The research leading to these results has received funding from the European Community’s H2020 research and innovation programme under grant agreement n° 731678.
<table>
<thead>
<tr>
<th>Project Number</th>
<th>731678</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Title</td>
<td>RestAssured - Secure Data Processing in the Cloud</td>
</tr>
<tr>
<td>Deliverable Type</td>
<td>External Report</td>
</tr>
<tr>
<td>Title of Deliverable</td>
<td>9.3 - First Impact and Innovation Management Summary Report</td>
</tr>
<tr>
<td>Nature of Deliverable</td>
<td>External Report</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Contractual Delivery Date</td>
<td>30 April 2018</td>
</tr>
<tr>
<td>Actual Delivery Date</td>
<td>30 April 2018</td>
</tr>
<tr>
<td>Contributing WPs</td>
<td>All</td>
</tr>
<tr>
<td>Editor(s)</td>
<td>John Boyle</td>
</tr>
</tbody>
</table>
Contents

List of Figures ........................................................................ 5
List of Tables ......................................................................... 6

1 Executive Summary ................................................................ 7

2 Introduction ....................................................................... 8

3 Context and Key Messages .................................................... 9

4 Impact ............................................................................... 10
  4.1 Expected Impacts ............................................................ 10
    4.1.1 Impact-01 (I-01) ......................................................... 10
    4.1.2 Impact-02 (I-02) ......................................................... 12
    4.1.3 Impact-03 (I-03) ......................................................... 16

5 Dissemination ..................................................................... 19
  5.1 Communication Activities and Tools ................................. 19
    5.1.1 Project Website ........................................................ 19
    5.1.2 Social Media ............................................................. 24
    5.1.3 Academic and Research Presentations ......................... 27
    5.1.4 Academic Publications ............................................ 28
  5.2 Common Dissemination Booster (CDB) .............................. 30
    5.2.1 CDB Summary .......................................................... 30
    5.2.2 Next Steps ................................................................. 31
  5.3 Dissemination Plan Task Update ....................................... 32

6 Exploitation ....................................................................... 33
  6.1 IBM Contribution ........................................................... 33
  6.2 UDE Contribution ........................................................... 33
  6.3 Thales Exploitation .......................................................... 33
  6.4 ITInnov Contribution ....................................................... 34
  6.5 Adaptant Contribution ...................................................... 35
    6.5.1 Product Development & Spin-Out Opportunities .......... 36
    6.5.2 GDPR Consultancy Services ..................................... 36
    6.5.3 Intellectual Property Rights ....................................... 36

D9.3 – April 24, 2018 3 of 40
6.6 OCC Contribution

6.6.1 Hosting Solution Costs

6.6.2 Tender Success

6.6.3 Certification, Compliance and Risk Management

6.6.4 Opportunities for Consultancy Services

7 Conclusion
List of Figures

Figure 5.1: Project website Home page ................................................................. 20
Figure 5.2: Project website Publications page ...................................................... 21
Figure 5.3: Project website Blog page ................................................................. 22
Figure 5.4: Monthly users since website launch ..................................................... 23
Figure 5.5: Comparison of website users (last quarter vs first quarter) .................. 24
Figure 5.6: Twitter analytics for the previous 28 days ........................................... 24
Figure 5.7: Twitter statistics January 2018 ............................................................ 25
Figure 5.8: Twitter statistics December 2017 ......................................................... 25
Figure 5.9: Twitter statistics November 2017 ......................................................... 26
Figure 5.10: Twitter statistics October 2017 ........................................................... 26
Figure 5.11: Twitter statistics September 2017 ...................................................... 27
Figure 5.12: CDB stages ......................................................................................... 31
List of Tables

Table 4.1: Expected impacts of a RestAssured approach to Social Care .................................................. 15
Table 4.2: Unique data protection characteristics of the PAYD use case ................................................. 16
Table 4.3: Success metrics for the initial PAYD Demonstrator ................................................................. 17
Table 4.4: Expected impacts of a RestAssured approach to PAYD ............................................................ 18
Table 5.1: Website objectives ..................................................................................................................... 23
Table 5.2: Project website quarterly visitor statistics ................................................................................. 23
Table 5.3: Twitter objectives ...................................................................................................................... 24
Table 5.4: Detailed list of events attended ................................................................................................. 28
Table 5.5: Projects participating in the DPSP cluster ................................................................................. 28
Table 5.6: Detailed list of accepted publications ....................................................................................... 29
Table 5.7: Detailed list of publications for the general public ................................................................. 30
Table 5.8: Dissemination task progress ..................................................................................................... 32
Table 5.9: Dissemination task deviations .................................................................................................. 32
1 Executive Summary

To date the main focus of the project has been to design and build the prototype code. This report explains how the partners will use the prototypes to demonstrate impact by the end of the project. This builds on the D9.2 report since we can now describe the impacts given what we now know about the RestAssured architecture and technologies.

This report shows how the 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. Our impact plans are therefore targeted at the scientific and business communities and the formation of the RestAssured lead Common Dissemination Booster is an important part of this process.

The project has successfully established a good dissemination baseline through a combination of the project website, blog and social media usage. Importantly, given the focus on the scientific and research communities the project has already produced a number of high profile journal and conference publications.
2 Introduction

Note: The named representatives for this deliverable are:

This First Impact and Innovation Management Summary Report outlines our progress against the plans and actions set out in D9.2. This document takes all dissemination and exploitation opportunities defined in D9.2. and reports on what has been done, the impact of what has been done, what will be done in the next reporting period.

This document constitutes the second of three reports that will be produced throughout the project in order to summarise the dissemination activities carried out.

The current document is articulated in these sections:

- Section 4 Impact. This describes the impact of the project against objectives of ICT-06-2016 “ICT-06-2016: Cloud Computing (Scope: a. Research and Innovation Actions)”. The section explores separately the impact achieved through the work of the research partners and the work of the pilot sites.
- Dissemination activities: a summary of the dissemination activities performed during the first reporting period and the materials that the various consortium members have produced.
- Dissemination plan update including the work the RestAssured project has done to successfully implement a Common Dissemination Booster project.
- An update on the Partners’ exploitation plans.
3  Context and Key Messages

RestAssured is a research project which is developing a reference implementation of 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 is targeted at the scientific and business communities.
4 Impact

This is an extension of the impact plan D9.2. We are now reporting on the impact the project will deliver given the work we have completed on the RestAssured architecture and components.

4.1 Expected Impacts

4.1.1 Impact-01 (I-01)

4.1.1.1 Description

Increased trust in clouds through stronger security and data protection practices, including open and auditable solutions for data security. Increased control by users of their data and trust relations.

4.1.1.2 I-01 Relevance

RestAssured will deliver a secure end-2-end cloud data processing chain, with secure nodes and encrypted data transfer among nodes. In addition, RestAssured will deliver data protection assurance tools and techniques during design time and during runtime in order to detect potential violations and non-conformance to data protection regulation and user-defined privacy policies. The data life-cycle approach of RestAssured will allow users to define and during the whole data life-cycle manage the data policies (decentralized sticky policy management).

4.1.1.3 I-01 Progress in year 1

**UDE Contribution** In accordance with the work plan, UDE has been leading the efforts on the RestAssured high-level architecture. Using several rounds of input from and discussion with the other project partners, the RestAssured high-level architecture has converged to form a common ground for all technical work carried out in the project. The architecture as a conceptual framework is complemented by the RestAssured testbed, which provides a common infrastructure for deploying, integrating, testing, and demonstrating the RestAssured technology. The details of the architecture and the testbed are described in deliverable D3.2.

The other focus of UDE’s work has been on run-time risk management using monitoring, models@runtime, and adaptation. The results achieved so far – which are described in detail in deliverable D5.1 – have been published in several high-quality scientific fora, e.g., the A-ranked CCGrid conference. The impact achieved through publications and presentations at scientific events are detailed in Section 5.1.3 of this deliverable. In accordance with the open access policy of the project and to maximize impact, all publications are available in a green or gold open access model.

**ITInnov Contribution** IT Innovation is responsible for leading WP7, which is creating the models and algorithms for actually computing risk levels. In the first period, we focused on developing our representation of a system or application in terms of assets, adding inputs and outputs that are needed to determine risk levels, and developing software tools for making this determination. The resulting tool now directly supports the calculation of risk levels using a methodology that is compatible with ISO 27005. The methodology and tools are described in Deliverable D7.1, from which content will be used for first publications later this year.

In addition, IT Innovation devised an overall methodology for applying the risk assessment approach within an ecosystem of stakeholders associated with a cloud-based application. The methodology takes into account the challenges posed by the supply chain for software and services, which make it very difficult for service operators to identify and assess risks. The proposed methodology handles this challenge by allowing suppliers to contribute to the risk analysis, in a way that is consistent with their own internal risk analysis,
and verification of system or software security properties using ISO 15408 (Common Criteria). We believe it is essential that the REST Assured methodology should be aligned with standards and support existing software and service business models and ecosystems, so this represents a necessary and significant step towards maximising project impact.

**IBM Contribution** The use of Intel SGX enclaves is extremely complicated, even for experienced programmers. In RestAssured, IBM has developed a Trust Management Framework (or TruCE - “Trust in Cloud Enclaves”) to handle all aspects of remote attestation and the process of secret (key) delivery for Intel SGX enclaves. This framework, with its libraries and SDK, enables application developers to focus their main efforts on creating their application code, giving them the ability to perform attestation by a simple API call. Additional calls are available for easy-to-use enclave sealing and secret passing to enclaves.

TruCE has been made publicly available through IBM’s official github link and as such, is supported by IBM. We also ran performance benchmarks to measure SGX supported encryption libraries. Subsequently, our findings attracted Intel to investigate Intel SGXSSL issues, resulting in a patch which significantly increases the usability of the library. We believe that the release of this code by IBM has the potential to significantly improve the adoption of SGX enclaves by the scientific community.

Additionally, IBM has been collaborating with the Berkeley RISE lab which is developing Opaque, an open source technology which integrates the Apache Spark SQL engine with Intel Software Guard Extension (SGX) hardware, and offers data protection by running SQL transformations inside trusted enclaves. As part of RestAssured, IBM has integrated TruCE with Opaque. This effort too, can have a major impact on scientific community, essentially allowing processing of Big Data with secure enclaves in the cloud.

The Query Gateway provides a standard way for applications to consume secured analytic platform services by wrapping it with REST API. We release this as reference implementation as part of the trust management platform and already see other projects, such as DTAS EU project, adapting this layer as a REST API to SQL Spark.

**Thales Contribution** Thales is responsible for leading WP6, which is about managing the complete data lifecycle security in a decentralized cloud setting. In the first period we focused on the definition of a methodology based on sticky policies for data protection in a decentralized computational environment. The methodology takes into account the General Data Protection Regulation (GDPR), the new regulation for protecting the personal data of European citizens and that will enter in force the 25th May 2018. The data lifecycle security methodology defines how data subjects can express their requirements in terms of protection of their data, how these requirements are formalized in sticky policies based on a semantic approach and on a formalization of the data usage purposes of various cloud services, and how these sticky policies are processed and enforced in a cloud context.

In addition, Thales designed and defined the first architecture of the Data Gatekeeper, the framework for managing the data lifecycle security based on the defined methodology. The framework provides components that specify and manages service provider contracts and sticky policies, reasoning and enforcing them. Thales implemented a first proof of concept of a Data Protection Decision Point that reasons on sticky policies. The methodology and the first architecture of the framework are described in Deliverable D6.1 which was edited by Thales. Thales strongly collaborated with the two use cases providers in this work as well as the WP4 to prepare the integration with SGX.

### 4.1.1.4 I-01 Plan for further progress

**UDE Plan** UDE will continue its work on run-time risk management. While the focus was on risk detection in the first half of the project, it will shift to risk mitigation in the second half. Further scientific publications are planned to continue making an impact.

[https://github.com/IBM/sgx-trust-management](https://github.com/IBM/sgx-trust-management)
Further work is also planned on the RestAssured high-level architecture to make it more versatile and applicable in a wider range of scenarios, thus further boosting the project’s technical impact.

**ITInnov Plan** IT Innovation plans to disseminate the initial prototype machine reasoning model and algorithms that underpin both design time and run-time risk level assessment in RestAssured.

We plan to then extend the models to handle a wider range of security issues in cloud-based systems. Initially our focus will be on threats and mitigation measures for service based applications hosted on IaaS cloud services. Later we may extend the models to cover at least some elements of PaaS clouds depending on the requirements of the project validation case studies.

Our tooling will also be extended to better address the extended (and multi-stakeholder) methodology described in D3.2, facilitating the integration of models from multiple parties, and the generation of documentation to support auditing of security configurations against risk management requirements.

**IBM Plan** IBM will continue to make technical improvements to TruCE, Opaque, and the Query Gateway as well as potentially investigate new enclave technologies which may emerge in the marketplace.

It is expected that as the use cases mature and expand to take full advantage of the capabilities of RestAssured enclaves, the use case owners will generate new requirements to be supported by the IBM infrastructure code.

**Thales Plan** Thales will continue to work on the data lifecycle security methodology and the Data Gatekeeper. A special focus will be put on the maturity of the Gatekeeper, the collection of context information and the reasoning about it to enforce the security of the data. The integration of the data lifecycle security management with restAssured enclaves and the adaptation and risk analysis environment will be one of the Thales priorities of the second period.

4.1.2 Impact-02 (I-02)

4.1.2.1 Description

Increased readiness for adoption of trustworthy cloud-based solutions for SMEs and public sector organisations, spanning from generic enabling services to specific applications.

4.1.2.2 I-02 Relevance

Even though this impact mainly relates to ICT-06-b, RestAssured will contribute to the expected impact through its “Social Care” use case, which involves public sector organizations as end-users thereby contributing to their readiness for adopting secure cloud solutions.

The CARE (Self-directed Social Care) use case shows the extreme end sensitivity for what concerns data protection as it involves citizen data and social care information. This sector thus has always been rather reluctant to adopt cloud technology. RestAssured will demonstrate the secure end-2-end data processing thereby facilitating trust in the use of cloud services, offering significant IT cost savings to health care providers.

4.1.2.3 I-02 Progress in year 1

**OCC Contribution** The social care software is a web-based application that matches volunteers with people requiring help (clients). Both the volunteers and the clients (on their behalf by third party volunteer organisations) provide personal data (i.e. are data subjects). The application matches the volunteer with clients based on their search criteria (location, interests etc.). When a volunteer finds someone that they would like to help, the application will advise them which voluntary organisation that client is registered with and invite them to sign up with the same organisation, which will then contact the volunteer to arrange
This use case will additionally demonstrate how the RestAssured system is able to detect real-time infrastructural events which will adversely affect the security, or functioning of the running system. Upon detecting such an event, RestAssured will be able to autonomously reconfigure itself to mitigate the event, guaranteeing that the new system configuration conforms to acceptable risk levels.

In particular, the use case will synthetically inject a fault, simulating a loss of communication with the running application SGX enclave on the cloud. The Adaptation and Risk components, working in conjunction, will trigger a reconfiguration to resort to running the application in an emulated SGX enclave, hosted in a trusted environment, such as an in-house machine, which typically would also offer a smaller compute cluster. In both configurations, the same application data, residing encrypted on the cloud, is used, allowing for essentially uninterrupted, secure service.

Specifically, the social care example we have built:

1. demonstrates, using the SGX environment, that the stored data cannot be accessed from the outside
2. adds a new client to the system. The example:
   i. updates the Sticky Policy Manager and
   ii. update the Data Gateway to register the new user in the system.
3. re-executes the query to show that the number of clients has increased
4. simulates an adaptation event (e.g. the cloud provider migrates a component from one data centre to another which may require re-active cryptographic protection) and subsequent migration to another SGX cluster
5. shows that we can still securely query that data following the adaptation.

To make these real for the use case, we have demonstrated that this covers:

- the process of matching clients and volunteers
- anonymous, 3rd party, report generation works.

The demonstrator thus shows that the RestAssured components work successfully on personal data stored in the cloud and the data stored or generated at user devices such as mobile phones or desktop computers.

Measurable outcomes: Social Care Pilot implemented using RestAssured technologies.

Success criteria: Demonstrator satisfactorily addresses specific technical concerns about data protection in the cloud. This includes our ability to:

i. detect and predict runtime data protection violations
ii. guarantee geo-location restrictions on personal data
iii. enforce data protection in a dynamic, multi-stakeholder and decentralized federated cloud systems.

4.1.2.4 I-02 Plan for further progress

OCC Plan

We are keen to produce measurable results and will base our impact studies on real requirements local authorities place on our application software. In particular, we will illustrate how we responded to these requirements pre-RestAssured and how we can respond to these requirements with RestAssured technologies.

The impact is that not only does RestAssured help us to ensure data security but it also helps us to convince clients that we have solutions to potential security issues. Below are the expected impacts we have identified during the first year of the project. These will be validated during the 2nd period.

---

4In our technical work we refer to the social care application as the SCANT (Social Care Adaptation) tool, rather than Ami, which is our live product. SCANT is an adaptation of Ami that we have modified for the RestAssured research work.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Pre-RestAssured</th>
<th>With RestAssured</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Information Commissioners Office states that data should only be hosted and processed within the EEA or a country considered safe by the ICO. The supplier should confirm that data will be hosted and processed within the EEA. Please provide details of data centre locations and the service management location.</td>
<td>The location of the data centres is detailed in section 3.2 of the OCC Hosting Policy. Depending upon the solution chosen by the Council then it will be either UK only or EEC only.</td>
<td>The data is encrypted, at rest and when being processed. The location of the data is thus less important, as it is not accessible by the controllers of the storage hardware. The sensitive portions of the RestAssured system (i.e. Data Gatekeeper) are hosted in the EU.</td>
</tr>
<tr>
<td>Please detail how the solution will be hosted (e.g. Public Cloud, Private Cloud) and whether it will be delivered as SAAS, PAAS or IAAS. Include in the response responsibility for the following (e.g. tenant, hosting provider, supplier).</td>
<td>We can confirm that we only provide hosting in EU/EEC data centers with a preference to UK only data hosting. Currently we host in UK: OCC, Saas-MT, Saas-PD, Saas-PI, Iaas-RS, Iaas-OCC, Iaas-PVT and DH all in the UK exclusively.</td>
<td>The sensitive data will be hosted in the public cloud using the Opaque SGX enabled encrypted database. This system prevents the cloud provider from accessing the sensitive data.</td>
</tr>
<tr>
<td>The solution shall have robust mechanisms for protection against attacks affecting system integrity, availability and confidentiality.</td>
<td>The OCC approach to penetration testing of its solutions is detailed in OCCs Hosting Policy.</td>
<td>No change. However, we will run penetration tests on the RestAssured adaption to compare the results.</td>
</tr>
<tr>
<td>Robust controls or counter measures should be provided by the system to ensure the confidentiality, integrity and availability of system data.</td>
<td>We ensure confidentiality through the use of a firewall, IPS and https protocol controls which are detailed in section 2.8 and 3.1 of the OCC Hosting Policy. We ensure the systems integrity by use of regular backups as detailed in section 3.6 of the OCC Hosting Policy. Redundant hardware provides system availability with backups stored in an alternative data centre. There has been no previous data loss.</td>
<td>No change.</td>
</tr>
<tr>
<td>The solution shall provide end to end encryption which includes data transmitted between client and services i.e. server and back-end platforms (including any login credentials).</td>
<td>All connections are through using SSL encryption via https on port 443</td>
<td>No change.</td>
</tr>
<tr>
<td>Question</td>
<td>Response</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Are routine electronic transfers of data containing sensitive data done through secure methods, and is the data encrypted before transfer?</td>
<td>Data uploaded to MarketPlace is using SSL encryption via https on port 443. The connection is restricted between a specific Council specified IP address and the MarketPlace server.</td>
<td>No change.</td>
</tr>
<tr>
<td>Are encryption methods that meet Advanced Encryption Standards (AES) always used to move sensitive data?</td>
<td>The Council has control over how it enters information that is deemed to be sensitive only through the administration screens.</td>
<td>The information is protected by the AES encryption integrated into the Opaque data store. This encryption affects data being processed in memory as well as data on disk.</td>
</tr>
<tr>
<td>Organisational policies, industry or government regulations and compliance, may require the use of encryption “at rest” to protect corporate data. Please describe if your solution has the option for encrypting “data at rest” as part of the proposed solution and what protective marking level the solution is accredited too.</td>
<td>MarketPlace stores data in a Microsoft SQL Server database which can be configured to use transparent data encryption. There are implications on performance and additional development and configuration may be required if the Council were to request this being enabled. MarketPlace should be considered to have the OFFICIAL protective marking level. The system has ASA Firewalls with IPS and racked in a Tier 3 DC this is sufficient for RESTRICTED. In addition the MarketPlace can be configured for two-factor authentication which would be required for RESTRICTED.</td>
<td>RestAssured stores data in the Opaque database. Opaque is a package for Apache Spark SQL that enables strong security for DataFrames using Intel SGX trusted hardware. The aim is to enable analytics on sensitive data in an untrusted cloud. Opaque allows encrypting the contents of a DataFrame. Subsequent operations in them will run within SGX enclaves.</td>
</tr>
</tbody>
</table>

Table 4.1: Expected impacts of a RestAssured approach to Social Care
4.1.3 Impact-03 (I-03)

4.1.3.1 Description
Demonstration, through appropriate use cases, of the potential to improve the competitive position of the European cloud sector and to facilitate the emergence of innovative business.

4.1.3.2 I-03 Relevance
RestAssured has brought together industry partners of relevant and growing sectors for cloud usage, thereby covering a wide range of possible application situations for RestAssured technology.

The PAYD (Pay-as-you-Drive / Usage-based Insurance) use case is positioned at the intersection of cloud computing and cyber physical systems, and thus shows an important combination and interaction among these two system paradigms. In particular, the unique data protection characteristics of the use case (outlaid in Table 4.2 below) present not only technological challenges, but real market barriers and user acceptance challenges for the technology in shifting from commercial (approximately 12% of the auto insurance market) to the much bigger personal auto insurance market (88% market share), further impacted by the changing regulatory environment and uncertainty with the GDPR coming into force.

### Data Protection Concern
- Privacy (personally identifiable information)
- Unintended or otherwise unauthorized use of data

### Cloud Architecture
- Fog/Edge (IoT devices, sensors, embedded controllers and storage, Edge devices, and Cloud)

### Stakeholders
- Citizens
- Car manufacturers
- Telematics providers
- Insurance providers

<table>
<thead>
<tr>
<th>Data Protection Concern</th>
<th>Cloud Architecture</th>
<th>Stakeholders</th>
</tr>
</thead>
</table>
| Privacy (personally identifiable information)| Fog/Edge (IoT devices, sensors, embedded controllers and storage, Edge devices, and Cloud) | Citizens
| Unintended or otherwise unauthorized use of data |                                          | Car manufacturers
|                                              |                                          | Telematics providers
|                                              |                                          | Insurance providers

Table 4.2: Unique data protection characteristics of the PAYD use case

4.1.3.3 I-03 Progress in year 1

Adaptant Contribution

The PAYD software system securely delivers telemetric data from connected cars to an insurance provider (in this case, the primary service provider with which a formal relationship exists), for the primary purpose of enabling the insurer to provide data-adjusted risk premiums (consented to by the data subject), whilst further enforcing the unique privacy expectations of the driver across the entire data life-cycle. The PAYD system utilises the RestAssured sticky policy API to codify and communicate driver privacy preferences and driver consent for data use and processing. Specifically, the PAYD system:

- Demonstrates, using the SGX environment, that the stored data cannot be accessed from the outside.
- Demonstrates driver data visibility to the analytics system based on privacy and consent settings. The example:
  - Updates the Sticky Policy Manager to reflect driver privacy settings to allow geo-location and instrumentation data to be used for a consented purpose;
  - Performs analytic search demonstrating inclusion of driver data in results;
  - Updates the Sticky Policy Manager to reflect driver privacy settings to disallow geo-location and instrumentation data to be used for a consented purpose;
  - Performs analytic search demonstrating exclusion of driver data in results.

[https://courses.cit.cornell.edu/j12545/4550/submitted%20presentations/insurance.pdf](https://courses.cit.cornell.edu/j12545/4550/submitted%20presentations/insurance.pdf)
iii simulates an adaptation event (e.g. the cloud provider migrates a component from one data centre to another which may require re-active cryptographic protection) and subsequent migration to another SGX cluster

iv shows that we can still securely query that data following the adaptation

To make these real for the use case, we have demonstrated that this covers the process of matching data analytics availability and driver purposeful consent settings via the RestAssured sticky policy API. User consent for the allowed purposes of data processing are collected through a user-facing front-end (supported by the work carried out by Adaptant in WP6) that in turn generates a standards-based consent receipt, which is validated before any data is moved or accessed (the dynamic creation of sticky policies from standards-based consent receipts inclusive of user-specified purposes remains an area for future work in WP6).

The demonstrator thus shows that the RestAssured components are able to adapt and limit the use of geolocation and instrumentation data to specific purposes consented to by the driver, while accounting for variance in individual privacy settings.

<table>
<thead>
<tr>
<th>Measurable Outcome</th>
<th>Success Criteria</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• GDPR-enabling PAYD demonstrator implemented using RestAssured technologies</td>
<td>• Demonstrator satisfactorily addresses specific technical concerns about data protection in the cloud</td>
<td>i guarantee consent-based data ingest restrictions on geo-locational and car instrumentation data stream;</td>
</tr>
<tr>
<td></td>
<td>• Demonstrator satisfactorily obtains driver consent and address specific privacy concerns</td>
<td>ii guarantee analytic usage restrictions on cloud stored geo-locational and car instrumentation data;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iii enforce data protection in dynamic, multi-stakeholder and decentralized federated cloud systems (including at the network edge).</td>
</tr>
</tbody>
</table>

Table 4.3: Success metrics for the initial PAYD Demonstrator

4.1.3.4 I-03 Plan for further progress

Adaptant Plan

We are keen to produce measurable results that work to address the challenges identified in Table 4.2, allowing us to demonstrate that a GDPR-compliant PAYD solution for the personal automotive insurance market is possible. In particular, we will contrast the pre-RestAssured state of Usage-based insurance in the commercial sector pre- and post- the application of RestAssured technologies. A direct comparison of the personal automotive insurance market is currently not in scope - the current restrictions have prevented EU-based insurance companies from rolling out these schemes outside of the context of commercial fleet management. The RestAssured results, therefore, together with the coming into force of the GDPR, have a strong opportunity to contribute to the opening up of a validated but otherwise unexploited market within the EU.

Further commercial enablement facilitated by the PAYD demonstrator is further elaborated in Section 6.5.1.2.
Below are the expected impacts we have identified during the first year of the project. These will be validated during the 2nd period.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Pre-RestAssured</th>
<th>With RestAssured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of sensitive data at rest.</td>
<td>Existing pay-as-you-drive insurance services do not provide data storage protection.</td>
<td>RestAssured offers data storage encryption utilising the Opaque package and SGX on top of Spark.</td>
</tr>
<tr>
<td>Protection of sensitive data in transit.</td>
<td>Existing pay-as-you-drive insurance services do not provide complete end-to-end data transmission protection.</td>
<td>Data transmission for ingest shall use TLS and SGX.</td>
</tr>
<tr>
<td>Protection of the processing of sensitive data.</td>
<td>Existing pay-as-you-drive insurance services do not provide complete end-to-end data transmission protection.</td>
<td>Data processing for ingest and analytics are secured by the RestAssured Data Enforcement Point for sticky policy enforcement (protected by TLS for data in transmission and protected by SGX attestation for data processing).</td>
</tr>
<tr>
<td>Fine grained consent based data access control for analytics.</td>
<td>Existing pay-as-you-drive insurance services do not provide analytics access control based on individual consent preferences.</td>
<td>Through the use of RestAssured sticky policies, all data analytics (via SQL through the Query Gateway) will be controlled by the Data Enforcement Point, dynamically granting analytic data access only from individuals who have currently given consent to the purposeful data usage.</td>
</tr>
<tr>
<td>Personal Data must be Collected for specified, explicit and legitimate purposes and be Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</td>
<td>Existing pay-as-you-drive insurance services do not provide consent and processing audit logs.</td>
<td>RestAssured sticky policies together with logging mechanisms will provide necessary data transmission, storage and processing audit trails required to demonstrate regulatory compliance.</td>
</tr>
</tbody>
</table>

Table 4.4: Expected impacts of a RestAssured approach to PAYD
5 Dissemination

5.1 Communication Activities and Tools

5.1.1 Project Website

The project website (restassuredh2020.eu) was initially created and launched at M3 and has since undergone a number of structural and performance related improvements. These can be summarised as follows:

- Blog section created for sharing project updates and associated content
- Publications section added to list published papers
- Search engine and performance optimisations to improve the overall efficiency of the website
- Dynamic content added to the home page (Recent blog posts and the project Twitter feed)

The project blog is regularly updated with details of conferences, publications and research that the consortium partners have been involved in where related to the RestAssured project.

The current website, with the aforementioned improvements is shown in Figures 5.1, 5.2 and 5.3 below:
RestAssured will deliver end-to-end cloud architectures and methodologies for ensuring secure data processing in the cloud, thereby empowering cloud providers and application developers to offer secure cloud services at competitive cost.

What is RestAssured?

Recent Posts

- Presentation at the Hostelling 2019 Conference (20th February 2019)
- Implementation of the First Version of the Data Gateway (29th February 2019)
- RestAssured Project Collaboration with UC Denver (15th Jan 2019)
- Impressions of IoTWIS performance test driven by ultra-slow speed measurements (2nd Jan 2019)
- Test Driving Intel X6 with Intel 60k on Encrypted Data (15th Nov 2017)

Publications


Our Partners

Subscribe to our newsletter

Enter your email address to be kept up-to-date.

This project received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 735075 (RestAssured).

Figure 5.1: Project website Home page
Publications


This publication addresses the question of how secure hardware enclaves as part of cloud servers may increase the optimization possibilities of cloud providers. New algorithms are proposed to take advantage of such capabilities with the aim of ensuring data protection and minimizing costs simultaneously. Experimental results suggest that even a small percentage of secure hardware enclaves may lead to significant cost savings.


This publication describes a new method and new algorithms for adaptively scaling and placing virtualized network functions (e.g., firewall, deep packet inspection, anti-virus, parental control) and their data flows in the cloud.


This paper suggests an algorithm portfolio approach in which multiple algorithms for dynamic optimization of resource allocation in virtualized data centers coexist. Based on continual monitoring and analysis of the state of the data center, the optimization algorithm that is most suitable is chosen on the fly. Thereby, the balance between optimization quality and reaction time can be tuned adaptively. Empirical results show that this approach leads to improved overall results.

Mann, Zoltan (UDC), Salent, Eliot (IBM), Surridge, Mike (IT Innovation), Ayed, Dhioua (Thales), Boyle, John (GCC), Heisel, Maritta (UDC), Hetager, Andreas (UDE), Hundt, Paul (Adaptaid), **Secure Data Processing in the Cloud.** ESOCC EU Workshop, 27 September 2017, Oslo.

---

This project received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 731679 (RestAssured).

---

**Figure 5.2: Project website Publications page**
Latest News

Presentation at the Modellierung 2018 Conference
By RestAssured / 7th February 2018
Categories: Events, Research

“Towards a real-time market for data protection in the cloud” – this was the title of the presentation given by Dr. Dieter Mann from Palantir (The Hive) Institute for Software Technology) at the University of Darmstadt. During the Modellierung 2018 conference (https://modellierung2018.wordpress.com/) in Darmstadt. The presentation has been organized by the German Information Society (Distributed).

Implementation of the First Version of the Data Gatekeeper
By RestAssured / 8th February 2018
Categories: Research

The Data Life Cycle is the sequence of stages that a unit of data goes through from its creation to its deletion. The Data Life Cycle specifies 6 operations on data, namely Create, Read, Update and Delete. The Data Life Cycle management is a crucial requirement for businesses that handle personal data. When these businesses...[ ]

RestAssured Project Collaboration with UC Berkeley RISELab
By RestAssured / 3rd January 2018
Categories: Events, Research

The RestAssured platform aims to create a secure environment for processing highly sensitive data, with strict consent based rules governing access to personal data, and with proactive risk analysis and adaptation. As part of RISElab’s work on RestAssured, we have identified the Apache open source technology, being developed by the UC Berkeley RISELab team...[ ]

Impressions of Intel® SGX performance
By RestAssured / 7th January 2018
Categories: Research

Intel® SGX enclaves provide hardware enforced confidentiality and integrity guarantees for running computations. This is achieved mainly by encrypting all information as it leaves the CPU, effectively shielding data in the memory from external observers. But what is the overhead of running computations inside an enclave? One would expect some overhead due to Intel...[ ]

Test Driving Spark SQL with Intel SGX on Encrypted Data
By RestAssured / 1st November 2017
Categories: Research

Protecting sensitive business and personal information is a cornerstone requirement when enterprises move to the cloud. Many aspects of this requirement are already handled at various levels. Data at rest can be secured in cloud storage by encrypting it before storage, while data in flight is transmitted over protected channels such as TLS and HTTPS. Data in-use, processed in cloud...[ ]

Figure 5.3: Project website Blog page
5.1.1.1 Website KPIs and Analytics

Google Analytics is used to monitor and record visitor statistics for the project website. The results against the KPIs set in D9.2 are shown below in Table 5.1.

<table>
<thead>
<tr>
<th>KPI</th>
<th>Objective</th>
<th>Result (22nd March 2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website creation</td>
<td>Available publicly</td>
<td>Website went live March 2017</td>
</tr>
<tr>
<td>Quarterly traffic</td>
<td>Uniform growth</td>
<td>54% increase from first to most recent quarter</td>
</tr>
</tbody>
</table>

Table 5.1: Website objectives

The statistics are broken down by quarter in Table 5.2 and the monthly trend can be seen in Figure 5.4. Note that website visitor statistics were recorded since June 2017, when Google Analytics was integrated with the site and only full quarterly results are listed, aligning to the calendar year.

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Users</th>
<th>Sessions</th>
<th>Page Views</th>
<th>Average Duration (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul-Sept 2017</td>
<td>106</td>
<td>157</td>
<td>314</td>
<td>1:33</td>
</tr>
<tr>
<td>Oct-Dec 2017</td>
<td>170</td>
<td>280</td>
<td>924</td>
<td>4:21</td>
</tr>
<tr>
<td>Jan-Mar 2018</td>
<td>195</td>
<td>284</td>
<td>925</td>
<td>2:59</td>
</tr>
</tbody>
</table>

Table 5.2: Project website quarterly visitor statistics

Figure 5.4: Monthly users since website launch
5.1.2 Social Media

5.1.2.1 Twitter KPIs

The project Twitter account (@RestAssuredH20) is mainly operated by OCC used to share updates related to the website blog, publications and events. The status of the objective set out in D9.2 is shown in Table 5.3. Statistics for the previous 28 day period are displayed in Figure 5.6.

<table>
<thead>
<tr>
<th>KPI</th>
<th>Objective</th>
<th>Result (22\textsuperscript{nd} March 2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of followers</td>
<td>100 followers by M12 (across all platforms)</td>
<td>26</td>
</tr>
</tbody>
</table>

Table 5.3: Twitter objectives

The following Twitter analytics show a summary of statistics for each month that the account has been active:
Figure 5.7: Twitter statistics January 2018

Figure 5.8: Twitter statistics December 2017
Figure 5.9: Twitter statistics November 2017

Figure 5.10: Twitter statistics October 2017
Figure 5.11: Twitter statistics September 2017

5.1.3 Academic and Research Presentations

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Name and type of audience</th>
<th>Countries addressed</th>
<th>Size of audience</th>
<th>People attending (organisation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE/ACM CCGrid 2017</td>
<td>14.05.17-17.05.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 200</td>
<td>Zoltan Mann (UDE)</td>
</tr>
<tr>
<td>ESOCC 2017</td>
<td>27.09.17-29.09.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 60</td>
<td>Zoltan Mann (UDE)</td>
</tr>
<tr>
<td>ESOCC 2017 – EU Projects Workshop</td>
<td>27.09.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 60</td>
<td>Mike Surridge (ITInnov)</td>
</tr>
<tr>
<td>NetFutures 2017 (Concertation)</td>
<td>28.06.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 100</td>
<td>Paul Mundt (Adaptant)</td>
</tr>
<tr>
<td>DPSP Cluster 2017</td>
<td>19.09.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 50</td>
<td>Adam Burns (Adaptant)</td>
</tr>
<tr>
<td>WESOACS 2017</td>
<td>13.11.17</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 20</td>
<td>Stefan Schoenen (UDE)</td>
</tr>
<tr>
<td>Modellierung 2018</td>
<td>21.02.18-23.02.18</td>
<td>Academic and Industry</td>
<td>Germany</td>
<td>approx. 50</td>
<td>Zoltan Mann (UDE)</td>
</tr>
</tbody>
</table>
5.1.3.1 Representation and Accession to the DPSP Cluster by Adaptant

RestAssured was represented by Adaptant at the NetFutures Concertation meeting in Brussels, which provided an opportunity for networking with other like-minded projects in order to explore synergies. As a result of this, we were invited to an initial meeting of the DPSP (Data Protection, Security and Privacy in cloud) cluster\(^1\) in order to further present the project to the rest of the cluster members (elaborated in Table 5.5 below). This presentation was well received, and was followed up with RestAssured being formally invited to join the cluster initiative. The accession to the DPSP cluster was subsequently concluded\(^2\), and we had our first in-depth presentation of the RestAssured project to the rest of the cluster members at the subsequent cluster meeting in Amsterdam.

### Table 5.4: Detailed list of events attended

<table>
<thead>
<tr>
<th>Event</th>
<th>Dates</th>
<th>Type</th>
<th>Location</th>
<th>Attendees</th>
<th>Contact Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>GI SE 2018</td>
<td>07.03.18-09.03.18</td>
<td>Academic and Industry</td>
<td>Germany</td>
<td>approx. 100</td>
<td>Zoltan Mann (UDE)</td>
</tr>
<tr>
<td>KuVS FFG 2018</td>
<td>08.03.18-09.03.18</td>
<td>Academic and Industry</td>
<td>Germany</td>
<td>approx. 20</td>
<td>Zoltan Mann (UDE)</td>
</tr>
<tr>
<td>SEAMS 2018</td>
<td>28.05.18-29.05.29</td>
<td>Academic and Industry</td>
<td>International</td>
<td>approx. 50</td>
<td>Zoltan Mann (UDE)</td>
</tr>
</tbody>
</table>

5.1.4 Academic Publications

Table 5.5 lists the papers accepted for publication and table 5.7 contains the publications aimed at the general public.

### Table 5.5: Projects participating in the DPSP cluster

<table>
<thead>
<tr>
<th>APPHUB</th>
<th>CLIPS</th>
<th>COCO CLOUD</th>
<th>ESCUDO-CLOUD</th>
<th>OPERANDO</th>
<th>RESTASSURED</th>
<th>SERECA</th>
<th>SPECS</th>
<th>SWITCH</th>
<th>UNICORN</th>
<th>A4CLOUD</th>
<th>CLOUDWATCH</th>
<th>CREDENTIAL</th>
<th>EUBRASILCLOUDFORUM</th>
<th>PAASWORD</th>
<th>SECCORD</th>
<th>SLALOM</th>
<th>STRATEGIC</th>
<th>TREDISEC</th>
<th>WITDOM</th>
<th>CLARUS</th>
<th>CLOUDWATCH2</th>
<th>DITAS</th>
<th>MUSA</th>
<th>PRISMA CLOUD</th>
<th>SECURE CLOUD</th>
<th>SLA-READY</th>
<th>SUNFISH</th>
<th>TRESCCA</th>
</tr>
</thead>
</table>

Some of these projects (such as OPERANDO) have notably already been selected for closer joint-collaboration through the Common Dissemination Booster (elaborated in Section 5.2 below).
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors (organisation)</th>
<th>Publisher</th>
<th>Place of publication</th>
<th>Year of publication</th>
<th>Open access</th>
<th>Conference / Journal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two are better than one: An algorithm portfolio approach to cloud resource management</td>
<td>Zoltan Mann (UDE)</td>
<td>Springer</td>
<td>Cham, Switzerland</td>
<td>2017</td>
<td>green</td>
<td>6th European Conference on Service-Oriented and Cloud Computing</td>
</tr>
<tr>
<td>Secure Data Processing in the Cloud</td>
<td>Mike Surridge (IT Innov), Zoltan Mann (UDE), Eliot Salant (IBM), Dhouha Ayed (Thales), John Boyle (OCC), Maritta Heisel (UDE), Andreas Metzger (UDE), Paul Mundt (Adaptant)</td>
<td>Springer</td>
<td></td>
<td>2018</td>
<td>green</td>
<td>6th European Conference on Service-Oriented and Cloud Computing</td>
</tr>
<tr>
<td>Using risk patterns to identify violations of data protection policies in cloud systems</td>
<td>Stefan Schoenen, Zoltan Mann, Andreas Metzger (UDE)</td>
<td></td>
<td></td>
<td></td>
<td>green</td>
<td>13th International Workshop on Engineering Service-Oriented Applications and Cloud Services</td>
</tr>
<tr>
<td>Towards a run-time model for data protection in the cloud</td>
<td>Zoltan Mann, Andreas Metzger, Stefan Schoenen (UDE)</td>
<td>Gesellschaft für Informatik</td>
<td>Bonn, Germany</td>
<td>2018</td>
<td>gold</td>
<td>Modellierung 2018</td>
</tr>
<tr>
<td>Resource optimization across the cloud stack</td>
<td>Zoltan Mann (UDE)</td>
<td>IEEE</td>
<td></td>
<td>2018</td>
<td>green</td>
<td>IEEE Transactions on Parallel and Distributed Systems</td>
</tr>
<tr>
<td>The special case of data protection and self-adaptation</td>
<td>Zoltan Mann, Andreas Metzger (UDE)</td>
<td></td>
<td></td>
<td>2018</td>
<td></td>
<td>IEEE/ACM 13th International Symposium on Software Engineering for Adaptive and Self-Managing Systems</td>
</tr>
<tr>
<td>Cloud simulators in the implementation and evaluation of virtual machine placement algorithms</td>
<td>Zoltan Mann (UDE)</td>
<td>Wiley</td>
<td></td>
<td></td>
<td></td>
<td>Software: Practice and Experience</td>
</tr>
</tbody>
</table>

Table 5.6: Detailed list of accepted publications
Table 5.7: Detailed list of publications for the general public

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors (organisation)</th>
<th>Event and publication (name, date, other info.)</th>
<th>Conference / Journal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ganz privat? (in German) [Fully private?]</td>
<td>Zoltan Mann, Andreas Metzger, Klaus Pohl (UDE)</td>
<td>UNIKATE</td>
<td>Magazine</td>
</tr>
<tr>
<td>Risiko in der Wolke? in German) [Risks in the cloud?]</td>
<td>Maritta Heisel, Denis Hatebur, Ludger Goeke, Isabelle Coté (UDE)</td>
<td>UNIKATE</td>
<td>Magazine</td>
</tr>
</tbody>
</table>

5.2 Common Dissemination Booster (CDB)

5.2.1 CDB Summary

The RestAssured project has coordinated and organised a cluster of projects to complete the Common Dissemination Booster service provided by Trust-IT. The cluster will complete the first service, Portfolio Identification. The CDB will help the cluster to define a compelling portfolio of results across the project group - fully exploiting diversity and leveraging commonalities in the CDB project group to better address a wider set of stakeholders, eager to learn about the results. The service will also identify other related projects in order to expand the project group further.

The current project group includes eight projects:

- RestAssured (lead project)
- OPERANDO
- MELODIC
- ACTiCLOUD
- SHiELD
- DECIDE
- CITADEL
- CloudPerfect

The service involves three stages (see figure 5.12) where the ultimate outcome will be a tailored dissemination portfolio of results for the project group highlighting commonalities and synergies as well as diversity and complementarities. In addition, the project group will share available public dissemination and exploitation plans to further share ideas and results and will attend planned joint events to boost the impact of dissemination activities.

[https://www.uni-due.de/unikate/050/unikate_050.html]
5.2.2 Next Steps

The CDB will allow the RestAssured partners to transfer knowledge and results between the projects. It will achieve this by:

Sharing the results of the projects. Project results of value to other projects in the CDB were identified during Service 1: Portfolio Identification of the CDB. These results will now be shared through a sharing of key deliverables on the CDB platform. For example, OPERANDO has developed a legally compliant privacy framework which the SMEs in RestAssured may be able to adapt. The SHIELD project has produced results on health data security which we may be able to adapt and use for the Social Care use case.

Awareness of dissemination activities. Each of the CDB projects will update (and hopefully maintain) a summary of their dissemination material. This will include details of any service offerings from each of the projects which can be used by other projects. It will also include details of any conferences or events the project partners are attending so that we can organize face-to-face meetings to share expertise and identify future collaboration opportunities. In particular, during our first CDB meeting in March 2018. The group discussed an action to take forward an application for a networking session & information stand at ICT2018 in December.
5.3 Dissemination Plan Task Update

The progress of the main dissemination activities defined in D9.2 is presented in Table 5.8 below:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description of activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Website</td>
<td>The content updates to the project website have been regular and the statistics (see Table 5.2) show visitor numbers increasing, thus the KPIs were reached. This can be attributed to both the structural improvements and also original content in the form of blog posts and publications.</td>
</tr>
<tr>
<td>Twitter</td>
<td>Although progress has been made towards the objective, the results in Table 5.3 show that the KPI was not met in this activity. Further work to engage with the target audience will be needed as the project moves forward.</td>
</tr>
<tr>
<td>Publications</td>
<td>In the first 16 months of the project there have been 5 papers, of which 4 have been published. The activity was achieved by the academic partners (UDE and ITInnov).</td>
</tr>
<tr>
<td>Events</td>
<td>The consortium attended 4 events during the first year of the project. The RestAssured approach and concepts were presented at international conferences, workshops and collaboration meetings.</td>
</tr>
</tbody>
</table>

Table 5.8: Dissemination task progress

The deviations from D9.2 are explained in Table 5.9:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description of deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>The decision was made to focus dissemination efforts through Twitter as the preferred social media platform. However, as the project matures, Facebook may be considered again for sharing content.</td>
</tr>
<tr>
<td>Physical Marketing Assets</td>
<td>The consortium have decided to focus on the Common Dissemination Booster as a vehicle for joining forces with similar projects to raise awareness in the area.</td>
</tr>
<tr>
<td>Newsletter</td>
<td>(As above)</td>
</tr>
<tr>
<td>GitHub forum</td>
<td>This activity has been put on hold until the project has developed suitable assets in GitHub.</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>This activity is aimed at the commercial community and therefore has been placed on hold until the software development work has reached sufficient maturity.</td>
</tr>
</tbody>
</table>

Table 5.9: Dissemination task deviations
6 Exploitation

6.1 IBM Contribution

IBM’s exploitation plans are very closely aligned with its achievements described in the Impact section 4.1.1.3. More specifically, through the release and support of TruCe in IBM’s Github, IBM is making this code freely available for the scientific community to increase the security of their cloud-based solutions. Additionally, IBM’s work with the Berkeley RISE Labs to improve Opaque, their Open Source, Spark-based SQL implementation will also allow the scientific community to benefit from its results in RestAssured.

6.2 UDE Contribution

As research and education institution, UDE is exploiting and will continue to exploit the results and other impetus from RestAssured to improve and extend its research and education activities.

Research UDE has combined its existing expertise in software engineering, self-adaptive systems, and cloud computing with new ideas from the project regarding data protection requirements of the use cases and innovative technologies for data protection assurance. This cross-fertilization has resulted in interesting new research questions and approaches relating to run-time modeling of cloud systems, detection of data protection violations at run-time, and optimization of cloud deployments taking into account the availability of secure hardware enclaves. The research results published so far are shown in Section 5.1.3 of this deliverable.

Education UDE has launched some educational activities relating to the RestAssured project context. In particular, two Masters’ project groups were run on the topic of data protection in the cloud using adaptation. This way, 10 graduate students could be trained in this topic using lectures, seminars, and hands-on programming assignments. One seminar group of three students were working on the topic of the specification frameworks for addressing end-users data protection requirements. Furthermore, several related Bachelors’ and Masters’ thesis topics have been defined. The first Masters’ thesis specifically on data protection in the cloud will be finished in April 2018.

6.3 Thales Exploitation

Thales is a leading security solution provider for mission-critical information systems, defense and security, aerospace and transportation sectors. It has earned particular recognition for its ability to develop and deploy dual civil and military technologies. The ThereSIS lab which is involved in RestAssured has strong expertise in Cloud Computing and Security. For example, through its participation in the Reservoir project, ThereSIS developed Cloud and Cloud Security solutions that are now part of the Thales group portfolio. THALES aims to leverage the innovations brought by RestAssured to enhance its existing Cloud Security solution. THALES is deeply involved in the field of privacy preserving mechanisms as well as in cloud computing, which has been recently strengthened with the acquisition of Vormetric, a Thales company. THALES also has a strong position in the cryptographic area through its joint lab with the French Department of Defense. THALES is positioned as an Infrastructure As a Service provider with its offer “CloudOMC”. Thales also recently acquired the company Gemalto to increase our expertise in the field of cryptography and IoT.

Product line manager & Sales department have been made aware of the work done in the RestAssured project and are investigating new milestones for their product roadmap.
In accordance with Thales Group governance principles, defining Thales Research and Technology (R&T) strategy and governance to develop technological synergies across the Group, the Technical Directorate through Key Technical Domains (KTD) governs the conduct of R&T in the Group. This includes policies to promote innovation outcomes exploitation. Thales Group R&T is characterised and managed in 4 domains, called Key Technical Domains (KTD): Hardware (KTD HW), Software (KTD SCIS), Processing (KTD PCC), Systems (KTD SYS). The Group R&T governance comprises definition of R&T strategies for each of the KTDs, and the cascade of these strategies to the entities undertaking R&T activities. With the objective to improve both the solution attractiveness and offer competitiveness, these R&T strategies aim at developing technological assets, and validated technological building blocks, to be inserted into Thales offers. The RestAssured outcomes are identified as key technology enablers by the KTD SCIS Software and Critical Information Systems.

Thales develops and acquires technologies to support the achievement of market outcomes. Consequently, not all technologies will be subject to the entire R&T process. In addition to internal development from TRL (Technological Readiness Level) 1-3 (Research Phase) technologies may be developed externally by third parties or under collaborative arrangements. These technologies may be candidates for Risk Reduction (TRL 4-5) activity and would therefore enter the process through the Initial Gate Approval.

The Initial Gate approval marks a decision to progress development of a technology beyond TRL 3. If such approval is achieved, the technology will be further developed to TRL 5 and an assessment made as to whether it will then be included as an element of product roadmaps or other Thales offers.

The development to TRL 5 is referred to as the Risk Reduction Phase. To achieve Initial Gate approval the KTD Board must first be satisfied that the technology has reached TRL 3. Second, the KTD Board must be satisfied that there is market pull for the technology. This is demonstrated through at least one Division identifying this technology as a long-term option in their product roadmaps and policies.

Finally, given that the investment to progress a technology from TRL 4-5 is significantly greater than from TRL 1-3, the KTD Board will take account of the anticipated return on investment when deciding to progress a proposal through the Initial Gate. This decision is supported by a plan for the Risk Reduction Phase, comprising schedule, budget and expected outcomes.

A technology that achieves Initial Gate approval will be inserted as a long-term option in the product roadmap. This approval is therefore referred to as an authorization to roadmap.

Regarding RestAssured outcomes, the main exploitation that it will be done with RestAssured results is the data lifecycle security methodology and the Gatekeeper. Thales needs a full implementation and first tests of an integrated version of the Gatekeeper based on the ontology-based solution to reach a TRL 3 before starting an initial gate approval process. These innovative technologies will not be sold as a standalone product but it will be sold internally as a building block for Thales solutions; the first offer that will integrate them is the CYRIS solution for data protection in the cloud. Our objective is also their integration to Vormetric solutions.

The expertise acquired on SGX environment will also be beneficial to the expanded and new market implied by the purchase of Gemalto.

6.4 ITInnov Contribution

IT Innovation is part of a UK University, whose success criteria are defined in three areas: high quality research outputs (i.e. publications), teaching excellence, and socio-economic impact. Our group’s remit is to carry out collaborative applied research with (mainly industry) technology suppliers and/or end users. Our primary success measure is therefore to promote socio-economic impact from applied research, with secondary goals to publish (at about one conference or journal paper per project per year), and contribute to teaching.

IT Innovation will 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, commercial licensing to partners, and/or release of Open Source Software supported by professional services, as appropriate.

RestAssured is of particular interest to SMEs. In 2015-16 IT Innovation led 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 showed 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 helping them to fill gaps left by Cyber Essentials, including local SMEs contacted in our previous study through the Solent Cyber Security Cluster, and the Federation of Small Businesses.

At this stage we have not decided whether it will be necessary to form a separate spin-off company, as opposed to working with (and licensing technology to) commercial RESTASSURED partners. For example, the best way to address markets in social care (at least in the UK) would be to team with OCC. However, other SME-rich sectors such as legal services may be addressed more effectively through a spin-off or through a (non-partner) organisation established in the relevant market. Other markets may be best addressed by engaging directly in commercial sales, e.g. through the industrially-funded University of Southampton Cyber Security Academy (CSA).

We can say that the CSA is our preferred channel for achieving impact through education and training, and the most likely channel for commercial exploitation of project results related to education and training. The CSA provides professional development courses for cybersecurity practitioners, as well as courses for non-specialists who need a basic understanding of cybersecurity, such as company Directors for non-IT business functions. We already have a PhD student co-supervised by IT Innovation and the CSA, who started her degree in October 2017, doing research on the cyber security needs of SMEs. We expect to deepen our engagement in teaching by contributing to CSA professional development course units in risk management, and supporting the development of a part-time MSc for cybersecurity practitioners based on the existing full-time MSc in Cybersecurity.

6.5 Adaptant Contribution

Adaptant is a software and services company that develops data ethical and privacy-preserving products, solutions, and services for both the B2C and B2B markets, the core of which is Adaptant’s user-centric data platform.

Adaptant’s exploitation strategy is focused across the following key areas, and aligns closely with the achievements outlined in section 4.1.3.3:

As a company, RestAssured will enable us to:

- Incorporating Secure data analytics and selective disclosure in our data management platform
- Prepare spin-out opportunities for products deriving from each of our use cases
- Create opportunities for, strengthen, and extend our consultancy services
- Create new intellectual property rights that complement our existing products & solutions

Each of these points are further explored below:
6.5.1 Product Development & Spin-Out Opportunities

6.5.1.1 Extending Adaptant's Data Platform with Secure Data Analytics & Selective Disclosure Capabilities

As a data platform designed from the ground up with the GDPR and the concepts of privacy-by-design, informed consent, and informational self-determination in mind, Adaptant’s user-centric data management platform enables users to determine what kind of information they would like to share, with whom, for what purpose, and in what form. The application of project results in the area of secure data processing within SGX Enclaves allow us to enhance our product offering with a unique feature for carrying out secure analytics of data under the user’s control, allowing the result of the query to be transferred to a service provider without exposing any of the underlying sensitive data. Taken together with the Dynamic Data Masking capabilities of the platform, a holistic data protection capability is provided to the user, allowing them to incrementally share more or less data with service providers as trust evolves. In addition to secure processing enclaves, it is also expected that this facility will be further augmented by other promising technologies in the future, such as secure multi-party computation (MPC).

6.5.1.2 InsurTech Spin-Out & Commercialization of PAYD Solution

The demonstrator developed by Adaptant for the PAYD use case has been designed with commercial application in mind, with the amount of effort needed to bridge the gap between technology demonstrator and minimum-viable product (MVP) kept as small as possible in order to enable rapid market entry of the solution (while the demonstrator is scheduled for the interim review of M18, market entry of the derived solution is envisioned by the end of Year 2 of the project). As Adaptant’s core business remains focused on its data platform, the commercial exploitation of the solution developed for the PAYD use case is expected to occur through a spin-out entity, for which an initial business plan has already been created. An extended variant of the demonstrator used for the PAYD use case will further be used for demonstrating the solution to prospective clients, investors, as well as at relevant industry (InsurTech) trade shows.

6.5.2 GDPR Consultancy Services

In addition to the product-facing improvements enabled by the exploitation of RestAssured project results, Adaptant aims to both broaden and strengthen the value propositions of its consultancy services through the continuous transfer of both explicit and tacit knowledge gained from Adaptant’s activities in RestAssured. Since the beginning of the project, Adaptant was able to elaborate and consolidate its GDPR know-how, and launch an initial GDPR Services portfolio focused primarily on start-ups and SMEs. Somewhat unexpectedly, strong interest has been expressed in these services from outside of the EU (primarily Australia and the United States), which may impact the market positioning of the service offerings as the GDPR comes into force.

6.5.3 Intellectual Property Rights

As part of the work carried out in the implementation of the PAYD use case, Adaptant is pursuing a patent that provides a method and apparatus for realizing policy compliance through dynamic data flow management of streaming data. As the first step to protection, the idea has been submitted to an i-DEPOT[1] at the Benelux Office for Intellectual Property, and is in the process of being elaborated into a provisional patent application to be filed with the United States Patent and Trademark Office during Year 2 of the project.

6.6 OCC Contribution

OCC is an IT services company that sells a range of products to Local Authorities and Health Trusts.

As a company, RestAssured will give us a competitive advantage by:

- Allowing us to host solutions less expensively
- Enabling us to answer tender questions better. This is both a matter of meeting minimum pass criteria as well as scoring as well as possible on each evaluated question
- Helping us complete Pen Testing and ISO certification quicker. This also applies to meeting Cyber Essentials requirements
- Reducing the risk that a data breach will occur in one of our products (since this would damage our reputation and could potentially lead to legal action against OCC.
- Creating opportunities for consultancy services

Each of these potential exploitation opportunities is explored below:

6.6.1 Hosting Solution Costs

RestAssured uses SGX hardware and partitioning of cloud services into parts that need secure (and thus more costly) computation vs. other parts. Thereby providing optimal use of resources, while delivering data protection and secure data processing. Thereby, cloud offerings based on RestAssured technology can be offered in a secure and trustworthy way, while keeping resource usage and thus costs at bay.

The commercial impact of this can easily be measured. Our average annual hosting costs for each client application are in the order of 20,000 per annum. We host just over 80 sites. Therefore, even a 10% saving would represent a cost saving of 160,000.

6.6.2 Tender Success

No current services for the management of social care contain the privacy assurance for citizens managing their own social and health services that RestAssured offers. This will become more prominent with the roll-out of the self-service portals and citizens take a more direct role.

In section 4.1.2.4 on ‘Impact’ we have detailed the data security requirements from tenders we receive from potential customers. RestAssured enables us to provide state-of-the-art responses to these requirements which will play a crucial part in winning contracts against UK and international competitors. Given that we are frequently competing against large corporates such as Oracle, having demonstrable technology solutions to risks is important.

6.6.3 Certification, Compliance and Risk Management

As a company, OCC maintains certified ISO 27001 compliance as well as pen testing all products. We are also working towards compliance with Cyber Essentials. Whilst pen testing evaluates the compliance of our software products, ISO 27001 evaluates OCC methodologies for risk and security management.

RestAssured Model-based engineering methodology provides a true risk-based approach to threat identification that aligns with ISO 27001. Compliance with ISO 27001 is an important overhead cost for OCC.

---

2Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.
and the RestAssured methodology provides a more rational, cost-effective use of security to identify, reduce or mitigate risks than the current goal-based approaches.

Using the Model-based engineering methodology developed in RestAssured, we are able to run models for capturing multi-stakeholder cloud systems and their security concerns. By the end of the project, we plan to have an example of these models that we can use and adapt for different customers. This will reduce the possibility of OCC failing to identify and model application risks and will provide valuable evidence that a due process was followed in our project work.

Looking at our certification, compliance and risk management within the context of RestAssured we believe we can derive the following commercial benefits:

**6.6.3.1 Pen Testing:**

IT Innovation’s work on monitoring run-time components using threat modeling software should prove useful for cloud applications using RestAssured technology. During the next phase of the project, we plan to test and validate how the software would identify and flag any known vulnerabilities and the associated impact level for the cloud application. The threat database is similar to what a pen testing service would use (i.e. known vulnerabilities for applications via network based attacks), but the benefit should be continuous monitoring with the possibility to carry out a remedial action if a threat is found (where a remediation is available, e.g. installing a software patch etc.).

If RestAssured technologies show that known risks were scanned for within a cloud application and any threats resolved (by some sort of adaptation), then that will show a relevant impact of the RestAssured project.

We will also give metrics that illustrate that a cloud application/service using RestAssured technology is less susceptible to some local threats through the use of Intel SGX.

**6.6.3.2 ISO Certification:**

One of the capabilities of RestAssured technologies is to adhere to GDPR and other local legislation for the whole data life-cycle, and update accordingly if the data moves to a different geographical location.

This will form part of our ISO27001 policies and we will be able to evidence our compliance via the evaluation for the RestAssured pilots.

Note: Until we are actually using RestAssured in our cloud services we cannot include this in our published ISO27001 policies since ISO deals with what is actually in place.

In the contract of ISO27001, it is important to note that our objectives only relate to cloud application/s/services from a system admin perspective and not internal network infrastructure as that isn’t something RestAssured targets.

**6.6.4 Opportunities for Consultancy Services**

OCC plan to further exploit the project results from RestAssured by offering consultancy services to new or existing clients. The project results can be used directly as case studies to demonstrate the project concepts and software working in real scenarios to engage and introduce clients to project work. This presents opportunities to sell additional customisation and integration of these tools, or consultancy advice and knowledge gained through the project work. This consultancy model is being used successfully for other H2020 projects, for example OPERANDO, where RestAssured results will add to the credibility of the current offering to clients. Innovative SMEs have expressed strong interest in consultancy services, where the most recent examples include businesses which have approached OCC:

- a spin-out from Oxford University building tools to manage consent. OCC are using project results as
both a source of software services that can be directly exploited in the management of consent and to establish credibility in the sector. This enables OCC to sell integration and consultancy services

- a spin-out from Royal Holloway University, London developing an application to manage and automatically audit access to personal data. This is an ambitious system which has many applications, for example the ability to support data access requests under the GDPR without altering existing databases. RestAssured establishes OCC as a supplier of specialized privacy software development services and connection into European networks concerned with European privacy.

In order to support these exploitation activities, the dissemination work package will collate materials for partners to use in these scenarios to demonstrate the project successfully to new clients or target markets - e.g. the RestAssured Implementation handbook
7 Conclusion

This First Impact and Innovation Management Summary Report outlines our progress against the plans and actions set out in D9.2. This document takes all dissemination and exploitation opportunities defined in D9.2. and reports on what has been done, the impact of what has been done, what will be done in the next reporting period.

While RestAssured itself is not aimed at creating a commercial product, this report shows how the 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. Our impact plans are therefore targeted at the scientific and business communities and the formation of the RestAssured lead Common Dissemination Booster is an important part of this process.

The project has established a good dissemination baseline through a combination of the project website, blog and social media usage. Importantly, given the focus on the scientific and research communities the project has already produced a number of high profile journal and conference publications.

IBM, IT Innovation and UDE’s exploitation plans focus on benefits to the scientific community, both within their own organization and to other universities and research labs. Thales, OCC and Adaptant will use the technologies as building block for their commercial offerings and to create a competitive advantage through reduction of hosting costs and the costs of building and demonstrating that our product offerings meet security, certification and compliance criteria.

Much remains to be done. The first 18 months have focused on research and prototype code development. This report is important because it sets out how the partners will use the prototypes to demonstrate impact by the end of the project given what we now know about the RestAssured architecture and technologies.