SecureDataCloud Final Project Report

Document information	
Project Title	SecureDataCloud
Project Number	E.02.27
Project Manager	[redacted] - Innaxis
Deliverable Name	Final project report
Deliverable ID	N/A
Edition	01.02.00
Template Version	03.00.00
Task contributors	
Innaxis, ITU, DHMI and team&cloud	

Abstract

The final report of the WP-E SCLOUD (SecureDataCloud) Project provides a publishable summary of the results. In addition it lists all deliverables, dissemination activities, eligible costs, deviations, bills and lessons learned.

Authoring & Approval

Prepared by - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] / Innaxis	Project leader	25/09/2015
[redacted] / ITU	WP3 Leader	25/09/2015
[redacted] / ITU	Consortium member	25/09/2015
[redacted] / ITU	Consortium member	25/09/2015
[redacted] / ITU	Consortium member	25/09/2015
[redacted] / ITU	Consortium member	25/09/2015
[redacted] / DHMI	Consortium member	25/09/2015
[redacted] / team&cloud	WP2 Leader	25/09/2015
[redacted] / team&cloud	Consortium member	25/09/2015
[redacted] / team&cloud	Consortium member	25/09/2015
[redacted] / team&cloud	Consortium member	25/09/2015

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] / Innaxis	Project leader	25/09/2015
[redacted] / team&cloud	WP2 Leader	25/09/2015
[redacted] / ITU	WP3 Leader	25/09/2015

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organizations.*		
Name & Company	Position & Title	Date

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
[redacted] / Innaxis	Project leader	25/09/2015

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
01.00.00	25/09/2015	Available for Internal review	INX	New Document.
01.01.00	20/10/2015	Revised version	INX	Comments from ECTL addressed.
01.02.00	16/11/2015	Revised version	INX	Comments from SJU addressed.

Intellectual Property Rights (foreground)

This deliverable consists of Foreground owned by SJU.

Table of Contents

List of tables

List of figures

No table of figures entries found.

Publishable Summary

Overview of SCLOUD

SecureDataCloud has been the first project to demonstrate the feasibility and usefulness of the application of SMC techniques to air transport problems. At the core of the project are:

- the review of the state of the art in SMC techniques;
- the identification of a set of AT scenarios in which SMC could be applied, to facilitate a seamless information sharing between different stakeholders; and
- the creation of a prototype allowing the execution of secure computations in two Case Studies.

These objectives were designed to answer the following research questions:

- Do existing SMC algorithms and protocols fit the needs (in terms of security levels and quantity of information being handled) of Air Transport?
- Does SMC effectively remove existing barriers in terms of data sharing for new operational procedures that leverage data sharing paradigms in the ATM domain?
- What are the benefits in terms of new (not previously allowed due to the confidentiality of data) business models that lean on relevant data sharing in ATM?

High-level conclusions from the project were that:

- There is a clear need for SMC solutions in AT and ATM, as demonstrated by the interest expressed by numerous stakeholders, and by the large number of relevant scenarios identified.
- Available SMC algorithms and SMC software frameworks are been shown to solve most of the problems encountered, with acceptable complexities and computational cost.
- SMC techniques and their implementation have also been shown to be suited to cloud environments, ensuring their scalability to large number of stakeholders.
- Technical issues to achieve commercial readiness have been identified, mainly related to system integration tasks between different components for automated scalability, high reliability and continuous operation in the required highly distributed computing solution.
- From the user side, it is feasible to develop simple interfaces, *e.g.* by means of web-based systems, to interact with the SMC libraries, thus minimizing the cost from this user side.

SecureDataCloud has reached a TRL4 level of maturity, including a laboratory assessment of the integrated secure computation elements and an evaluation of the performance of the system. Future research work will be focused on the integration of SMC with existing AT concepts, *e.g.* SWIM; and on addressing technical issues, like the design of mechanisms for supervising the correct execution of the computation.

The need for an SMC approach in AT

The air transport, as all other socio-technical systems, is always in the search of ways for improving its cost efficiency. Programs pursuing this aim have appeared throughout the world: SESAR in Europe, NextGen in USA, OneSky in Australia, SIRIUS in Brazil, or CARATS in Japan. Beyond these different names, they all share a similar concept: efficiency can be improved only by ensuring a continuous flow of information between the agents and stakeholders involved in the operation. Some

examples include sharing future trajectory intentions by aircraft, negotiations for slot exchange by airlines, or the continuous monitoring of global mobility and CO_2 emissions. Such data flow is also necessary when increasing safety is the objective, *i.e.* in the analysis of past incidents and accidents, thus of historical operational data.

Achieving such seamless flow of information entails two important and contradictory challenges. First, most ATM data are considered confidential and sensitive and, hence, private - both for their commercial value, and for the political or social consequences some of the analyses may cause; any solution should thus guarantee an adequate level of confidentiality. Second, at the same time, data should be stored and processed in a safe and efficient way, which usually implies the use of a *cloud*-based infrastructure. This may generate security problems, as the exact location of data in the cloud is generally not known [1].

Present solutions, like SESAR's System Wide Information Management (SWIM) [2], only partially tackle these two problems. Specifically, SWIM is based on a public-key infrastructure, allowing users to only access those sets of data included in their authorisation class. Data are released to the parties requiring them, hence the security of the system is as good as the security of the worst procedure implemented by the entities. As a result, the usefulness of the whole paradigm depends on trust: both between users, and between these and the system managers.

A completely different approach to this problem is provided by the use of *secure computation techniques*, allowing dealing with confidentiality issues without limiting the ability of performing relevant computation on private data. Generally speaking, *Secure Multi-party Computation* (SMC) is a set of techniques and algorithms that allows two or more untrusted parties to perform some kind of computation over a data set, while keeping their respective information private. Thus, once the computation is over, the only new information that each party should possess is the output of that computation, without any additional knowledge on the information provided by the other party. In other words, instead of providing any party with the full data set (and thus creating a security issue to be managed) or denying the access to it (effectively blocking any possibility of using the data), the data owners could allow third parties to run computations on encrypted information, without real access to the full dataset. Secure computation has hitherto been used to solve several real-world problems, from secure sealed-bid auction [3], elections with an electronic voting scheme [4], benchmarking [5], up to defense applications in military operations [6].

In spite of the large number of scenarios in which computations on private data should be executed, SMC has never been evaluated in air transport. The goal of SCLOUD is therefore to assess the impact that such technology may have in AT / ATM, through the development of two relevant Case Studies, and through the study of the limiting factors (*e.g.* computational cost, theoretical complexity) that may prevent a wider adoption.

Business Cases and Case Studies selection

As a first step, the project identified a large set of Business Cases, *i.e.* high-level description of situations in which SMC can solve a current or future problem in air transport and ATM, or can help improving the efficiency of the system by allowing a seamlessly information sharing between different partners. Among others, they included:

- airport slots and CO_2 allowances trading;
- airlines ranking, both considering business elements (flight efficiency, occupancy rates, *etc*.) and the behaviour of their own pilots (*e.g.* number of safety events encountered in specific routes);
- airport CO_2 and noise fees estimation;
- secure ATFM, *i.e.* involving flights whose trajectories cannot be fully disclosed;

- anomalies detection in safety data, *e.g.* detection of abnormal days or airspace regions from a safety point of view;
- secure analysis of delay reports;
- contingency planning, involving the optimisation of resources of both airports and airlines during abnormal operations;
- secure auditing of airline financial status.

Of these, two have been selected for further development. The selection has been performed by merging different criteria, including: their relevance for AT and ATM, as assessed through several consultations with relevant stakeholders (including airports and ANSP key people, airline managers, *etc.*); their feasibility, in terms of algorithms and protocols availability; and the availability of real and/or synthetic data for their evaluation. The selected Case Studies are:

1. **Slots trading.** This Case Study deals with the secure trading of airport slots, merging three different scenarios. In the first market scenario, it is considered that an airline is planning to operate a new route between two airports. Therefore, at a strategic level, the airline first tries to buy slots from both airports, *i.e.* in the primary market. Second, an airline can also attempt to buy a suitable slot in the secondary market, *i.e.* from other airlines. The third scenario is the trading of specialized trajectories, *e.g.* a slot in a priority landing queue at a given airport, which is characterised by a shorter timeframe than the first two scenarios (that is, the auction should be executed within some strict time constraints). Although the reason for participating in the market corresponding to such third scenario is slightly different than the first two, such as lower fuel cost and lower delay, the underlying market mechanism is similar, as both the buyer and the seller do not want to reveal their bids. As entities with commercial concerns, both the buyers and the seller do not want to reveal their business strategies. Thus, in an auction, they do not want the other parties to know their bidding prices so as to not reveal any sensitive information.

2. **Analysis of delay reports.** This second Case Study aims at defining a system of delay reports using cleared information coming from different participants, securely merged in order to achieve additional knowledge about causes of delays. Here, *cleared information* refers to delay information whose causes and amounts have already been processed by the stakeholders, thus reaching a consensus about them. The following four statistical analyses are performed on those delay data: (*i*) statistical indicators related to the delay minutes of all flights in a route during a specific time window; (*ii*) airlines ranking by means of total delay minutes in a route during a specific time window; (*iii*) statistical indicators related to the delay minutes of each cause in a route during a specific time window; and (*iv*) statistical indicators related to the delay minutes of all the flights in a route during a specific time window, excluding each airline's flight with the highest delay – and thus excluding extreme values.

The first Case Study has also been extended to the secure trading of CO_2 allowances, as presented in [7, 8].

Key results

In order to implement the two Case Studies previously described, two software elements have been developed:

1. **A set of SMC libraries**, designed to perform the secure computations required by each Case Study. Among their characteristics, it is worth mentioning that: (*i*) they have been implemented in Java, to ensure cross-platform operability; (*ii*) communications between all machines are encrypted according to the TLS standard; and (*iii*) data input and output are

performed through CSV files, in order to simplify the interface with external programs, including UI or automatic data processing software [9]. The basic secure computational elements of the system have been drawn from SEPIA, a free open-source library [10]. This ensured that all used algorithms have a solid theoretical background, published and peer-reviewed in international journals and conferences; and that the implementation of those algorithms can also be validated by the scientific community. All developed SMC libraries will be openly distributed to any SJU member requiring it.

2. **A web-based interface**, enabling a simple interaction with the SMC computational engine. This interface manages all interactions with the users, from his/her authentication, gathering of their inputs for the secure computation, output display, up to computation configuration functions. The system has been developed as a web service, accessible through Java Server Pages (JSP). A Tomcat v7.0 server operates all activities of the users (*e.g.* login, registration, selection of trade). The login information of the participants and the data set associated with the computation are stored in a MySQL database. In order to reach this database through the Java platforms, the system utilises a JDBC (Java Database Connectivity) interface. The next Figure depicts some screenshots of the interface.

The complete software system was tested using synthetic data sets, created in order to mimic the kind of data that would be expected in an operational scenario. For the first Case Study, these have been generated by an *ad-hoc* Slot Demand Allocation Model (SAM) algorithm. Starting from flight-track data and airport capacity reports, it calculates the desired departure and arrival time of each flight, for then applying a random noise to this information. As a result, the SAM algorithm can generate synthetic (yet realistic) slot interests, by simulating the collective behaviour of a set of airlines interested in the same resource. Delay data for the second Case Study have been obtained by combining delay calculation models for each phases of the flight, with available real flight, ATM event and meteorological data. The delay causes library (as in the IATA-Airport Handling Manual) is used as a model, by selecting a subset of delay codes that can be modelled as airline- or CFMU-dependent. A set of significant days in Europe have subsequently been selected, in which some special events (*e.g.* adverse weather) took place, and delays for all affected flights estimated.

Conclusions and a look ahead

The most important conclusion reached by the project is that **SMC techniques can, and should be applied in AT / ATM**. As for the possibility, it should be noticed that the algorithms and libraries that can be found in the Literature have always been created with a different application in mind; nevertheless, they can be adapted to the kind of problems encountered in air transport. As in any software adaptation process, this may require some effort, as input data requirements may be different, and because public libraries are not always fully documented. As for the necessity of applying SMC, in all organised interviews with stakeholders, as well as in all spontaneous interactions with colleagues at different air transport conferences and events, a strong interest towards such techniques has emerged. Everyone perceives that there is a plethora of different scenarios in AT / ATM, in which some computation has to be performed on private data; and that the value of such data, or simply a problem of trust between the involved parties, usually limit the possibilities for collaboration. SMC then appears as a simple solution, allowing overcoming these problems with a minimum increase in technical complexity.

One of the mains challenges limiting the applicability of SMC to real-world problems is the large computation cost required to perform even simple analyses. Even an operation as simple as comparing two numbers using SMC requires multiple computational steps, from dividing the initial data in shares to manipulating them in separate servers. The situation is even more complicated when non-linear operations are included in the mix, like multiplications, which greatly increase the computational complexity and the evaluation cost. SCLOUD demonstrated that this limitation can be avoided by combining good programming techniques (in terms of data preparation and handling) with a *cloud*-based architecture. Even with high numbers of participants, all analyses described in this document can be performed in less than one minute, well below the time constraints set by, for instance, a slot trading problem.

At the end of the project, SecureDataCloud has reached a TRL4 level of maturity: a laboratory assessment has been completed, integrating all the elements of the system, and evaluating the performance with respect to the requirements expected in future applications (*e.g.* computing times). This validation has been developed with realistic data, in order to mimic as closely as possible future implementations. In spite of the positive results here obtained, we foresee that more research work will be needed to reach higher levels of maturity, *i.e.* to get closer to an operational deployment.

Specifically, two challenges have to be overcome. First, the integration of SMC with AT concepts like SWIM. While the latter is mainly a data and information transfer infrastructure, it may be used as the backbone for connecting different parties performing a secure computation; this will require an understanding of the limitations of the infrastructure (*e.g.* available bandwidth), and a subsequent adaptation of available SMC algorithms. Second, any SMC computation is inherently a "black box": no external actor can interfere with it, nor obtain knowledge about the computation being performed. This may be a problem from an AT validation point of view, in which it may be desirable to have a central authority overviewing the correct functioning of the system. Solving this problem will require both IT and SMC research: the former to design way of monitoring the exchanged information, the latter for opening the algorithms to an external supervisor, without jeopardizing the security of the computation.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to:

- summarise the technical results and conclusions of the project (see 'Publishable Summary');
- provide a complete overview of all deliverables;
- provide a complete overview of all dissemination activities (past and in progress), where appropriate, providing feedback from presentations;
- describe exploitation plans;
- provide a complete overview of the billing status, eligible costs, planned and actual effort (including an explanation of the discrepancies);
- analyse the lessons learnt at project level.

1.2 Intended readership

This report is written for the professional reader and assumes an understanding of air transport and ATM. A basic knowledge of Secure Multiparty Computation concepts is also advisable, although not essential for understand the content of the document.

1.3 List of acronyms

Acronym	Meaning
AT	Air Transport
ATM	Air Traffic Management
CFMU	Central Flow Management Unit
IATA	International Air Transport Association
SEPIA	Security through Private Information Aggregation (Library)
SMC	Secure Multiparty Computation
TRL	Technology Readiness Level

2 Technical Project Deliverables

Number	Title	Short Description	Approval status
D1.1	Business Cases analysis	This first deliverable of the project presents an introduction to the field of Secure Multi-party Computation, the subfield of cryptography dealing with the computation of functions over private data sets. It defines its main characteristics and available techniques, along with real-world examples of SMC applications. The document further presents and describes a set of Business Cases, *i.e.* air transport and ATM scenarios in which Secure Multi-party Computation is expected to provide a benefit to involved stakeholders. (52 pages)	Approved
D1.2	Business Cases selection	This document reports on the selection of the two Business Cases that are to be developed and implemented in future phases of the project, by taking into account both the availability of real data and suitable algorithms to construct and validate a prototype, and several interviews with stakeholders. (20 pages)	Approved
D2.1	Report on Analysis of Algorithms	This document reports on the business and technical requirements for the implementation of the two Case Studies (previously Business Cases), as described in D1.2 Slot Trading & Dynamical Landing Queues and Analysis of Delay Reports. All requirements can be classified in two groups: those related with the characteristics of the system to be implemented, thus including both hardware, software and user interface; and the mathematical requirements of the SMC algorithms, as needed to execute the computations in a secure way. Both sets of requirements have been developed using the User Stories methodology; user stories have been written after outlining the complete business model, including a list of relevant usage scenarios, the roles that intervene in the prototype and the high-level requirements that define the Case Studies as a whole. Additionally, a recommendation of the mathematical algorithms needed to implement the Case Studies has been done. These algorithms are implemented (in D2.2) by means of SMC protocols, leveraging in the operations provided by an open-source software framework. (47 pages)	Approved
D2.2	Report on Framework Implementation	This deliverable reports on the development of the Secure Multiparty Computation libraries, as required for the two Case Studies addressed in the project. The full life-cycle of the libraries is described: from the rationale of their architecture, executed unitary tests, basic deployment instructions, up to the integration in cloud computing environments. It also defines a global Cloud computing reference architecture for SMC. (206 pages)	Approved
D3.1	Simulation and Data Model for Case Studies	This document reports on simulation and data models for the two Case Studies considered in the project. First, three market simulation frameworks, for the “Slot Trading & Dynamical Landing Queues” Case Study, are described, including strategic primary market, strategic secondary market and operational primary market. They rely on a Slot Demand Allocation Model (SAM) algorithm to generate potential slot interests, starting from historical flight-track data and airport capacity reports. In the second part of the report, a simulation prototype for the “Analysis of Delay Reports” Case	Approved

		Study is developed, based on delay calculation models for each phases of the flight and available real flight, ATM event and meteorological data. The delay causes library (as in the IATA-Airport Handling Manual) is used as a model, and the delay reporting is distilled to a subset of this library inline with the available real data. (69 pages)	
D3.2	Results from case studies	This document reports on simulation results and processed data sets for the two Case Studies considered in the project. The synthetic data sets generated in D3.1 have been used to simulate real SMC computations, through a web-based system incorporating the SMC libraries developed in D2.2. An extensive analysis of results is presented, along with practical considerations (as, for instance, the computational cost and scaling properties of the system). (374 pages)	Submitted
D4.1	SID participation	For details, please see Section 3. (10 pages)	Approved
D4.2	SID participation	For details, please see Section 3. (11 pages)	Approved

Table 1 - List of Project Deliverables

3 Dissemination Activities

An on-line dissemination and exploitation plan is maintained in the project's development website, for the partners' planning of future opportunities, which already extend beyond the project close-out. Selected activities are listed below and include some firm future commitments.

3.1 Presentations/publications at ATM conferences/journals

Event	Location and date	Title of presentation	Description (and feedback)
SESAR Innovation Days 2013	Stockholm 16/11/13	*SecureDataCloud: Introducing Secure Computation in ATM*	Poster presenting the main objectives of the project, and the main principles behind SMC. The poster attracted the attention of several people. Of special interest has been the interaction with the members of the WP-E ALIAS 2 project, who were interested in the liability consequences of the use of secure computation techniques. More generally, feedbacks received have been positive, with good interest in the possibilities offered by such approach.
Legal and Social Impact of Automated Systems in Aviation	Firenze 02/10/14	*SecureDataCloud Project: Legal Challenges*	Presentation about the legal challenges associated to the use of SMC technologies in ATM. The full video recording of the presentation is available in YouTube.
SESAR Innovation Days 2014	Madrid 25/11/14	*Enabling the Aviation CO_2 Allowance Trading Through Secure Market Mechanisms*	Presentation about how SMC can be applied to an AT problem, specifically a CO_2 allowance trading. General positive feedbacks received.
Journal of Air Traffic Management	N/A	*Performance metrics and scenarios in ATM*	(Submitted) Invited paper, extending the results presented at the SESAR Innovation Days 2014 talk.

3.2 Presentations/publications at other conferences/journals

Event	Location and date	Title of presentation	Description (and feedback)
IEEE Services 2015 - Visionary Track: Security and Privacy Engineering	New York 28/06/15	*Design and Implementation of a Secure Auction System for Air Transport Slots*	Presentation of the SMC libraries developed in the project, and their application to the problem of slot trading. The contribution was well received, especially by some people in the audience who were experts in SMC. Positive feedbacks were received about the web interface of the library, and about efficiency (low computation time).
IEEE Services 2015 - Visionary Track: Security and Privacy Engineering	New York 28/06/15	*Design and Implementation of a Secure Auction System for Air Transport Slots*	Poster synthesising the main point of the corresponding talk.

In addition, the following dissemination activities are being completed or planned:

- Participation to the SESAR Innovation Days 2015 (December 2015, Bologna), and presentation of a talk with the main outcomes of the project.

- The outcome of D1.1 is being used to create a "review / opinion" paper, *i.e.* firstly reviewing the SMC techniques available in the Literature, and secondly presenting how could these techniques be beneficial for AT and ATM. Such publication may create a high impact in the sector, as it would be the first one merging SMC and air transport.

3.3 Demonstrations

A first prototype of the SMC libraries and web interfaces were presented at the SESAR Innovation Days 2014. Several people interacted with the demonstrator, and expressed their interest in the technology. Especially noteworthy has been the case of Roland Guraly, of the company Slot Consulting Ltd. Further contacts with them have been planned for the end of the project.

3.4 Exploitation plans

This Section presents the main guidelines for the future of the SecureDataCloud concept, explaining the main steps to be taken in order to fully exploit the technology in the Air Traffic Management context.

We consider that SecureDataCloud has reached a TRL4 level of maturity: a laboratory assessment has been completed, integrating all the elements of the system (including the computing engine, web-based interfaces and a cloud deployment), and evaluating the performance of the system with respect to the requirements expected in future applications (*e.g.* computing times). This validation has been developed with realistic data, in order to mimic as closely as possible future implementations.

Not just the technology itself has been evolved: each one of the partners involved in the Consortium has benefitted from the participation in the project, and has gained new knowledge that will be exploited in the future. More in detail, ITU has gained a higher visibility of the SESAR's long-term research & innovation plans. In addition this project was a great opportunity to fuse ITU's already existing experience on air transportation technical data analytics with commercial aspects associated within the air transportation realm. Specifically, exposure to concepts such as SMC and case studies such as slot management, delay reporting and CO_2 emission trading enhanced the local vision and the capabilities. Team&Cloud has gained first hand experience in an area, SMC, that will eventually emerge as critical for distributed multi-authority IT systems, as these systems strive to solve new business needs in a trustful way. This project has reduced the technical risks for an SMC solution, since it has shown that it was feasible at a reasonable cost. It will allow Team&Cloud to progress towards commercial implementation, working in two directions: additional SMC business applications, and cloud integration, for ATM. Additionally, this project represented a great opportunity for Innaxis to master the techniques and concepts of SMC, which are planned to be used in future research projects.

A special note should be devoted to DHMI participation. It's been the first time for DHMI, one of the biggest ANSP (3rd last year as per managed traffic, expected 2nd this year) and airport operator in Europe, to realize and work with the application of SMC. Following this perspective, DHMI convened different stakeholders in İstanbul Atatürk Airport (air traffic controller, slot managers, TAV airport operator managers, Turkish Airlines pilots) in order to analyze different air transport scenarios that can benefit from an SMC application. A large set of Business Cases was extensively analyzed by DHMI, results were discussed at multiple meetings, and two of them were selected for further developments and integration. Consequently, while analyzing these two scenarios with different stakeholders and agreeing that most of the ATM data are confidential and private for the aviation

companies, the SMC application is seen as very valuable and useful, since it allows executing some kind of computation over the aforementioned private ATM data while keeping the corresponding information private. Currently, DHMI is using its own auction system for slot trading in İstanbul Atatürk Airport. But after working on this project and exploiting the results, DHMI operational experts find the use of SMC technologies as cost effective and feasible, including its cloud feature. From an operational point of view, Secure Data Cloud project has been a good starting point to solve safe auction problems in AT, and this system can be further developed and used not only for slot trading or delay reports but also for most of the auctions in AT/ATM systems, especially for the airport operators and airlines. On the other hand, collaborative information collecting and computation through SMC, which was another demonstration of SecureDataCloud project through the delay reporting, has an also good potential for cooperative operational processes such as collaborative decision-making.

The future commercial implementation of SMC in ATM will require a deeper understanding of the challenges created by operational environments. In what follows, some exploitation guidelines are provided, following the standard TRL scale. Although the TRL scale is marked by milestones, it is more realistic to forecast a gradual evolution throughout it, which is better described by considering two future steps: first operational environment trials; and shadow mode and deployment.

Future Step 1 -The laboratory validation and first operational environment trials

This step encompasses from TRL 5 to 7, *i.e.* from a laboratory validation phase to a demonstration in an operational environment. At the end of the process, an actual system prototype should be developed, at the scale of the planned system and operating in real operational conditions. The infrastructure prototype must provide acquisition, validation and represented assessment through an automated procedure. The TRL7 laboratory should be an operational fault-tolerant environment: beyond the assessment of the algorithm robustness and stability, aspects such as privacy, confidentiality and security should be implemented and monitored.

Future Step 2 - Shadow mode and deployment

TRL8 shall achieve shadow mode operations and an operational qualification milestone, *i.e.* the actual system must be completed and evaluated through tests and demonstrations in the operational environment. At this level, developments for most technology elements should be concluded, shifting the focus to the integration of the new technology into an existing system. The infrastructure leaves the laboratory and moves into production, and all data-related elements of the system are integrated on the operational environment. Also, the algorithms are qualified for operation through appropriate methodology or certification procedure.

Finally, TRL9 is the milestone in which an actual system is proven operationally fit through a successful mission operation. This TRL does not include planned product improvement of on-going or reusable systems; however, the data infrastructure operation is monitored, improved and enhanced as needed by the system operation.

The challenges inherent each one of these future steps should be analysed during future projects planning, in order to understand the strengths, weaknesses, opportunities and threats for the implementation and deployment of SecureDataClouds in Europe.

4 Total Eligible Costs

Date	Deliverables on Bill	Contribution for Effort	Contribution for Other Costs (specify)	Status
09MAY14	D0.0; D0.1; D0.2; D1.1; D4.1	90.885,00 €	8.303,42 € (travel); 529,10 € (meeting room)	Paid
25NOV14	D0.3; D0.4; D1.2; D2.1	142.416,25€	5.915,26 € (travel); 30,00 € (communication material)	Paid
25AUG15	D0.5; D0.6; D2.2; D3.1; D4.2	202.323,75 €	4.197,21 € (travel); 95,00 € (meeting room); 138,81 € (communication material)	Pending
OCT15 (estimated)	D0.7; D0.8; D3.2	127.338,75 €	7.193,25 € (travel)	Pending
DEC15 (estimated)	-	-	5.497,95 € (travel); 100,00 € (communication material)	Pending
GRAND TOTAL		**562.963,75 €**	**32.000,00 €**	**594.963,75 €**

Table 2 - Overview of Billing

Company	Planned man-days	Actual man-days	Total Cost	Total Contribution	Reason for Deviation
Innaxis	577	577	297.155,00 €	222.866,25 €	-
Team&Cloud	590	590	206.500,00 €	154.875,00 €	-
ITU	724	724	155.660,00 €	155.660,00 €	-
DHMI	275	275	59.125,00 €	29.562,50 €	-
GRAND TOTAL	**2.166**	**2.166**	**718.440,00 €**	**562.963,75 €**	-

Table 3 - Overview of Effort and Costs per project participant

5 Project Lessons Learnt

What worked well?
State of the art SMC algorithms and freeware libraries have proven that secure computation can effectively be used to solve AT problems. The computational cost, usually an important limiting factor in real-world SMC applications, has proven to be low enough to support the analysis proposed in the project.
The joint effort of different types of partners, including scientific, technical and aeronautical backgrounds, enabled a very rich development process, in which different expertise and points of view have successfully been integrated.
The feedbacks received in the different dissemination activities have highlighted the perceived importance of the SMC approach, with people stating their interest in the development of libraries for different AT problems.
Despite the partners being based in multiple European locations, remote from each other, they collaborated very well together in the on-line tool used (InGrid) for day-to-day communications, project planning, model development, and deliverable production.
The Project Officer was supportive and flexible regarding appropriate planning and timescale changes and helped to keep the administrative burden down.
What should be improved?
More theoretical work may be needed to fulfil all AT requirements. Some analyses, involving nonlinear mathematical operations, had to be approximated, due to the lack of suitable secure algorithms.
It might be useful to have more tools for submitting results, complementing the “deliverables” system. In some cases (see D2.2 and D3.2), the need of including large sets of data in the deliverables dramatically increased their size. This may have been avoided if the submission of appendices in other formats (*e.g.* Excel spread sheets) had been possible.

Table 4 - Project Lessons Learnt

6 References

[1] Kaufman, L. M. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE*, *7*(4), 61-64.

[2] Meserole, J. S., & Moore, J. W. (2007). What is System Wide Information Management (SWIM)?. *Aerospace and Electronic Systems Magazine*, IEEE, 22(5), 13-19.

[3] Damgård, I., Geisler, M., & Krøigaard, M. (2007, January). Efficient and secure comparison for on-line auctions. In *Information security and privacy* (pp. 416-430). Springer Berlin Heidelberg.

[4] Vegge, H. (2009). Realizing secure multiparty computations.

[5] Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying secure multi-party computation for financial data analysis. In *Financial Cryptography and Data Security* (pp. 57-64). Springer Berlin Heidelberg.

[6] Pathak, R., & Joshi, S. (2009). Secure Multi-party Computation Protocol for Defense Applications in Military Operations Using Virtual Cryptography. In *Contemporary Computing* (pp. 389-399). Springer Berlin Heidelberg.

[7] Zanin, M., *et al.* (2014). Enabling the Aviation CO2 Allowance Trading Through Secure Market Mechanisms. SESAR Innovation Days.

[8] Zanin, M., *et al.* (2015). Performance metrics and scenarios in ATM. Journal of Air Traffic Management. Submitted.

[9] Zanin, M., Pereira, E. A., Mirchandani, V., Enrich, A., & Triana, J. C. (2015, June). Design and Implementation of a Secure Auction System for Air Transport Slots. In *Services (SERVICES), 2015 IEEE World Congress on* (pp. 160-166). IEEE.

[10]Burkhart, M., Strasser, M., Many, D., & Dimitropoulos, X. (2010). SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics. *Network*, 1, 101101.