still be continued. Furthermore, WP5 provides innovative solutions for the following three aspects:

- It introduces new methods for applications of searchable encryption to biometric identification, which improve the state of the art by being easily parallelizable [20]. The highly sequential design of the previous solution prevented efficient outsourcing to several external nodes.

- It addresses parallelized search over encrypted text. WP5 explores searchable encryption based on constrained functional encryption which also provides key-message homomorphic

properties. WP5 further investigates the possibility of extending the new searchable encryption scheme with a MapReduce execution framework to outsource and parallelize the search workload on the cloud service provider. It also provides insights on the limitation of this scheme in terms of performance, and provides some suggestions to improve it.

- Only very few solutions so far focus on the problem of searchable encryption multi-tenancy. The majority of multi-user searchable encryption solutions are either not secure, or rely on the existence of a trusted third party.WP5 aims at analysing the vulnerabilities of existing MUSE solutions, and designing a new MUSE solution that is scalable with the number of users.

4 Minutes of Innovation Management Plenary Meetings

Following the Innovation Strategy Plan laid down in deliverable D1.5, the Innovation Director chaired a dedicated meeting in each plenary General Assembly gathering that was attended by TREDISEC's Executive Board. In what follows, we briefly summarize the meeting minutes of the innovation management slots held in Sophia Antipolis, Heidelberg, and Salzburg.

4.1 Minutes of Innovation Management Meeting during the GA at Sophia-Antipolis

During this GA, the Innovation Director reminded partners the procedure for publishing research articles and announcements related to TREDISEC work(s). Namely, the Innovation Director reminded partners to provide a camera ready version of the public announcement to the press office before publishing it. This process ensures that no information is published which could be detrimental to the protection of some innovative project results.

We now proceed to summarizing the outcome of the innovation status check with respect to the technical WPs.

4.1.1 *WP2 and WP6*

WP2 and WP6 leaders commented that there are no new risks with respect to WP2/WP6 innovation. Namely, the Executive Board was not aware of any similar framework that can uniquely combine various such primitives.

4.1.2 *WP3*

WP3 leader commented that there are no new risks with respect to WP3 innovation. Namely, there was consensus that there are no solutions in the literature/market that provide integrity and availability guarantees of multi-tenant data in presence of storage efficiency.

4.1.3 *WP4*

WP4 leader pointed out a new paper at ACM CCS'15 by Liu et al. [21] which does not rely on any independent server but on the collaboration of the users uploading the same file. Here, a cloud user encrypts a file with the same encryption key that was used by previous uploaders of the same file. Owing to the use of an additively homomorphic encryption, Password-Authenticated Key Exchange (PAKE), and a short hash function, the solution achieves deduplication with better security guarantees compared to previous solutions. More specifically, by leveraging the PAKE-based protocol, the proposed scheme prevents dictionary attacks without the aid of an assisting server. However, there was a general consensus that this scheme achieves worst performance when compared to PerfectDedup and ClearBox as it requires communication amongst file owners.

Besides this proposal, WP4 leader commented that the TREDISEC outcomes, PerfectDedup and ClearBox have a clear chance in the market as they address a number of relevant cloud security concerns without penalizing performance.

4.1.4 *WP5*

WP5 leader commented that there are no new risks with respect to WP5 innovation. Namely, there was consensus that there are no solutions in the literature/market that support storage efficiency in the presence of securely outsourced DBMS data, or that offer secure outsourced analytics/processing in a multi-tenant environment.

4.1.5 *Conclusion*

As a conclusion of this meeting, we update the risk likelihood of the various risks associated with TREDISEC innovation (and outlined in deliverable D1.5) as follows in Table 1:

Description of risk	Risk Likelihood
State-of-the-art environment / project objectives lose relevance	**Small**
Technological changes require significant redesign	**Medium**
Conflict between innovations produced by the project and existing/ new patents	**Small**
Results produced by TREDISEC are not well exploitable	**Medium**

Table 1: Summary of risks identified at the GA meeting in Sophia-Antipolis.

4.2 Minutes of Innovation Management Meeting during the GA at Heidelberg

This session was chaired by the Innovation Director and was attended by the Executive Board members.

4.2.1 *WP2 and WP6*

WP2 and WP6 leaders commented that there are no new risks with respect to WP2/WP6 innovation. Namely, the Executive Board was not aware of any similar framework that can uniquely combine various such primitives.

4.2.2 *WP3*

WP3 leader commented that there are no new risks with respect to WP3 innovation. The participants quickly discussed the paper [22] which offers to reconciliate proofs of ownership and proofs of data retrievability. The Executive Board members however reached the conclusion that this result does not threaten in any way the innovation in TREDISEC since it does not offer any solution for POR over deduplicated data.

The Innovation Director and Executive Board members then discussed the status of innovation in Task 3.3 where participants are working on an approach to combine Proof of Ownership (PoW) and key distribution for deduplication. While there are several existing schemes in the literature to solve both problems, there was consensus that these have never been combined. Combining both

approaches in a unified offering would allow TREDISEC to plug the security holes associated to key distribution schemes for deduplication that only require the participants to contribute with a short and unchanging digest of a file to obtain key material associated to that file. On the other hand, this would allow existing PoW schemes to be used for encrypted data. Therefore, for the moment, the Innovation Director decided to maintain the risk level associated to this task as low.

4.2.3 *WP4*

WP4 leader commented that there are no new risks with respect to WP4 innovation. Namely, there was consensus that TREDISEC solutions (ClearBox and PerfectDedup) already offer innovative solutions to the problem at hand.

With respect to secure deletion (i.e., Task 4.4), ETH commented that their secure deletion technology is ready, but cannot be fully exploited by the TREDISEC consortium since the solution was developed in collaboration with another university.

The Innovation Director and the Executive Board members agreed that secure deletion with non-cooperating cloud can be easily done. Furthermore, there are no new published works in this area that could threaten TREDISEC's work(s).

4.2.4 *WP5*

WP5 leader has identified no risks with their work. Namely, the WP5 leader reported that there are neither existing works, nor patents threatening their work.

4.2.5 *Conclusion*

The Innovation Director pointed out that while there were clear individual exploitation plans by TREDISEC partners for the developed technology and innovation, TREDISEC needs to clarify the business models that would allow project-wide exploitation of innovation. For this reason, the Innovation Director decided to maintain the risks associated exploitability of TREDISEC output to "medium".

As a conclusion of this meeting, the Innovation Director updated the risk likelihood of the various risks associated with TREDISEC innovation (and outlined in deliverable D1.5) as follows.

Description of risk	Risk Likelihood
State-of-the-art environment / project objectives lose relevance	**Small**
Technological changes require significant redesign	**Small**
Conflict between innovations produced by the project and existing/ new patents	**Small**
Results produced by TREDISEC are not well exploitable	**Medium**

Table 2: Summary of risks identified at the GA meeting in Heidelberg

4.3 Minutes of Innovation Management Meeting during the GA in Salzburg

This session was chaired by the Innovation Director and was attended by the Executive Board members.

4.3.1 *WP2 and WP6*

WP2 and WP6 leaders commented that there are no new risks with respect to WP2/WP6 innovation. Namely, the Executive Board reported that there are no existing frameworks with objectives similar to TREDISEC's. Moreover, it was remarked that TREDISEC's framework has unique features that act as clear differentiators from other running H2020 projects.

4.3.2 *WP3*

WP3 leader commented that there are no new risks with respect to WP3 innovation. Namely, there was consensus that there are no solutions in the literature/market that provide integrity and availability guarantees of multi-tenant data in presence of storage efficiency.

4.3.3 *WP4*

WP4 leader commented that there are no new risks with respect to WP4 innovation. Namely, there was consensus that there are no solutions in the literature/market that provide secure deletion in the presence of deduplication. There were also no new solutions for achieving resource isolation in multi-tenant systems.

4.3.4 *WP5*

WP5 leader commented that there are no new risks with respect to WP5 innovation. Namely, there was consensus that the newly released solutions based on the CryptDB technology do not threaten the innovation planned in this work package, namely relating storage efficiency in presence of securely outsourced DBMS data.

4.3.5 *Conclusion*

The Innovation Director also raised the point that it is important to involve end-users in testing the innovation produced by TREDISEC.

Partners then had a discussion on how to involve end-users with TREDISEC's final product. All partners agreed, and expressed their opinion, on the need of validating the impact of TREDISEC technology:

- NEC suggested gathering opinions from the end-users. They pointed out that mainly use-case partners should be responsible for suggesting viable solutions for validating the impact of the project.
- ARSYS seemed to prefer marketing solutions, and suggested to provide a solid infrastructure for end-users, in order to allow them to try the product. On top of that, they agreed with the idea of gathering opinions from the end-users.
- GRNET promised that, by month 36, they will provide a web demo to gather feedback, together with a questionnaire for (thousands of service) users. They offered to organize an awareness campaign to promote the usage of the platform.

In any case, all partners agreed to support either a workshop or an exhibition, after which WP7 activities will follow. As a conclusion of this meeting, the Innovation Director updated the risk likelihood

of the various risks as follows.

Description of risk	Risk Likelihood
State-of-the-art environment / project objectives lose relevance	**Small**
Technological changes require significant redesign	**Small**
Conflict between innovations produced by the project and existing/ new patents	**Small**
Results produced by TREDISEC are not well exploitable	**Medium**

Table 3: Summary of risks identified at the GA meeting in Salzburg.

5 Quantifying Innovation in TREDISEC

5.1 Methodology: Framework for the continuous assessment of project innovation

In D1.5, the Innovation Strategy and Plan outlined a framework to help the TREDISEC project with assessing the level of innovation of its activities throughout its duration.

This framework defines a set of innovation indicators grouped into three main dimensions: technological/scientific, market, and organisational. The goal of this framework is to continuously monitor TREDISEC's main lines of work, namely: research and technological advances, new developments and solutions, and methodologies and conceptual models or business models.

This information also helps to put in place the necessary actions to limit the deviation from the strategic innovation objective. The diagram depicted in Figure 4 shows the three dimensions used to assess the innovation of TREDISEC as aforementioned. Following, Figure 4 details each of these dimensions.

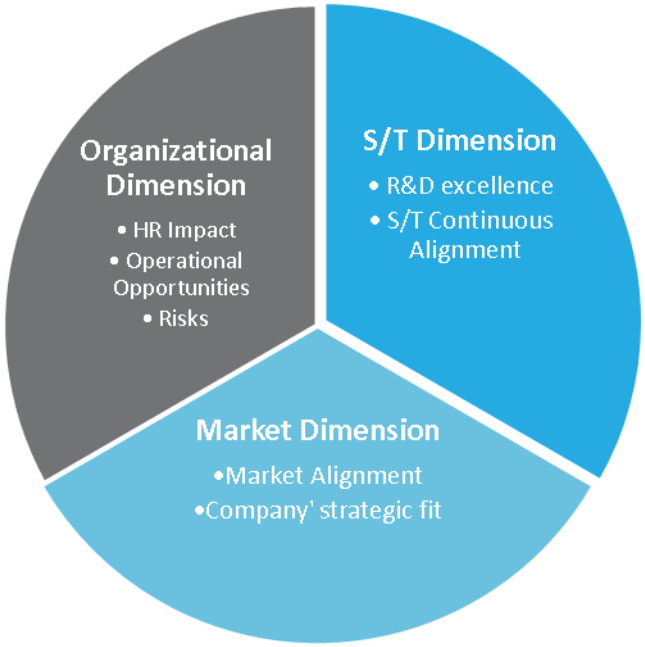

Figure 4: Framework dimensions used to assess innovation activities.

5.2 Scientific Technical Dimension

The Scientific/Technical dimension focuses on assessing the alignment of the R&D activities to what constitute current and long term concerns from a scientific/technical point of view: that is, being relevant, timely and adaptable. S/T dimension also assesses the excellence of the R&D work, as a combination of high quality and relevance.

5.2.1 *Project R&D Excellence*

Project R&D excellence is an indicator that assesses the relevance of the project investigations and research developments by looking at their impact in the R&D community. This assessment consists in

measuring the quantity and frequency of dissemination activities of the consortium members, as well as the quality and impact of these activities.

To quantify this set of activities we have selected a specific number of **Technological/Scientific KPIs:**

- Number of accepted publications in top tier ranked conferences, journals or venues (A*, A, B).
- Average of Relative Citations (ARC).
- Number of talks and presentations given to an expert audience.
- Presence of the project in events of relevance and high impact.
- Joint workshops/Networking sessions.
- Cross-references in official dissemination vectors (e.g. website, LinkedIn group, presentations, etc.).
- Contribution to educational programs (summer schools, courses, masters, degrees, etc.).

In the following paragraphs, we report a quantitative result for each of these KPIs:

Number of accepted publications in top tier ranked conferences, journals or venues (A*, A, B)	**19**

Within TREDISEC project we have released 19 publications describing the innovative research results obtained so far.

Along the period reported, partners have published the results of the conducted research in relevant conferences and journals. The project targets top quality conferences and journals in order to maximize the impact within the research community, and increase the value of the publications.

List of Conference Proceedings:

1. Transparent data deduplication in the cloud, F.Armknecht et al., ACM CCS 2015.
2. Logical Partitions on Many-core Platforms, Masti et al., ACSAC 2015.
3. Initial encryption of large searchable data sets using Hadoop, F. Wang et al., SACMAT 2015.
4. PerfectDedup: Secure data deduplication, Puzio et al., DPM 2015.
5. Some applications of verifiable computation to biometric verification, Bringer et al., WIFS 2015.
6. TREDISEC: Trust-aware Reliable and Distributed Information Security in the Cloud, Bringer et al, e-Democracy 2015
7. Efficient techniques for publicly verifiable delegation of computation, Elkhiyaoui et al., ASIACCS 2016, Xi'An, China.
8. Deniable Functional Encryption, de Caro et al., PKC 2016, Taipei, Taiwan.
9. A transparent defense against USB eavesdropping attacks, Neugschwandtner et al., EUROSEC 2016, London, UK.
10. Study of a verifiable biometric matching, Chabanne et al., IH&MMSec.
11. Mirror: Enabling Proofs of Data Replication and Retrievability in the Cloud, Armknecht et al., USENIX Security 2016, Austin, Texas.

12. A verifiable system for automated face identification, Chabanne et al., BIOSIG 2016, Darmstadt, Germany.
13. Searchable encryption for biometric identification revisited, Amchyaa et al., DPM 2016, Heraklion, Greece.
14. Delegating Biometric authentication with the sumcheck protocol, Chabanne et al., WISTP 2016, Heraklion, Greece.
15. Encrypting Analytical Web Applications, Fuhry et al., CCSW 2016, Vienna Austria.
16. Poly-Logarithmic Range Queries on Encrypted Data with small leakage, Hahn et al., CCSW 2016, Vienna Austria.
17. On Information Leakage in Deduplicated Storage Systems, Ritzdorf et al., CCSW 2016, Vienna Austria.
18. Message-Locked Proofs of Retrievability with Secure Deduplication, Vasilopoulos et al., CCSW 2016, Vienna Austria.
19. AyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves, Weichbrodt et al., ESORICS 2016, Heraklion, Greece.

Average of Relative Citations (ARC)	**Not yet applicable**

Since all publications were published over the course of 2015 and 2016, it is premature to evaluate this KPI, as there was not enough time to acquire citations.

We will update the ARC in the final Innovation Report, (D1.7, M36).

Number of talks and presentations given to a specialized audience	**9**

Since the start of the project, partners have disseminated TREDISEC's technology through keynote speeches to both industry and research communities, with the aim of increasing awareness about the main innovation advances of the project, and receiving feedback from an expert audience.

List of Talks/Keynotes for Industry/General public

1. CSP Forum 2015, Beatriz Gallego, Brussels, Belgium, April 2015.
2. Codemotion 2015, Olof Sandstrom, Madrid, Spain, November 2015.
3. Cybercamp 2015, Beatriz Gallego, Madrid, Spain, November 2015.
4. e-Democracy 2015, Panos Louridas, Athens, Greece, December 2015.

List of Talks/Keynotes for Research Community

1. Secure Data Storage, Ghassan Karame, ZISC Seminar, Zurich, Switzerland, January 2016.
2. Security for Cloud storage and processing, Melek Önen, Cyber Security Workshop, Ankara, Turkey, March 2016.
3. Confidentiality and Verifiability for Cloud Computing, Refik Molva, Mathematics School, Marseille, France, March 2016.
4. Verifiable storage and processing, Melek Önen, SEC2, Lorient, France, July 2016.

5. Approaches to Container Isolation in the Cloud via Kernel Attack Surface Reduction, Anil Kurmus, SEC2, Lorient, France, July 2016.

Presence of the project in events of relevance and high impact	**2**

List of Events of relevance and high impact with presence of TREDISEC

1. “Key challenges in end-to-end privacy/security in untrusted environments” ICT 2015; Lisbon, Portugal, October 2015.

   ICT is one of the most relevant events organized by the European Commission to promote projects financed by European funds, whose research produces technological advances beyond the state-of-the-art.

2. "Reconciliating Security and Functional Requirements in the Cloud”, TDL 2016, The Hague, Holland, June 2016.

   The Trust in Digital Life (TDL) community was formed by leading industry partners and knowledge institutes that believe trust and trustworthy services to be an essential ingredient of the digital economy. TDL covers key challenges, visions, and strategies surrounding Trust.

Joint workshops/ Networking sessions	**2**

List of joint workshops/ Networking sessions

1. “Key challenges in end-to-end privacy/security in untrusted environments” ICT 2015; Lisbon, Portugal, October 2015.

   (Also reported in Events of relevance and high impact).

2. SECODIC Workshop 2016, ARES Conference, Salzburg, Austria, August 2016

   Workshop organized by the consortium with the aim of discussing the recent advances in managing security and performance in the cloud, as well as protection of data at rest and in transit. It involved the collaboration of other 5 EU-funded R&D projects: WITDOM, CREDENTIAL, PRISMACLOUD, Coco Cloud, and CLARUS.

Cross-references in official dissemination means (e.g. website, LinkedIn group, presentations, etc.)	3

Specific dissemination activities relevant to Innovation due to the channel of dissemination:

1. Presentation to Canopy. Canopy is the Atos Cloud Service Line, and it is a good source of feedback about current cloud security market trends.
2. Post in IBM Research Blog focused on Innovation in Technology: IBM scientists bring trust and reliability to the cloud with advanced cryptography in EU projects.
3. Contribution to the white paper "Challenges for trustworthy (multi) Cloud-based services in the DSM", focused on research challenges in Cloud Security for future years.

Contribution to educational programs (summer schools, courses, masters, degrees…)	4

List of collaborations with educational programs:

1. Seminar on genomic privacy, Dagstuhl, 2015.
2. Modern cryptography and security: an inter-community dialogue, Dagstuhl, 2016.
3. IFIP Summer School, Edinburgh, 2015.
4. ZISC Workshop on Big Data Security and Privacy, Zurich, 2016.

5.2.2 *S/T Continuous Alignment*

This section assesses the fulfilment of challenges in the field of cloud security and privacy, which reflect both the scientific-technical agendas of the EU.

To measure the S/T alignment of TREDISEC's key innovation points, the ID will closely monitor the instruments outlined in the framework of D1.5 which, regularly, provide an insight on current research and technological gaps and reflect long-term, ongoing objectives at the EU-level.

The following excerpts were taken from many leading publications in digital and technological research to illustrate the importance of cloud security in the immediate future.

- **EU Digital Agenda: Magazine Net Cloud Future**[1]

"Also cloud computing presents opportunities to reduce security risks. In the past, customers would mostly run their applications on local servers, on their own premises. In such a setting the burden of securing systems, patching, updating, hardening, falls on the customer. But in cloud computing IT is outsourced and consumed online, as a pay-as-you-go service. While this does introduce security risks, the cloud also presents security"

"ENISA is also working with the Commission and industry to support the use of voluntary certification schemes for security. Cloud services are also gaining relevance from a CIIP perspective (Critical Information Infrastructure Protection). The adoption of cloud computing effectively moves multiple IT resources to a (smaller) number of platforms and datacentres.

The incident with Tieto, a Swedish ICT provider, is a good example – following a security incident in 2011, pharmacies across Finland could not operate for weeks.

The proposed EU directive on network and information security mentions large cloud providers as potentially critical for the digital society.

Always when there are new IT products and developments, it is tempting for information security professionals to focus on the new risks. But it is important not to forget the security risks of existing technology. This is not the time to stay put. ENISA will continue to work with industry and government experts to help customers leverage the security opportunities of cloud computing, and at the same time mitigate the risks."

"Enhanced cryptography for Cloud Services: Cloud services need assurances from providers that effective technological solutions have been put in place to manage and mitigate the security risks facing their data stored on the cloud. More work should be done to preserve privacy and the confidentiality of data in the cloud, such as privacy-preserving cryptology including anonymous credentials and practical techniques for processing encrypted data. Furthermore, research into functional encryption such as attribute based cryptography and cryptography in a cloud service context would be of value."

- **NIS WG3**[2] **Strategic Research Agenda, secure ICT landscape**

"As we go forward, the Cloud is becoming the dominant form of ICT consumption – whether as Infrastructures, Platforms or Software as a Service, the Cloud will be the way in which customers both private and public consume new ICT. Ensuring cloud services are secure and resilient is in itself a significant challenge given the complexity, scale and interconnectedness of cloud ecosystems. This means having security metrics and a maturity model, employing security by design across the entire ecosystem, and for resilience, ensuring interoperability and adaptability of systems at all levels."

"In a highly interconnected digital civilisation, cloud services are the dominant way to access and consume information technologies. Data will usually be stored and processed by other parties as cloud Infrastructures and software services. Stronger encryption, enhanced cryptographic techniques

[1] https://ec.europa.eu/digital-single-market/en/news/net-cloud-magazine
[2] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents

with special attention to low power requirements for the 2025 world of billions of resource constrained devices and their applications that enable encrypted processing and policy based decryption techniques are the only way to ensure that data remains opaque in transit, at rest, and during processing and accessible only those persons with legitimate access."

"The size and complexity of collected data in most cases leads to the use of cloud technology and to their storage at external cloud-based repositories using cloud-based services, which offer flexibility and efficiency for accessing data. While appealing with respect to the availability of a universal access to data and scalable resources on demand, and to the reduction in hardware, software, and power costs, the outsourced storage may produce the side effect of exposing sensitive information to privacy breaches. The security and privacy requirements then create the need for scalable and well-performing techniques allowing the secure storage and management of data at external cloud providers, protecting their confidentiality from the cloud providers themselves. However, protecting data means ensuring not only confidentiality but also integrity and availability. Integrity and availability of data in storage means providing users and data owners with techniques that allow them to verify that data have not been improperly modified or tampered with, and that their management at the provider side complies with possible availability constraints specified by the data owner. The variety of data formats (i.e., structured, unstructured, and semi-structured) makes the definition and enforcement of such techniques a challenging issue."

- **Results of the FP7 CAPITAL project evaluation**[3]

"As part of the research CAPITAL analysed over 30 research agendas on cyber-security, at a European and international level in order to feed into the work of the Final Research Agenda, over 300 research activities were extracted and have been clustered. One of the cyber security and privacy topics selected was Security of Cloud Computing.

Key research challenges identified:

- A research challenge will be to study virtualization architectures to enable full security/performance isolation at all levels (e.g., I/O, memory, TLB, cache) as well as data flow analysis in hypervisors applying statistical machine learning to detect attacks.
- Current Service Level Agreements are mostly directed towards the prevention of legal action against vendors and offer insufficient security assurances to customers. A research question therefore is how customers can be empowered in their legal relation to vendors.
- As service providers in most cases do not have access to the physical security system of data centres, they must rely on the security measures taken by the infrastructure provider. An important research question related to this is how a situation can be reached in which service providers and other parties involved can assess and evaluate the security measures taken by the infrastructure provider. Trust mechanisms should be built on every architectural layer of the cloud.
- Secure cloud interoperability; the ability of separate clouds to exchange and use each other's data in a secure way. Many public cloud networks are configured as closed systems, which makes it difficult for organisations to benefit from shared data. A research challenge is the development of industry standards that help cloud service providers to develop secure interoperable platforms.
- Security of public clouds, especially new vulnerabilities (e.g., are cryptographic crossVM side channels feasible?) and countermeasures for new threats (e.g., placement algorithms).
- As cloud computing is a relatively new domain, security risks should be investigated that might appear in the future (e.g. side-channels, reactive stability, cross-layer robustness and digital preservation)."

[3] http://www.capital-agenda.eu/files/CAPITAL_D4.4_11302015.pdf

5.3 Market Dimension

5.3.1 *Market Alignment*

This indicator assesses the alignment of TREDISEC key innovation points to current and forecasted market trends. This assessment entails a continuous monitoring of market evolution with regards to some strategic aspects:

- Evaluate how TREDISEC results help to bypass known barriers that prevent adopting cloud services.
- Evaluate how TREDISEC results contribute to build incentives that foster the adoption of cloud services in both public and private sectors.
- Evaluate how TREDISEC-based cloud solutions could constitute a benefit that SMEs may exploit (since SMEs do not always understand all the information security risks and opportunities of cloud computing).

Market Alignment provided by ISP Consortium members

ATOS

The Atos Scientific Community defines Atos' vision for the major trends and future business challenges regarding digital technologies, and considers how these will be addressed by emerging technologies.

In 2016, the Atos Ascent Journey 2018 [23] has been released to reflect Atos' Scientific Community Vision. In this issue, a number of 3rd Digital Revolution Challenges have been identified. One of them is the provisioning of trusted Cloud Services with guaranteed levels of Data Security & Privacy and regulatory compliance.

The core of TREDISEC is to provide a set of security primitives that will ensure the confidentiality and integrity of the outsourced data and computations to the cloud. Therefore, we believe that the TREDISEC project is well aligned with Atos Scientific Community research agenda.

IBM

In its most recent issue, IBM's Journal of Research and Development focused on Managed Cloud Services [24]. Articles including "Building the IBM Containers cloud service", "Building scalable, secure, multi-tenant cloud services on IBM Bluemix" and "Managing sensitive applications in the public cloud" give an insight on how latest technology is incorporated in IBM's cloud solutions, and show that research on security and privacy for cloud solutions continues to be of great interest.

Market Alignment provided by ISP Consortium members

IBM (cont.)

TREDISEC's research agenda is well aligned with this interest, developing solutions for the following problems:

- Client-side deduplication provides a very powerful mechanism to reduce storage and communication cost in the cloud storage environment. Unfortunately, client-side deduplication introduces security vulnerabilities that have been already exploited in the past. Dropship [25] is one of the most cited examples that showed how to exploit client-side deduplication in Dropbox. A countermeasure to this issue is offered by the so called "Proof of Ownership" (PoW) that requires the cloud storage user to prove she indeed knows the file she is trying to access. The goal of the TREDISEC project is to make PoW widely available and accessible.
- Security primitives such as containers have significantly contributed to resource isolation in the cloud. Still, software vulnerabilities in resource monitors, such as OS kernels, are uncovered on a regular basis. Security aspects of one of the most popular resource monitors that power today's cloud software stacks, the Linux kernel, is becoming of interest to the public [26].

TREDISEC's research towards improving research isolation includes, among others, attack surface reduction for the Linux kernel, and is thus well aligned with these concerns.

NEC

Trust in Digital Life Alignment

NEC, represented by Dr. Ghassan Karame, chaired a session on cloud security at the annual conference of Trust in Digital Life in the Hague, the Netherlands. The topic of the session was the need to reconcile security and functional requirements in the cloud. Besides shedding light on this event and advertising the various research activities conducted in TREDISEC, this session acquired considerable feedback from various representatives from the TDL consortium, EEMA, and various industry experts. It was evident from the animated discussions that the topic addressed by TREDISEC, which basically consists of reconciling security and functional requirements in the cloud, aligns very well with the agenda of the TDL consortium. This is further evident from the recent publication from the TDL consortium (available from https://trustindigitallife.eu/publications/research-publications/tdl-strategic-research-agenda/) which urges for the need for cloud security mechanisms that are workable, effective, and can be easily integrated with current clouds.

NEC Technical journal

TREDISEC's research agenda is well confirmed by the NEC's periodical "NEC technical Journal". In an issue released in early 2016, researchers from NEC published in this periodical a 5 page article in Japanese and English, outlining the need for integrating security mechanisms in the cloud that are compatible with storage efficiency techniques, such as data compression and data deduplication.

Market Alignment provided by ISP Consortium members

SAP

According to Gartner "What is Cloud Security?" [27] security and/or privacy concerns are still the main reason why companies do not plan to use the public cloud. Furthermore, the Gartner report "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence" [28] says that in 2020 enterprises have to shift information security from a device and network-centric strategy to an information centric strategy. The reason is that network, server, and applications may no longer be in control of enterprises.

TREDISEC is concerned with providing a secure storage of data within the cloud. SAP especially envisions a secure, encrypted cloud database which works against the number one fear of cloud computing. Additionally, a cloud database fits the scenario of the mentioned control loss while the encrypted database fits the information centric security strategy. SAP's research within TREDISEC is based on the frequently cited concept of adjustable encryption by Popa et al. [29] that describes a possible approach for an encrypted database. This work is from 2011, but it was since further developed (e.g. in [30]), including work by SAP (e.g., [31], [32], [33]). However, the inevitable transition from an unencrypted on-premise database to an encrypted cloud database is still an open challenge. It is straightforward to encrypt all data, but it may easily take months to do this naively, and the system has to be offline during this transition. SAP fosters research on this area, and works on the required solution within TREDISEC, thus contributing to the shift to information centric security strategies needed by customers to move to a secure cloud solution.

5.3.2 *Company´s Strategic Fit*

This indicator evaluates how ensuring the alignment of TREDISEC outcomes to individual project partners' strategic market objectives/lines (e.g. business/exploitation plans) will have a positive effect in maximizing the success of the Technology Transfer (TT) process, and, thus, the exploitation opportunities.

Company´s Strategic Fit provided by each individual consortium member
ATOS
The innovative security primitives developed within the TREDISEC project will help Atos to improve its cloud security portfolio. Atos vision is involved in the objective of enabling a Trusted European Cloud. TREDISEC can contribute in the research about cloud certification, aligned with this purpose. Atos has periodic ongoing discussions with Canopy, the Atos Cloud, to analyse how TREDISEC outcomes could enrich Atos offering. Additionally, there are promising possibilities to enrich other Atos solutions such as yourSAM (Secure Attribute Management), and Atos MASS (Managed Application Storage Services).
ARSYS
TREDISEC outcomes will impact the portfolio of Arsys by increasing the security offers of some of Arsys products. Online storage and cloud storage are potential products that would benefit from TREDISEC, as these products could add premium security services to those customers that are especially interested in advanced security features. Arsys estimates that it may take around 6 months to integrate TREDISEC's technology output in its products.
EURECOM
As an engineering school in telecommunications, EURECOM expects to integrate the findings of the TREDISEC project results into new courses on cloud security. Future modules of the security track of EURECOM's curriculum will also greatly benefit from the findings of TREDISEC in the field of security and privacy in the cloud. EURECOM already defined three semester projects (MSc projects) on the topics of verifiable computation, verifiable storage, and searchable encryption which were successfully completed. Furthermore, by participating in TREDISEC, EURECOM reinforces its position within the scientific community in the areas of security and privacy for the cloud. Another benefit of developing an expertise on cloud security and privacy is the technology transfer to EURECOM's consortium of academic and industrial partners. EURECOM also offers dedicated training programmes for its industrial partners' personnel on a regular basis.
ETH Zurich
ETH is using TREDISEC outcomes to improve education and research. In terms of education, ETH started one semester project which has been completed successfully, and helped the student gain a deeper insight into cloud security technologies. Additionally, ETH has started three master theses with topics connected to TREDISEC. In this theses students gained a better knowledge about cloud storage technologies, isolation solutions, and secure enforcement of policies. Furthermore, ETH leverages TREDISEC outcomes in its lectures and thereby also transfers the knowledge to students.

Company´s Strategic Fit provided by each individual consortium member

ETH´s (cont)

In terms of research, TREDISEC's outcomes are a vital part in ETH's research work, and form a solid foundation that ETH will continue to build upon. TREDISEC's outcomes provide deeper understandings that will aid future research especially related to cloud storage and isolation solutions based on trusted hardware.

GRNET

GRNET plans to utilize the majority of the security schemes developed by the project. Besides, GRNET's cloud service ~okeanos is the perfect recipient for numerous primitives. Through well controlled test cases on the already implemented infrastructure, GRNET aims to continue its efforts on improving cloud security for its clients, while also providing its academic users with better research opportunities on the cloud security area. Currently, GRNET is trying to identify primitives that could be integrated in ~okeanos. Concretely, the "container privacy and isolation" primitive is in the first integration stages with more to follow. While the result of the project is going be around TRL 5/6, after the integration of the various primitives with GRNET's cloud service, it is expected to have products with TRL 7 or 8.

IBM

As the largest European branch of IBM Research, IBM Research Zurich's mission, in addition to pursuing innovative research for tomorrow's information technology, is to cultivate close relationships with academic and industrial partners. IBM Research Zurich strives to help driving Europe's innovation agenda.

The research agendas pursued as part of TREDISEC are aligned with the product portfolio offered by IBM's Cloud Business Unit. IBM's cloud portfolio caters to many needs: Bluemix is a platform-as-a-service, Softlayer is an infrastructure-as-a-service, and both Cleversafe and Spectrum Scale are storage solutions. The close connection between research and development divisions within IBM allows for early evaluation of research prototype, efficient products integration, and alignment with customer interests.

NEC

Expanding on its SaaS, IaaS and thin client solutions, NEC plans to use this technology to enhance current products in this area by focusing on production-ready security components, thereby making them more attractive and competitive in the market. NEC research laboratory is in contact with the relevant business units for operations and development of the SaaS Marketplace, Cloud Manager, VDC, and storage solutions. It is expected that parts of the technology developed by NEC Laboratories Europe in the context of TREDISEC will be funneled back to NEC's product portfolio to further differentiate NEC's cloud products. As an example, the secure deduplication technology, Clearbox, which is partly funded by TREDISEC, has been exhibited as parts of NEC's Cloud offering at the Mobile World Congress in February 2016 in Barcelona, Spain. In addition to its infrastructure and cloud provider services, NEC is also a cloud application developer for its own end-users, such as is the case of the ISP NEC Biglobe, and a system integrator.

SAFRAN MORPHO

The new technologies produced within the project are expected to be combined with Safran Identity and Security's biometric system solutions. Authentication based on verifiable computing techniques may be used by Safran Identity and Security within the FIDO alliance for supplying strong online authentication. Verifiable computation technologies could also enhance Safran Identity and Security's solutions at airport gates. In particular, they might be used to accelerate the throughput at the boarding gates. Lastly, the processing of encrypted biometric data might be used on the one hand, for private identification over encrypted biometric database, and on the other hand, for processing encrypted biometric images. At the time of this writing, current innovations achieved within the project belong to the TRL 2-3 level.

Company´s Strategic Fit provided by each individual consortium member
SAP
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 recently announced as a 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 seamlessly deployed 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 our main stakeholders for transferring and exploiting the research results. It is of utmost importance to create visibility, determine the product roadmap, and involve the developers and development managers in the exploitation process. We therefore created the following updated exploitation plan for TREDISEC.

5.3.3 *Organizational Dimension*

This indicator evaluates the following aspects at the level of each individual consortium organization:

- Staff diversification: new roles created in the company structure, new Labs, Units, etc. due to TREDISEC project.
- Competence strengthening: enhancement of existing capabilities, or new knowledge creation.
- Corporate culture shift: incorporation of end-to-end security cloud solutions to corporate tools and procedures, commitment of top management roles in related events, influence in corporate strategy and governance model (from static perimeter security to decentralization of security policy and security governance).

Organizational Dimension provided by each individual consortium member
ATOS
The TREDISEC project has definitely contributed to create new jobs in Atos. Two new members hired in 2015, at the beginning of the project, are currently working in the project, specifically in the Communication and Exploitation activities. Additionally, TREDISEC is an opportunity for the company to acquire knowledge about state-of-the-art technologies related to Data Security and Privacy in Cloud Services, one of the main challenges defined by the Scientific Community of Atos for the 3rd Digital Revolution, that is, an agenda-setting initiative in upcoming years.
ARSYS
The TREDISEC project has contributed to Arsys' organization by creating knowledge in the security area of cloud services, especially around access issues and encrypted data. No new jobs were created so far.

Organizational Dimension provided by each individual consortium member

EURECOM

TREDISEC has given EURECOM the opportunity to hire one PhD student working on the project's topic. EURECOM also offers internship opportunities: currently an internship student is working on the implementation and benchmarking of one of the TREDISEC's primitives.

ETH Zurich

TREDISEC has severely impacted ETH's human resources. More specifically, TREDISEC has led to new fields of work, new cooperations and generally enhanced knowledge about TREDISEC-related issues in the workforce.

TREDISEC has given ETH's employees the opportunity to explore new fields of work, and work in new, challenging environments. Employees were able to learn about the research efforts of TREDISEC partners, and made direct contact with them, leading to multiple lines of cooperation.

Internally, TREDISEC helped to give ETH's workforce a deeper understanding of new emerging technologies such as Intel's Software Guard Extensions (SGX), and sparked ideas on how such technologies could be used in the future. Finally, some of ETH's existing competences, e.g., in the area of secure deletion, were strengthened, thus allowing ETH's employees to pursue research in this area.

GRNET

TREDISEC has provided GRNET with the opportunity to recruit new personnel with expertise in the cloud security field from top universities around the world. Additionally, the work done in TREDISEC provides GRNET with the knowledge to enhance its cloud service ~okeanos with more efficient security features, and identify new threats, thus making the infrastructure more robust and secure.

IBM

IBM Research Zurich strives to be one of the premier places to work for top researchers, and to promote women in IT and science.

To drive the research agendas in TREDISEC, IBM Research Zurich opened several positions for both student interns and regular employees. On the one hand, student interns allow IBM to both maintain and deepen ties with universities by transferring knowledge back to the higher education sector. On the other hand, hiring regular employees shows prolonged interest in TREDISEC's research agendas, and ensures that the knowledge gained in the course of the project becomes a permanent asset. To integrate and exploit the outcome of TREDISEC research into IBM's product portfolio, additional resources in the corresponding product teams will be required.

NEC

NEC Laboratories Europe focuses on software-oriented research and development of technologies to enable advanced solutions for society. NEC Laboratories Europe provides an excellent working environment supporting individual creativity as well as strong teamwork. The TREDISEC project has offered the security group of NEC Laboratories Europe a good opportunity to intensify cloud security research, and to collaborate with the various European partners involved in TREDISEC. Moreover, TREDISEC enabled the security group of NEC Laboratories Europe to diversify the staff members, increase their cloud security job openings, and to offer a number of additional internships in the area of cloud security research.

Organizational Dimension provided by each individual consortium member

SAFRAN MORPHO

The benefit of the TREDISEC project for Safran Identity and Security is the enhancement of its knowledge about verifiable computing technologies, and technologies for processing encrypted data, especially encrypted biometric data. Verifiable computing techniques are relatively new and the TREDISEC project is a key step for Safran Identity and Security to acquire both knowledge about these technologies, and capabilities to apply these new techniques to the biometric field. Techniques for processing encrypted data developed within the project will enhance existing Safran Identity and Security's knowledge for achieving private biometric processing. With regards to human resources, a PhD student has been appointed.

SAP

The work on TREDISEC is part of the internal project SEEED which aims at providing a secure database system which can be used as hosting provider for storing encrypted customer data, while still being able to run queries over the encrypted data. For the TREDISEC project, SAP specifically hired two PhD students. Additionally, the aim for productization of the research results of SEEED will create further impact on resources within other units of SAP. Moreover, SAP’s Security Research department, which works on TREDISEC, developed and gained new knowledge on encryption schemes and their applicability for its customer’s applications. Such new insights are being actively propagated internally in the company via several communication channels.

6 Conclusions

This document presented in detail the current progress of the TREDISEC project with regards to Innovation Management activities.

The given preliminary overview of present-day cloud security market affirms the importance of TREDISEC for both users and enterprises. TREDISEC's main innovation points provide a long-sought solution for security and privacy issues that no technology in the market is currently able to offer. Such objectives will remain relevant even in the face of a continuously evolving cloud market.

Additionally, this deliverable provides a detailed innovation management report of three general assembly meetings held in 2015/2016, as well as an up-to-date assessment of the innovation level within each technical WP in TREDISEC, which clearly show that, as a direct consequence of the partners work toward achieving some of the project's milestones, the innovation level of TREDISEC is thriving, and the risk that the project goals lose relevance over time is negligible. This has been confirmed by means of quantitatively assessing the innovation level achieved by TREDISEC using the framework described in deliverable D1.5.

During the remainder of the project lifetime, we foresee the following innovation management activities:

- Continuously monitor market trends to support the definition of the business cases and plan sustainability activities.
- Monitor the WP progresses according to the Innovation Strategy and propose necessary actions to be taken if necessary.
- Regularly assess the innovation level of the project with regards to a set of innovation-related indicators grouped into framework dimensions.

Finally, in the late stages of the project, we plan the following activities:

- Conduct an assessment of the maturity of the project technical results to support the exploitation and sustainability plans.
- Produce a report on the main innovations and achievements of the project and identify candidates for a technology transfer process.
- Provide input to the exploitation and sustainability plan with regards to the procedure to handle potential market opportunities.
- Introduce our solutions to end-users and acquire their feedback on the usability of and services offered by the solutions.

7 References

[1] MarketsandMarkets, “Cloud Security Market worth $8.71 Billion by 2019,” 2015. [Online]. Available: http://www.marketsandmarkets.com/PressReleases/cloud-security.asp.

[2] “Boxcryptor - Encryption software to secure files in the cloud,” [Online]. Available: https://www.boxcryptor.com/en. [Accessed 21 November 2016].

[3] “IBM Cloud Object Storage,” [Online]. Available: https://www.ibm.com/cloud-computing/products/storage/object-storage/. [Accessed 21 November 2016].

[4] “Wuala,” [Online]. Available: https://en.wikipedia.org/wiki/Wuala. [Accessed 21 November 2016].

[5] “Swisscom Residential Customers: Mobile, TV, Internet and fixed network,” [Online]. Available: https://www.swisscom.ch/en/residential.html. [Accessed 21 November 2016].

[6] “Telefónica,” [Online]. Available: https://www.telefonica.com/. [Accessed 21 November 2016].

[7] HP, “Optimizing storage solutions for unstructured and archival data,” [Online]. Available: https://www.hpe.com/h20195/v2/getpdf.aspx/4AA4-9855ENW.pdf?ver=1.0.

[8] C. Suisse, “IT Hardware & Global Communications Technology,” 2014. [Online]. Available: https://doc.research-and-analytics.csfb.com/docView?language=ENG&format=PDF&source_id=csplusresearchcp&document_id=1027437471&serialid=%2baVamKvWkbJz1Rl9fUGbZnbIGNmotE0aq2ny3bmxpdk%3d.

[9] F. Armknecht, J.-M. Bohli, G. O. Karame and F. Youssef, “Transparent Data Deduplication in the Cloud,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communication Security (CCS)*, 2015.

[10] G. K. C. S. S. C. Hubert Ritzdorf, “On Information Leakage in Deduplicated Storage Systems,” in *Proceedings of the ACM Cloud Computing Security Workshop (ACM CCSW)*, Vienna, Austria, 2016.

[11] D. Vasilopoulos, M. Önen and K. M. R. Elkhiyaoui, “Message-Locked Proofs of Retrievability with Secure Deduplication,” in *Cloud Computing Security Workshop (CCSW)*, Vienna, 2016.

[12] L. B. J.-M. B. G. K. Frederik Armknecht, “Mirror: Enabling Proofs of Data Replication and Retrievability in the Cloud,” in *USENIX Security*, Austin, TX, 2016.

[13] K. E. a. M. Ö. a. M. A. a. R. Molva, “Efficient Techniques for Publicly Verifiable Delegation of Computation,” in *ACM ASIACCS*, Xi'an, China, 2016.

[14] H. C. F. K. R. L. a. E. S.-V. Julien Bringer, “Some Applications of Verifiable Computation to Biometric Verification,” in *WIFS*, Rome, Italy, 2015.

[15] Y. Shoshitaishvili, R. Wang, C. Salls, N. Stephens, M. Polino, A. Dutcher, J. Grosen, S. Feng, C. Hauser, C. Krueger and G. Vigna, “Driller: Augmenting Fuzzing Through Selective Symbolic Execution,” in *Proceeding of the Network and Distributed System Security Symposium*, 2016.

[16] M. Bellare, S. Keelveedhi and T. Ristenpart, “DupLESS: Server-aided Encryption for Deduplicated Storage,” in *Proceedings of the 22nd USENIX Conference on Security (USENIX SEC)*, 2013.

[17] P. Puzio, R. Molva, M. Önen and S. Loureiro, “PerfectDedup: Secure data deduplication,” in *10th International Workshop on Data Privacy Management (DPM)*, 2015.

[18] J. Stanek, A. Sorniotti, E. Androulaki and L. Kencl, “A Secure Data Deduplication Scheme for Cloud Storage,” in *18th International Conference on Financial Cryptography and Data Security (FC)*, 2014.

[19] W. Feng, M. Kohler and A. Schaad, “Initial Encryption of large Searchable Data Sets using Hadoop,” in *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, 2015.

[20] A. Ghassane, J. Bringer and R. Lescuyer, “Searchable Encryption for Biometric Identification

Revisited.," in *International Workshop on Data Privacy Management*, 2016.

[21] N. A. B. P. Jian Liu, "Secure Deduplication of Encrypted Data without Additional Independent Servers," in *ACM CCS*, 2015.

[22] S. X. Qingji Zheng, "Secure and efficient proof of storage with deduplication," in *ACM CODASPY*, 2012.

[23] Atos, "Ascent White Papers," 2016. [Online]. Available: https://ascent.atos.net/ascent-white-papers/.

[24] IBM, *Journal of Research and Development,* vol. 60, 2016.

[25] "Dropbox snuffs open code that bypassed file-sharing controls," 26 04 2011. [Online]. Available: http://www.theregister.co.uk/2011/04/26/dropbox_moves_to_squash_open_source_dropship_project/.

[26] T. W. Post, "The kernel of the argument," 05 11 2015. [Online]. Available: http://www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument/ .

[27] Gartner, "What is Cloud Security?," 21 07 2016. [Online]. Available: http://www.gartner.com//it/content/3347100/3347121/july_21_what_is_cloud_security_jheiser.pdf?userId=91802990.

[28] Gartner, "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," 27 01 2016. [Online]. Available: https://www.gartner.com/doc/2500416?srcId=1-3931087981.

[29] R. A. Popa, C. S. Redfield, N. Zeldovich, H. Balakrishnan and M. Catherine, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," in *Symposium on Operating Systems Principles (SOSP)*, 2011.

[30] S. Tu, M. F. Kaashoek, S. Madden and N. Zeldovich, ""Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013.

[31] F. Kerschbaum, M. Härterich, M. Kohler, I. Hang, A. Schaad, A. Schröpfer and W. Tighzert, "An Encrypted In-Memory Column-Store: The Onion Selection Problem," in *ICISS*, 2013.

[32] F. Kerschbaum, M. Härterich, P. Grofig, M. Kohler, A. Schaad, A. Schröpfer and W. Tighzert, "Optimal Re-encryption Strategy for Joins in Encrypted Databases," in *DBSec*, 2013.

[33] P. Grofig, M. Haerterich, I. Hang, F. Kerschbaum, M. Kohler, A. Schaad, A. Schroepfer and W. Tighzert, "Experiences and observations on the industrial," SAP, 2014.

[34] European Comission, "How to convert research into commercial success stories? Analysis of EU-funded research projects in the field of industrial technologies," 2013. [Online]. Available: http://ec.europa.eu/research/industrial_technologies/pdf/how-to-convert-research-into-commercial-story-part2_en.pdf. [Accessed June 2015].

[35] Microsoft, "Microsoft cluster shared volumes," 2013.

[36] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramchandran, "On compressing encrypted data," *IEEE Transactions on Signal Processing,* 2004.

[37] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon and M. Theimer, "Reclaiming Space from Duplicate Files in a Serverless Distributed File System," ICDCS, 2002.

[38] M. Bellare, S. Keelveedhi and T. Ristenpart, "Message-locked Encryption and Secure Deduplication," in *EUROCRYPT*, 2013.

[39] M. Bellare, S. Keelveedhi and T. Ristenpart, "DupLESS: Server-Aided Encryption for Deduplicated Storage," IACR Cryptology ePrint Archive, 2013.

[40] D. Harnik, B. Pinkas and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," in *IEEE Security & Privacy*, 2010.

[41] S. Halevi, D. Harnik, B. Pinkas and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in *Computer and Communications Security (CCS)*, 2011.

[42] NIST, Computer Security Division, “Attribute-based access control”.

[43] X. Jin, R. Krishnan and R. S. Sandhu, “A unified attribute-based access control model covering DAC, MAC and BAC,” in *DBSec*, 2012.

[44] F. Kerschbaum, P. Grofig, I. Hang, M. Härterich, M. Kohler, A. Schaad, A. Schröpfer and W. Tighzert, “Adjustably encrypted in-memory column-store,” in *ACM Conference on Computer and Communications Security*, 2013.

[45] A. Schaad and F. Kerschbaum, “Experiences and observations on the industrial implementation of a system to search over outsourced encrypted data,” in *GI Sicherheit*, 2014.

[46] E. Blass, R. Di Piedro, R. Molva and M. Onen, “PRISM: Privacy-Preserving Search in MapReduce,” in *Privacy Enhancing Technologies Symposium* , 2012.

[47] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *STOC*, 2009.

[48] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, “Provable data possession at untrusted stores,” in *ACM Conference on Computer and Communications Security*, 2007.

[49] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson and D. Song, “Remote data checking using provable data possession,” 2011.

[50] G. Ateniese, R. Di Pietro, L. Mancini and G. Tsudik, “Scalable and efficient provable data posession,” in *SecureComm*, 2008.

[51] A. K. C. P. R. T. C. Erway, “Dynamic Provacble Data Possession,” in *16th ACM Conference on Computer and Communications Security (CCS)*, New York, USA, 2009.

[52] B. K. A. Juels, “PORs: Proofs of Retrievability for Large Files,” in *14th ACM Conference on Computer and Communications Secruity (CCS)*, New York, USA, 2007.

[53] A. Shamir, “How to Share a Secret,” *Communications of the ACM,* pp. 612-613, 1979.

[54] Agile Alliance, “"What is Agile Software Development?",” 2013. [Online]. Available: http://www.agilealliance.org/the-alliance/what-is-agile/. [Accessed April 2015].

[55] European Conmission, “Communicating EU research and innovation,” 2014. [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-guide-comm_en.pdf. [Accessed June 2015].

[56] European Commission, “Net-Cloud Future,” 2013. [Online]. Available: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/NET-CLOUD_DIGITAL-AGENDA_clickable_0.pdf. [Accessed June 2015].