RestAssured

Secure data processing in the cloud

Deliverable D9.2

Impact Plan

Release 1.0

The research leading to these results has received funding from the European Community's H2020 Research and Innovation programme under grant agreement n◦ 731678.

IBM ADAPTANT iT innovation THALES Oxford Computer Consultants PALUNO UNIVERSITÄT DUISBURG ESSEN

Secure data processing in the cloud

RestAssured

Author(s):	Balint Nagy; John Boyle
Responsible Partner:	OCC
Version:	0.1
Date:	09/04/2017
Distribution level (CO, PU):	PU

Project Number:	H2020 - 731678
Project Title:	RestAssured

Title of Deliverable:	Impact Plan
Due Date of Delivery to the EC:	Month 4, 30/04/2017

Work Package:	WP9
Contributor(s):	Balint Nagy, OCC
Reviewer(s):	Eliot Salant
Approved by:	Eliot Salant

Document Revision History

Version	**Date**	**Modifications Introduced**	
		Reason	**by**
0.0	12/01/2017	First Version	Balint Nagy, OCC
0.1	11/04/2017	Content added, merged partner contributions, applied RestAssured document template	John Boyle Balint Nagy
0.2	27/04/2017	Updated based on review comments and suggestions from Eliot Salant.	Balint Nagy

RestAssured Consortium Partners and Acronyms

OCC	OXFORD COMPUTER CONSULTANTS LIMITED
IBM	IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD
Adaptant	ADAPTANT SOLUTIONS AG
ITInnov	UNIVERSITY OF SOUTHAMPTON
THALES	THALES SERVICES SAS
UDE	UNIVERSITAET DUISBURG-ESSEN

Glossary of Terms and Abbreviations

EU	European Union

Contents

List of Tables

1. Executive Summary

This plan sets out the channels and protocols by which partners communicate outside of the project, establishing a consistent and clear message, including dissemination and communication.

This document gives an overview of all dissemination opportunities identified through traditional communication channels such as event attendance (conferences, seminars, workshops), project publications (leaflets, press releases, conference papers, articles) and project presentations These activities are complemented by online activities based around the project website, and through the main social platforms (Twitter, Facebook). The dissemination activities will target the key project audiences and stakeholders and to maximise awareness of the project's objectives and training activities.

2. Introduction

2.1 Abstract

The success of the RestAssured project is subject in part to the ability of its partners to identify, reach and engage the potential users of the project's technical outcomes. In this sense, an effective liaison between the project and its interested stakeholders is a key factor for the replication and rapid uptake of the RestAssured platform. The set-up of the appropriate communication channels and materials will be carefully designed to create the most effective engagement tools.

2.2 Purpose of this Document

This Impact Plan provides directions for conducting concrete actions related to the dissemination and exploitation of the RestAssured project. This document intends to cover all dissemination and exploitation steps, from the correct and prompt identification of external users to the use of dissemination tools and its success analysis. Therefore, it defines an overall communication strategy and a set of tools for dissemination.

It also analyses and details how the consortium will organise itself to maximise the impact of the project results.

3. Context and Key Messages

RestAssured is a research project which is meant to show a new software architecture for data protection/privacy on the Cloud. While RestAssured itself is not aimed at creating a commercial product, it is expected that project results and spinoff technologies will be commercially utilised both by the partner organizations, and by third-parties wishing to take advantage of RestAssured research.

Therefore, our communication will be targeted at the scientific and business communities.

3.1 Image

RestAssured should be the enabler for increased trust in clouds through stronger security and data protection practices.

RestAssured wants to improve the competitive position of the European cloud sector and to facilitate the emergence of innovative business.

3.2 Brand

We created branding material for the RestAssured project. This consists of the following:

- Logo: In .png format, various sizes, for dark and light environments.
- Branding Guide: Describes the logo itself, graphical usage information, examples on how it should and should not be used, colour palettes and fonts to create printed and electronic material, with practical information on how to use those components.
- Word document template. A ready to use, RestAssured brand-conform source for Word documents.
- PowerPoint template. RestAssured brand-conform presentation template.
- A LaTex document template is also available.

3.3 Target Groups

A set of key messages have been defined to transmit the principal objectives of the project so that they reach and impress the diverse target groups. The key messages have been chosen according to their purpose and target audience. They should be clear, focused, understandable and easy to remember. According to the nature of the target group, the focus of the messages should be technical, societal, commercial or political. The groups identified so far are the following:

3.4 Target groups and key messages

Audience	Message	Channels
Service providers	RestAssured provides enabler technology to build services that provide secure data processing in the cloud. Encourage service providers to include such secure data processing in their offerings.	Conferences Project newsletters Social media
Cloud providers	Encourage cloud providers to offer secure data processing on their platforms. Use RestAssured technology to gain trust and confidence with their customers. European cloud providers should use RestAssured technology to gain advantage over the competition.	Conferences Project newsletters
Enterprise cloud users	Secure cloud has come of age. Secure data processing based on RestAssured technology allows them to migrate more of their applications to the cloud. Such a cloud offering is trustworthy.	Conferences Indirect via service providers
Individual citizens	Cloud-based data processing can be secure. Increase awareness of the RestAssured technology.	Social media Project website

Audience	Message	Channels
Academic	RestAssured will use cutting-edge technologies and practices, tested in realistic scenarios.	Conferences Project newsletters Scientific papers Open Source releases
Government	RestAssured technology can support governmental privacy directives, such as GDPR.	Project website Project newsletters Scientific papers

Table 1: Key messages for each target group of the RestAssured project

3.4.1 Complimentary Projects

We have identified other EU projects that may benefit from RestAssured results, whose results RestAssured could benefit from, or may otherwise be interested in each other's work. RestAssured will maintain an awareness of the progress being made in these efforts, and, where there appears to be a high potential for collaboration, reach out to these other efforts either individually, or through Commission-driving initiatives.

EU Research Projects

Name	ID	Why Complimentary
OPERANDO - Online Privacy Enforcement, Rights Assurance and Optimization	653704	The goal of the OPERANDO project is to specify, implement, field-test, validate and exploit an innovative privacy enforcement platform that will enable the Privacy as a Service (PaS) business paradigm and the market for online privacy services. The OPERANDO project will integrate and extend the state of the art to create a platform that will used by independent Privacy Service Providers (PSPs) to provide comprehensive user privacy enforcement
ACTiCLOUD - ACTivating resource efficiency and large databases in the CLOUD	732366	Despite their proliferation as a dominant computing paradigm, cloud computing systems lack effective mechanisms to manage their vast amounts of resources efficiently, leading to severe resource waste and ultimately limiting their applicability to large classes of critical
UNICORN - A novel framework for multi-cloud services development, orchestration, deployment and continuous management fostering	731846	Unicorn aims to simplify the design, deployment and management of secure and elastic – by design - multi-cloud services. This will be achieved by a) development and design libraries that will provide security enforcement mechanisms, data privacy restrictions, monitoring metric.

cloud technologies uptake from digital smes and startups		
PrEstoCloud - PrEstoCloud - Proactive Cloud Resources Management at the Edge for Efficient Real-Time Big Data Processing	732339	PrEstoCloud project will make substantial research contributions in the cloud computing and real-time data intensive applications domains, in order to provide a dynamic, distributed, self-adaptive and proactively configurable architecture for processing Big Data streams.
CloudPerfect - Enabling Cloud Orchestration, Performance and Cost Efficiency Tools for QoE Enhancement and Provider Ranking	732258	Cloud environments are notorious for their lack of stability in performance characteristics, a feature that makes it extremely difficult for owners of time-critical applications to make the decisive step for migration and owners of SaaS to be unable to present performance vs cost trade-offs to their customers when acting as IaaS customers. CLOUDPERFECT will enable a) Cloud providers to enhance the stability and performance effectiveness of their infrastructures, through modelling/understanding of the overheads, optimal groupings of concurrently running services, runtime analysis and adaptation
mF2C - Towards an Open, Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem	730929	Fog computing brings cloud computing capabilities closer to the end-device and users, while enabling location-dependent resource allocation, low latency services, and extending significantly the IoT services portfolio as well as market and business opportunities in the cloud
CloudDBAppliance - European Cloud In-Memory Database Appliance with Predictable Performance for Critical Applications	732051	The project aims at producing a European Cloud Database Appliance for providing a Database as a Service able to match the predictable performance, robustness and trustworthiness of on premise architectures such as those based on mainframes.
COLA - Cloud Orchestration at the Level of Application	731574	SMEs and public sector organizations increasingly investigate the possibilities to use cloud computing services in their everyday business conduct. Accessing services and resources in the cloud on-demand and in a flexible and elastic way could result in significant cost savings.
MELODIC - Multi-cloud Execution-ware for Large-scale Optimized Data-Intensive Computing	731664	MELODIC will enable data-intensive applications to run within defined security, cost, and performance boundaries seamlessly on geographically distributed and federated cloud infrastructures. Serving the user's needs and constraints, MELODIC will realise the potential of Cloud computing for big data and data-intensive applications by transparently taking advantage of distinct characteristics of available private and public clouds and dynamically optimise resource utilisation.
DITAS - DITAS: Data-	731945	There is an increasing need to develop data intensive

intensive applications Improvement by moving daTA and computation in mixed cloud/fog environments		applications able to manage more and more amounts of data coming from distributed and heterogeneous sources effectively, quickly, correctly, and securely. However, the current adoption of Cloud Computing paradigm is not fully appropriate to store and analyse such data: latency, security, and compliance are still significant barriers.

Other Related Research Projects

Project	Summary
Innovate UK ASSURED	This project aims to speed up and improve the security assurance procedures for applications connected to the UK NHS network by using models and machine reasoning. The focus is on modelling application networks and supporting analysis of risks to the application including risks of non-compliance with NHS regulations, and exploitation of the resulting models for run-time compliance checking at an NHS-connected data centre. Like RestAssured, ASSURED aims to exploit models created at design time to analyse and maintain security compliance at run-time in applications involving the collection and use of personal data. www.it-innovation.soton.ac.uk/projects/assured

Table 2: List of other complimentary research projects

4. Dissemination

4.1 Tools

In the final year of the project, we intend to produce a 2-3-minute animation video explaining the RestAssured tools and methodologies developed during the project and illustrating the benefits that RestAssured assured brings to different sectors as demonstrated in our use cases.

4.1.1 Website

The project website is available at the address www.restassuredh2020.eu and will act as a single point where all the latest information, outcomes and achievements will be available in a structured way, compared to the social media accounts of the project that will also include all the latest information, given on a spontaneous basis.

The website contains sections that are suitable to host the various kinds of content to be available during the project. The website news will be regularly updated to reflect the latest developments, upcoming events etc.

The first official launch of the RestAssured website took place on M3 of the project (March 2017). A first set of information was included regarding the aim of the project, the list of the partners in the consortium and how to contact the project.

The site has been created such that content can be added easily. We will publish project related events in an on-going manner throughout the project.

4.1.2 Scientific Publications and Conferences

The dissemination of the scientific results of RestAssured is a major goal for the project. To that end, the project will be emphasizing the presentation of its results both in scientific papers and journals, as well as through presentations and participation in high profile European conferences.

4.1.3 Twitter

Twitter has become a valuable tool for connecting people interested in specific topics and issues. It provides opportunities to listen to conversations and gather information in real-time. This channel is an effective outreach to individuals, organisations, corporations and federal agencies, and will give RestAssured researchers the opportunity to gain Internet visibility for their research.

4.1.4 Facebook

Facebook provides an immediate and personal way to deliver general project information targeted at the end user.

4.1.5 Newsletter

A newsletter is an excellent tool to communicate with the active third parties in the project, and connect with the inactive or absent ones. The newsletter will assure that all third parties are informed and aware of the project results and activities. It will serve to link all interested members into a cohesive unit and build interest in the project. It can be of great assistance in obtaining third parties involvement in the project's activities and create the desired community feeling.

4.1.6 Mass Media, Press Kit

The website of the project serves as the main source of information for any third party, and will distribute project dissemination information, such as the press kit. This kit will be aimed at offering introductory information to the project.

This press kit will contain the following items, either in paper or digital format:

- Letter from the coordinator presenting the project.
- PowerPoint presentation containing introductory information to the project.
- Any audiovisual produced material (images, videos), if available.
- Logo and Branding guide
- Press releases

4.2 Dissemination Team

The Dissemination Team ensures an efficient dissemination activity and a continuous update of contents. The Dissemination Team consists of one representative per partner. Each member is the champion for a target group, where they will lead this activity. However, they will not be the exclusive user of their channel, as every partner will be able to use any tool freely to disseminate project results. The members are:

Partner	Representative
IBM	Eliot Salant
Adaptant	Markus Hasinger
ITInnov	Mike Surridge
OCC	Reynold Greenlaw
Thales	Dhouha Ayed
UDE	Andreas Metzger

Table 3: Communication team

4.2.1 Partner Responsibilities and Channels

IBM will contribute blogs, tweets, and presentations/publications in relevant scientific forums as part of its RestAssured activities

Adaptant will contribute to dissemination of results in a number of ways, 1) through contributing blogs and social media content across a diverse range of channels to maximise engagement with relevant stakeholder groups, 2) through supporting tone and message consistency across social channels by contributing to editorial planning and content

scheduling, 3) through privacy-related industry events related to RestAssured's areas of impact and use cases , and finally 4) through European initiatives in which it is engaged, including the Big Data Value Association, the European Cyber Security Organisation, and the NESSI ETP. Based on Adaptant's work on the High Performance Computing (HPC) use case, future engagement of the ETP4HPC is also envisioned.

ITInnov will coordinate targeting by the project of scientific journals and conferences. This will include maintaining a target list for scientific publications. At this stage, this list comprises our preferred scientific dissemination channels, i.e. which conferences and journals do we regard as most credible and able to reach the relevant scientific communities (see the table below). During the first year of the project, we will begin to identify specific results that could be published through each of these channels, and help to organise and schedule work on papers across the consortium to ensure that opportunities to publish (especially at conferences) are not missed.

OCC will be the Twitter champion of the consortium thanks to its previous experience in the use of this channel. The Twitter feed will be the diary of the consortium and it will report not only RestAssured project related activities but also more general privacy related news and research that the consortium wants to show and increase awareness around. During the Consortium events, Twitter will be used for the live commentary of such events. OCC will also be the responsible for fostering the connection with public bodies.

Thales In addition to scientific publications, Thales will use European initiatives as channels to disseminate the Rest-Assured results, such as TDL (Trusted Digital Life), the privacy working group and the Public-Private Partnership (cPPP) on cybersecurity.

UDE offers pushing dissemination as part of European activities such as the NESSI ETP and the Big Data Value Association. Through these activities, dissemination channels with other relevant stakeholders, such as EOS and ENISA (for Security) and ARTEMIS-IA (for Cyber-Physical Systems) may be established.

4.3 Strategy for community building on social media

Social channels are the most interactive tools we will use, as these are places for asking questions, sharing thoughts, and replying to other members. The RestAssured Consortium can get the most out of these tools by involving all the potential interested parties by applying these principles:

Be relevant: Social networks are informal spaces. RestAssured will have a real voice that is knowledgeable, genuine and scientifically engaging.

Ask questions: Our followers are not going to comment unless we ask them what they think. We will constantly invite fans to join the discussion by asking questions. This will be an effective way to get feedback and make improvements too.

Share regularly: We will use our social channels to share the latest news in our project. Publishing regular updates will give our followers a reason to keep coming back to our page. This will keep our project in the forefront of people's minds when we show up on their newsfeeds.

Be visual: We will aim to include pictures or other visual media with most of our posts. This will catch people's eyes, create interest, and portray our project as dynamic and exciting.

Expand our content: We believe that sharing regular updates on the project is just as important as sharing different kinds of stories. We aim to share a mix of impactful stories on online privacy issues, announcements for special events, video posts, pictures, surveys, and links to keep interest in our content. We will also share updates that are not just about our project: posting articles about relevant legislation, industry news, highlighting the work of other projects in our field.

4.3.1 Different platform different strategies

Twitter, Not Only Hashtags: One of Twitter's greatest strengths is its ability to link communities. Most people are familiar with hashtags, which, at a basic level, function like the subject line on an email. However, what is more challenging, is finding which are the key people and organisations to follow and reaching them. Just because someone uses a hashtag does not mean they are concerned about the topic on a regular basis. First, RestAssured will look out for big Twitter accounts in our field and start following them (privacy news profiles, ICT companies, and journalists who regularly write about online privacy). Then, look deeper into the follower lists of those profiles, as these are the people who are interested in learning more about privacy online, and they will probably be interested in following RestAssured, too.

Dissemination is all about engagement, and simply following people is not enough; also want to communicate with them. Every time we follow someone, we will add them to a list: privacy news, online-privacy-entrepreneurs, online-privacy- researchers, and as our lists grow, we will have more people to talk with and we will have created wider stakeholder groups to promote our work.

LinkedIn, Groups: On LinkedIn, groups are the best tool for developing a following. We will start by researching groups in our field and join or request an invite to them. Only after getting a minimum recognition on the platform we will have members joining our RestAssured-specific group. Our group interactions will continue to build our network so that we can send direct messages to relevant people as our articles are produced.

Facebook: One of Facebook´s greatest strength is its ability to create awareness and continuously increase the audience. What is more challenging is reaching the target audience for each of the use cases, especially the B2B-oriented ones. The purpose is making people aware of the project itself, the main objectives, the main outcomes, and to point out the benefits for the community. Storytelling as a key issue.

Facebook will be also used to interact and engage with the audience, to get real-time feedback, and to involve them in other privacy-related discussions, especially about social networking privacy.

Moreover, Facebook will be also a direct line with the partners and the main companies and organizations involved in the project.

4.4 Dissemination activities

We understand that throughout the consortium there will be many people communicating to various audiences. Instead of assigning specific channels to partners, we will assign various target audiences to specific members of the consortium, and share the channels to reach those audiences. Also, this communication should be synchronised to represent consistent values, to reinforce a single image. In order to achieve that, OCC will implement an internal wiki page to spread editorial information throughout the consortium. There OCC will compile and present the project vision and main messages, and partners are expected to contribute their pieces of information (like achievements, upcoming events, etc.) to be used as a source of information by communicators.

The relevant events/papers identified in GA 2.2.1

Target Audience (Community)	**Name**	**Description (including reputation / impact)**
Cloud	ICSOC	A-ranked, main international conference on cloud and service-oriented computing
	ESOCC	Premier conference on advances in the state of the art and practice of service-oriented computing and cloud computing in Europe
	CCGRID	A-ranked, major international forum for research results and technological developments in the fields of cluster, cloud and grid computing
Security & Privacy	IEEE Security & Privacy	A-ranked, IEEE Symposium on Security and Privacy
	TrustCom	A-ranked, IEEE International Conference on Trust, Security and Privacy in Computing and Communications
	ESORICS	A-ranked, European symposium on research in computer security

	TrustBus	Long-running, international forum for researchers and practitioners to exchange information regarding advancements in the state of the art and practice of trust and privacy in digital business.
Software Engineering & Computer Science	ICSE	Premier A*-ranked international conference on software engineering
	ESEC/FSE	A-ranked, biannual European software engineering conference (jointly with Fundamentals of Software Engineering conference)
	IEEE Computer	Premier scientific magazine of the IEEE
	Comm. of the ACM	Premier scientific magazine of ACM

The relevant events/papers identified in GA 2.2.2

The project has an ambitioned impact and communication plan. Below, the key events and communication activities are outlined. Some KPIs have been modified from the initial DoA to better adhere to expected obtainable project results

Specific Communication Activities and Assets	**KPI**	**Responsible**
Project Website with RestAssured domain name be created. It will present the project brand and include all public project outputs and documentation.	Website publicly available. Quarterly traffic grows uniformly throughout project.	OCC
Social media such as Facebook, Twitter, SlideShare, LinkedIn. A strong social media presence will help the consortium to reach a wider audience.	Facebook, Twitter, LinkedIn accounts set up at M3. 100 subscribers/friends/followers by M12. 200 subscribers/friends/followers by M36.	All but lead by OCC.
A set of branded official templates (for documents, deliverables and presentations) will be prepared to promote a cohesive project image. These will be accessible to all partners via a private area on the website.	All templates privately available at M3. All public deliverables use templates throughout project.	OCC

Physical marketing assets will be produced including a project brochure and posters. These will be aimed at the general public and will present the impact of the project in accessible language.	Physical dissemination assets available at M6. Revisions available annually.	OCC (reviewed by all partners but in particular IBM)
A six-monthly newsletter will be published to the website and mailed to a list of subscribers. This will present an update on project results, activities and next steps.	Newsletter produced every six months from M6 to M36. Mailing list is 100 at M12. Mailing list is 300 at M36.	OCC to collate but each partners to write the contribution for each WP they lead.
A Github developer forum will be created and maintained.	Github forum available at M6. Github forum maintained and developed throughout project.	OCC
Presentation at academic conferences, workshops and research seminars.	Academic partners to be able to demonstrate communication of RestAssured through academic channels by end of project. Every presentation to be available publicly on website or slideshare.	Duisburg; Southampton; IBM
Scientific and international publications will be produced. RestAssured will preferentially target peer reviewed journals.	Academic partners to be able to demonstrate communication of, or plans to communicate RestAssured through academic channels by end of project.	Duisburg; Southampton; IBM
Presentations to commercial audiences and industry conferences	Industrial partners to be able to demonstrate communication of, or plans to communicate RestAssured to commercial audiences by end of project.	Thales; OCC; Adaptant

4.5 Monitoring, evaluation and reporting

To correctly follow the evolution and correct development of the different dissemination activities and tools described in this document, every partner participating in WP9 has been appointed as directly responsible for one or more activities.

In terms of reporting, the work done in the WP9 “Impact” of this project will be reported with internal reports every 6 months and through official reports sent to the EC every year.

In terms of assessing the success of the activities described in this document, several indicators will be monitored per the following indicators:

- Web activity (Google Analytics tools)
- Targeted activities (number of attendees)
- Media (presence in the press)
- Social networks activity (mentions, followers, friends)
  Since the project includes both B2B and B2C use cases, audience is wide and diverse. Therefore, a combination of qualitative and quantitative KPIs would help validate the social strategy.
    - Quantitative KPIs
        - Followers and fans
        - Social shares
        - Referral traffic
        - Conversions
        - Subscribers
        - Inbound links
    - Qualitative KPIs
        - Sentiment
        - Conversations
        - Comments
        - Mentions
        - Meaningful engagement

5. Exploitation

The main project exploitation activities include:

- Definition of draft joint and individual exploitation plans
- Each partner defines individual exploitation plans
- Concretization, assessment and validation of exploitation plans.

This section outlines how and why each partner will develop their individual exploitation plans. As it is expected that a portion of the RestAssured solution will be proprietary, the project will take a more pragmatic approach to exploitation, namely focusing on exploitation of individual assets, rather than joint exploitation of the entire RestAssured stack.

The final project exploitation plan will include a full business analysis and definition of any potential business models.

5.1 IBM Exploitation Plans

IBM is researching the use of secure enclaves, such as Intel SGX, in RestAssured. Providing both secure cloud-based platform services and a cloud infrastructure platform to

its customers is critical to IBM's line of business. The result of IBM's work in RestAssured will be targeted at strengthening these offerings, exploring opportunities for releasing spinoff technologies both as Open Source and as proprietary offers to existing IBM product lines.

5.2 OCC Exploitation Plan – Outline

OCC is an SME and works closely on several aspects of data protection, privacy in the health and social care domain. We are building and supporting applications to manage the delivery of care services to citizens (oxfordcc.co.uk/products) and currently incubating a social enterprise called Ami (withami.co.uk) to support adults living alone. These are systems in which individuals upload personal data and where individuals have the choice of sharing this data with service providers, carers, as well as their local authority and health professionals.

Our oldest and largest products (SPOCC and ContrOCC respectively) are desktop applications and the take up of cloud services in our target market of health and social care is slow. RestAssured will transform the way OCC can offer cloud-based services to our clients and the credibility with which the cloud is perceived. No current services for the management of social care contain the privacy assurance for citizens managing their own social and health services that this would offer. This will become more prominent with the rollout of the personalization of care as citizens take a more direct role.

Enabling more local government to move health and social care systems into the cloud is in line with the UK Government policy paper "Personalised health and care 2020: a framework for action" which includes "'health-as-a-platform', using technology to break down silos, join up services and reduce duplication…and make use of cloud technology where appropriate." We believe this would result in annual product sales turnover increase of 10%-15%. Since our consultancy services tend to grow in proportion to the product sales, it is reasonable to expect a 10% increase in consultancy services turnover as well.

5.2.1 Specific Exploitation Activities: OCC Social Care Pilots

Ami. At present, all personal data is considered highly sensitive and the pilot organizations we work with are not willing to store this data on the cloud. With RestAssured technology we will introduce peer-to-peer volunteering where personal data about both volunteers and service users is stored in the cloud. Our aim is to go from the 0% of personal data currently stored to having at least 30% of personal data available on the cloud. To achieve this, we will need to:

- demonstrate the ability of the pilot to withstand a range of different types of threats and attacks,
- demonstrate the compliance of RestAssured with data security requirements such as external penetration tests.

Finance Portal. OCC's new finance portal will provide access to client data via the cloud. This is a new OCC product. We will run control experiment with this platform to compare the data protection offered with and without RestAssured.

5.2.2 Commercial Implications

Our two pilots have different commercial objectives and implications. Ami is a social enterprise designed to help people who are lonely and isolated in our communities. It's impact on people's lives is hard to measure though many studies have shown the loneliness has a greater impact on people's health than smoking 15 cigarettes a day. As such Ami will help to reduce to burden on the health and social care systems. It's value to OCC is indirect through the good will Ami builds up with our clients as well as the positive impact on staff and staff retention

Our finance portal will deliver savings to Local Authorities. OCC envisages an annual charge of £15,000 per LA for the finance portal. This means that the potential value of the product to OCC is £1.05M equivalent to an increase of about 14% in OCC's annual turnover.

5.3 Thales Exploitation Plan

One of the objectives of Thales is to further extend its cybersecurity capabilities and offer its customers a comprehensive data protection suite of solutions for protecting enterprises against cybersecurity threats at the highest levels of assurance.

The results of RestAssured are innovative answers to its customers' concerns when it comes to verifiable and enforceable information security and privacy policies and will complement the Thales solutions to enhance privacy, trusted identities, and secure payments with certified, high performance encryption and digital signature technology for customers in a wide range markets including financial services, high technology, manufacturing, and government.

In addition to the contribution of the data protection suite, the results of this project and mainly sticky policy management and security assurance of externalized data are also expected to have a major impact on the capacity of Thales to build security solutions that protect data-at-rest across physical, big data and cloud environments which are one of the strategic goals of Thales especially after the acquisition of Vormetric's to complement Thales's market leading cybersecurity activities, and further strengthens the Group's overall profitable growth strategy.

5.4 Adaptant Exploitation Plan

Adaptant's vision is that through empowering users to take control of their own data, new user-centric business models and services will be realised, fundamentally changing the data

value chain. To this extent, Adaptant's exploitation of RestAssured results will be carried out in a number of ways:

5.4.1 New Market Exploration

Through development of the Use-based Insurance and commercial HPC use-cases, Adaptant will be able to leverage the project outcomes to explore new market positioning opportunities and drive new offerings across the full breadth of its products, solutions, and services. Adaptant will further augment its own offerings with RestAssured technologies as the basis for engaging with promising new and emerging market segments, such as InsurTech, where it presently does not have a market presence, while building on existing competencies.

As part of the exploitation activities, Adaptant will elaborate initial business plans to enable establishment of new products & solutions, as well as market positioning and diversification strategies based on RestAssured results. These will in turn provide the basis for Adaptant's product and solution diversification.

5.4.2 Standards Contributions

Adaptant will drive standardisation contributions in the areas of personal data usage control, particularly in the pre-normative CEN Workshop 84 on a 'Self-Sovereign Identifier(s) for Personal Data Ownership and Usage Control' (CEN WS ISÆN) where Adaptant, as Vice-Chair of the Workshop, is responsible for curating industry requirements, use-cases, and business model innovation, which the RestAssured results will make a direct contribution to.

Contributions to ISO/IEC 24760/27018 applying RestAssured methodologies in secure data processing and cloud storage will also be pursued, together with advances in partial identity management from the implementation of the Usage-Based Insurance use case.

5.4.3 Professional Services and Consulting

Adaptant will round out the exploitation of results by providing bespoke solutions, professional services, and consultancy services across its existing business domains where RestAssured results are able to make a meaningful contribution, while elaborating new services and solution offerings for the new vertical industries driven by use case implementation and resulting tacit knowledge creation across the project lifecycle.

5.5 IT Innovation Exploitation Plan

Measurable results: RestAssured research results are used in future commercial or public funded research. Security analysis tools are released as OSS or on commercial terms directly or through other project partners to SMEs, and supported by consultancy services,

as appropriate. We expect these outcomes to be achieved after, but probably not during the lifetime of the project.

IT Innovation plans exploit the results in collaborative projects supported by public programmes and in professional services, including customer-specific and commercially confidential research and innovation, bespoke development of operational systems for early adopters, and consultancy.

IP we generate is exploited by the above means and via spin-out companies, licensing to partners, and release of Open Source Software, as appropriate. We use OSS as a means of promoting adoption of ideas as well as to promote uptake of the software itself. We choose OSI licenses which prevent closure of our own work while allowing partners to use the software in products without restricting the license terms for their components. We support OSS with associated professional services, we dual-license as needed, and we team with commercial partners for closed source software exploitation. We also consider establishing spin-out companies where appropriate to accelerate the commercial adoption of our technologies.

RestAssured is of particular interest to SMEs. IT Innovation recently completed a study for the UK government into the effectiveness of its Cyber Essentials accreditation scheme for SMEs, and specifically how effective the security measures would be. This revealed that Cyber Essentials is effective in protecting a traditional enterprise network with a well-defined perimeter, but it falls well short of the expected protection when SMEs run services in the cloud, especially when used by mobile workers. We intend to exploit our research in RestAssured within 12 months of the project end, to provide security and privacy analysis tools and associated consultancy to SMEs, including local SMEs contacted in our previous study through the Solent Cyber Security Cluster, and the Federation of Small Businesses.

Measurable results: RestAssured research results are used in future commercial or public funded research. Security analysis tools are released as OSS or on commercial terms directly or through other project partners to SMEs, and supported by consultancy services, as appropriate. We expect these outcomes to be achieved after, but probably not during the lifetime of the project.