TCOMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

CIP-ICT-PSP-2013-7

AN ADVANCE SERVICE DISTRIBUTION NETWORK AND TOOLS FOR INTEROPERABLE PROGRAMMABLE, AND EXPLOITATION OF UNIFIED PUBLIC CLOUD SERVICES

Deliverable D4.4a

Integrated STRATEGIC Framework and Cloud Infrastructures

Workpackage	WP4 – Framework Implementation, Integration, and Test
Editor(s):	Enric Pages (ATOS), Joshua Daniel (BT), Gery Ducatel (BT), Giannis Ledakis (SILO)
Responsible Partner:	ATOS
Quality Reviewers	BT and SILO
Status-Version:	V1.0.
Date:	22/06/2015
EC Distribution:	Public
Abstract:	This deliverable will reflect the outcome of task T4.5. It comprises the prototype implementation of the integrated STRATEGIC framework, including the cloud infrastructures that supports it. The framework is going to be delivered into two iterations and it will comprise the results of deliverables D4.1, D4.2 and D4.3.

This project has received funding from the European Union's Competitiveness and Innovation Framework Programme under grant agreement no 325138

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	**Modified by**
v1.0	09/03/2015	Initial specification of ToC	ATOS
V2.0	11/03/2015	Section 1	ATOS
V3.0	20/03/2015	Section 1, section	ATOS
V4.0	05/04/2015	Validation	ATOS
V5.0	15/04/2015	Requirements list and TC list	ATOS
V6.0	29/04/2015	All sections.	ATOS
V7.0	11/05/2015	Review	ATOS
V9.0	15/05/2015	Address reviewer's comments.	ATOS

Contents

List of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym	Title
Administrator	Customer account administrator, typically, the user who has opened the account in the Marketplace.
API	Application Programmatic Interface: input and output channels into software products for interaction.
AWS	Amazon flagship virtualisation service (Amazon Web Service).
CBA	Cross-Border Authentication
COR	Certificate of Residence
Cloud Broker	An application that allows end users to choose a cloud service on the basis of price and capabilities.
CloudPlatform	A Citrix private cloud interface software originally based on CloudStack.
CloudStack	An Apache licensed private cloud interface software which is the basis of CloudPlatform.
CRUD	Create Remove Update Delete. This refers to a user management interface.
CSV	Comma Separated Values. A file standard to save, and transfer platform independent data.
Developers	Software providers for the Marketplace.
IaaS	Infrastructure as a Service. A virtualisation technology that creates Virtual Machines loaded with an Operating System accessible remotely.
IMS (user store)	Identity Management Service. A user directory product in the Marketplace.
ISV	Independent Software Vendor.
KSM	Kernel-based Virtual Machine. A technology that allows the deployment of a hypervisor onto a Linux kernel. This allows the transformation of a standard Linux server into a low level virtualisation server.
LDAP	Lightweight Directory Access Protocol. A protocol to read and write information from a user database. Often used to also refer the said user database.
Marketplace	The Marketplace is the web based console user access to buy and sell services. The marketplace is the host of the Service Store.
Multi-cloud	The ability to target different cloud targets.
OpenStack	A private virtualisation software which was originally developed by Rackspace. OpenStack is Open Source under Apache licence.
OPTIMIS	A European project which focussed on optimisation tools for cloud brokering services.
OS	Operating System, e.g. Linux, Windows, etc…
OVA	Open Virtualisation Archive. A file that is used to save an entire Virtual Machine usually for backup, or transfer.
P2V	Physical to Virtual. A tool to create a Virtual Machine from an existing physical machine or server.
PaaS	Platform as a Service. A cloud computing service that

Acronym	Title
	provides access to software stacks and services.
Rackspace	A company that provides public cloud platform technology.
RDP	Remote Desktop Access. A Microsoft proprietary protocol to view and interface with a virtual machine.
REST	Representational State Transfer. An interoperability framework for web based applications. This is typically used for web consoles, or applications to obtain read and write access to an on-line service.
Server Template	A file that can be loaded to obtain a Virtual Machine manageable from a virtual interface console (such as the Marketplace).
Service Store	The service functions of the Marketplace.
STRATEGIC Administrators	Users that have access to the administrative console of the marketplace.
URL	Universal Resource Locator. Used to represent locations such as web addresses.
VMWare	A company selling low level virtualisation technology.
VMWare VCloud	A VMWare product for private cloud.
Windows Azure	A cloud computing platform from Microsoft providing IaaS, and PaaS.
Xen	A type of hypervisor provided Open Source under the GPL license (General Public License)

Table 1: Definitions, Acronyms and Abbreviations

Executive Summary

The goal of the STRATEGIC project is to facilitate organizations and notably public bodies to leverage the benefits of public cloud services. STRATEGIC Framework is supporting pilot partners to make an informed decision with regards to cloud hosting. Public bodies are adopting IaaS solutions for deploying online governmental services using for this purpose different cloud topologies such as private cloud solutions while other public bodies uses hybrid or public offerings.

T4.5 Platform Integration and Validation task will integrate the STRATEGIC framework on the basis of results from the previous tasks. It will also ensure that the cloud infrastructures (e.g., hosting infrastructures, marketplace infrastructures) required for the validation and the operation of the framework are in place and operational. The integration will be carried out in an iterative and evolutionary way. The first iteration/release provides the baseline STRATEGIC framework that is exploited in order to start the pilot operations, as well as an accompanying report D.4.4a Integrated STRATEGIC Framework and Cloud Infrastructures.

This document reflects the outcome of task T4.5. It comprises the prototype implementation of the integrated STRATEGIC framework, including the cloud infrastructures supporting it. The framework will be delivered into two iterations and it will comprise the results of deliverables D4.1 [7], D4.2 [8] and D4.3 [9].

The STRATEGIC architecture was designed taking into consideration the business requirements for public bodies, captured during the stakeholder's interviews in combination of the requirements depicted from the analysis of diverse set of public and private sector organizations, as well as analyzing the applications used by the public organizations within STRATEGIC.

The accompanying report of the prototype implementation of the STRATEGIC platform (D.4.4a) goes through the bottom up approach followed during the project, from the requirements to meet, captured during the first half of the project, to a granular reference implementation of the framework. Following with the aforementioned bottom up approach, several software components and 3rd party systems have been put in place, in order to came up with a platform that covers the requirements stated at design phase by stakeholders and pilot partners, offering a secure cloud environment where to on-board their applications.

The first STRATEGIC iteration is focused on the core Managed Services needed to operate the Cloud Service Providers while the second iteration will be devoted to the implementation of horizontal security services and the enhancement of the application workflow. More in detail, the STRATEGIC Service Store released in this first iteration is a top layer interface allowing the management of service and infrastructures deployed onto the cloud. Additionally the Service Store offers multi-provider support enabling the use of both private and public providers, as well as other cloud topologies that are based on the combination of the previous ones such as community or hybrid cloud topologies.

In this first stage, the deployment of the cloud infrastructures comprising the STRATEGIC framework have been installed in the premises of some of the technology partners (BT, SILO) in order to support the early operation of the pilots.

Finally, this document enumerates the validation test cases executed from the STRATEGIC Service Store to verify the correctness of the functionalities and assess the added value offered by the platform. In an initial stage, the first iteration of the STRATEGIC framework has been validated against a public cloud provider, using Amazon EC2 and Amazon S3 cloud services for this purpose. A traceability table where requirements are mapped into test cases is also provided.

1 Introduction

The goal of the STRATEGIC project is to facilitate organizations and notably public bodies to leverage the benefits of public cloud services, through boosting three complementary adoption directions: (a) The porting of existing online services to the Cloud, (b) The adaptation and localization of existing services, which have been successfully deployed by other organisations and (c) The composition of new public cloud services on the basis of available legacy services.

T4.5 Platform Integration and Validation: This task will integrate the STRATEGIC framework on the basis of results from the previous tasks. It will also ensure that the cloud infrastructures (e.g., hosting infrastructures, marketplace infrastructures) required for the validation and the operation of the framework are in place and operational. The integration will be carried out in an iterative and evolutionary way. The first iteration/release provides the baseline STRATEGIC framework that is exploited in order to start the pilot operations, as well as an accompanying report D.4.4a Integrated STRATEGIC Framework and Cloud Infrastructures.

1.1 Scope of the document

D4.4a Integrated STRATEGIC Framework and cloud infrastructure: This deliverable will reflect the outcome of task T4.5. It will be the prototype implementation of the integrated STRATEGIC framework, including the cloud infrastructures that will support it. The framework will be delivered into two iterations and it will comprise the results of deliverables D4.1, D4.2 and D4.3.

D4.1a, D4.1b, D4.1c STRATEGIC Cloud Broker / Marketplace: This deliverable will be a prototype and an accompanying report associated with the implementation of the STRATEGIC Cloud Broker (based on OPTIMIS), as well as with the establishment of the marketplace infrastructure of the project. It will be based on the outcomes of tasks T4.2. It will be delivered in three iterations. The early iteration will provide an infrastructure for the early commencement of the pilots and for the conclusion of the pilot preparation activities, the second iteration will include horizontal security services (required for WP5), and the final iteration will provide the deployment capability in the marketplace.

D4.2a, D4.2b Migration, Adaptation, Localization and Governance Tools: This deliverable will reflect the outcomes of tasks T4.1 and T4.3. It will be an integrated prototype of the migration, adaptation, localization and governance services of the STRATEGIC framework, along with an accompanying report.

D4.3a, D4.3b: Trust and Security Components: Prototypical implementations for integration in the overall architecture. The implemented security functionalities will move the 'trust anchor' to the Cloud and are related to electronic identity authentication, authorization policies, privacy-related issues, user consent to release personal information, collaboration and trust management between identity federations, origin discovery service and policy management. The deliverable will reflect the outcomes of task T4.4.

In addition the second iteration of this document will include the outcomes of T.4.6 Application and Data protection as Service, as part of the enhancements and fine-tuning that are going to be included in the second release of the framework.

1.2 Target audiences

This document is addressed to public organizations that plan to on-board STRATEGIC. It is also addressed to pilot partners in preparation and conduction of their use cases within WP5 and WP6.

1.3 Structure of the document

The document has two main sections which describe the reference implementation of the STRATEGIC framework based on the previously provided design and architecture, as well as the early validation of the aforementioned reference implementation focusing on public cloud offering for this first iteration.

2 Integrated STRATEGIC Framework

2.1 Framework requirements overview

The STRATEGIC architecture was designed taking into consideration the business requirements for public bodies, captured during the stakeholder's interviews in combination of the requirements depicted from the analysis of diverse set of public and private sector organizations, as well as analyzing the applications used by the public organizations within STRATEGIC.

The main functionalities to archive by the framework are related to:

- Porting Public Bodies applications to the cloud.
- Adapt the aforementioned applications to take under consideration localization and privacy aspects at deployment and operation time of the cloud service.
- Allow the composition of complex services (multi-tiered applications), publishing them if applicable in a "re-sellable" way.

The requirements considered to build the framework are summarized below:

Requirements elicitation was conducted through:

- Interviews from stakeholders (cloud users and cloud providers)
- Analyzing a diverse set of public and private sector organizations.

The platform functionalities to archive are divided into functional and non-functional requirements, prioritizing the functional ones.

Functional requirements	**Non-functional requirements**
• Security and privacy • High Availability • Interoperability, portability	• Good performance • Lower costs

The technical requirements were captured after analyzing the applications used by the municipalities within STRATEGIC project.

- Common Application Packaging Format
- Configuration Management
- Interoperability at hypervisor level
- Interoperability on monitoring

An extended overview of STRATEGIC requirements is included in **Table 4:** STRATEGIC Requirements, further information was included in "D.2.1 report on Stakeholders Requirements" [1] and "D.2.2 Pilot Scenarios, Use Cases and Pilot Operations Requirements" [2].

2.2 Technical Design and Implementation

2.2.1 Framework Design

As stated before, the architecture was designed taking into consideration the requirement analysis performed under tasks T.2.1, T.2.2, T.2.3 and their associated deliverables within WP2.

The framework design was produced using a bottom up approach, from the requirements to the high level architectures, as stated in previous section, and from the high level architecture to a granular reference implementation of the architecture, which will be covered in the following sections within this document.

The high level architecture consists mainly of the following software components:

- Packaged Application Repository
- Configuration Recipes Repository
- Application Instantiation Workflow Component
- Governance Component
- Credential Management Component
- Configuration Server
- Billing Component.

Moreover, the Cloud Orchestrator is accompanied by two external Services:

- The Threat Intelligence Service
- The Monitoring Service

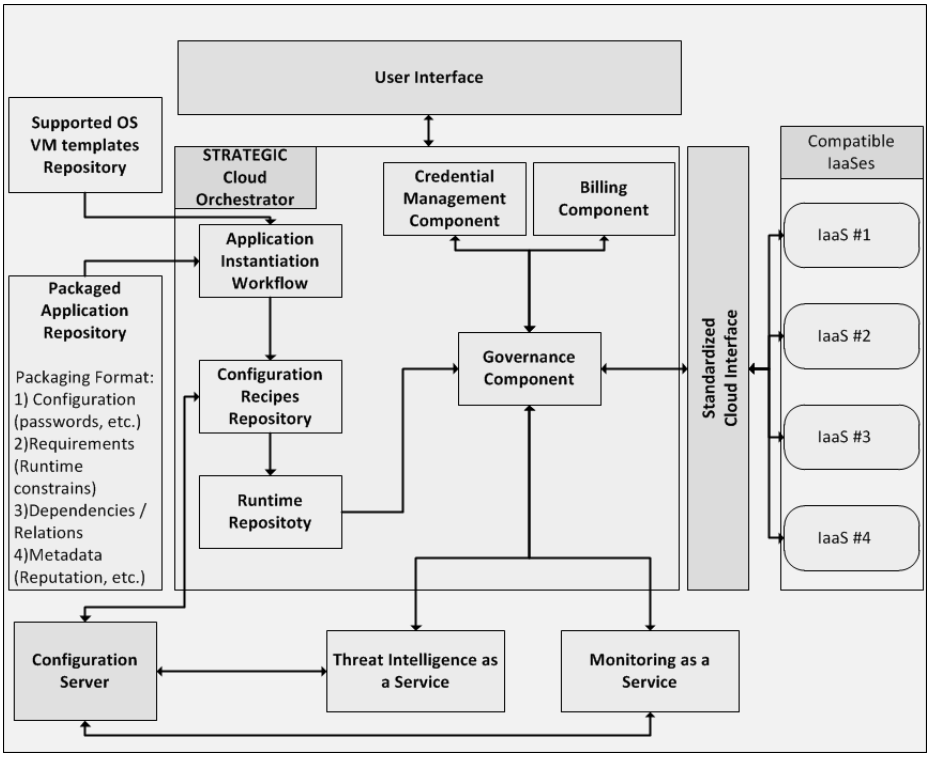

Figure 1: STRATEGIC High Level Architecture

The technical specifications for all the components that compose the STRATEGIC framework were fully described within the document "D.2.3 STRATEGIC Framework Architecture and Technical Specifications" [3].

The following section will illustrate how the components specified in the high level architecture are mapped within a reference implementation to cover the STRATEGIC goals.

2.2.2 Framework Reference Implementation

There are many alternatives that can fit the needs of STRATEGIC Architecture (see Figure 1). Some of them include heavy adaptation of existing Cloud orchestrators and other alternatives, which reduce the support that is required during the implementation, include the possibility of radical enrichment of a tool that is provided and used by one of the partners (e.g. BT Service Store).

Following with the aforementioned bottom up approach, from the high level architecture depicted in Figure 1 towards the implementation of a granular reference implementation of the architecture (see Figure 5 and Figure 6), several software components and 3rd party systems have been put in place, in order to came up with a platform that covers the requirements stated at design phase by stakeholders and pilot partners, offering a secure cloud environment where to on-board their applications.

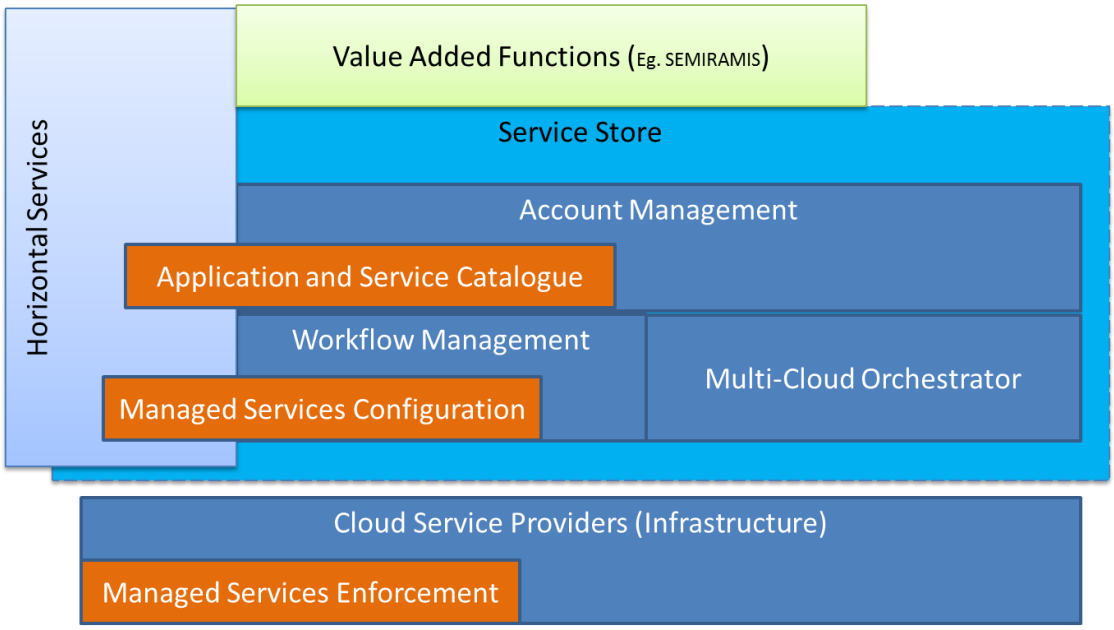

Figure 2: STRATEGIC offering layers

Figure 2 representing the STRATEGIC offering layers that include Infrastructure layer, Managed Services layer (security horizontal services, Service Store) and added value application/workflow components like STORK/SEMIRAMIS. The first STRATEGIC iteration includes de core Managed Services needed to operate the Cloud Service Providers while the second iteration will be focused on horizontal security services and the enhancement of the application workflow.

The STRATEGIC Service Store released for the first iteration is a top layer interface (see **Error! Reference source not found.** and **Error! Reference source not found.**) which allows the management of service and infrastructures deployed onto the cloud. The framework offers a marketplace accessible through a web portal where pilots are able to interact with the platform providing applications to be deployed in the cloud, and allow developers to configure and manage the cloud based applications flows enabling the development, integration, life cycle management and monitoring of applications.

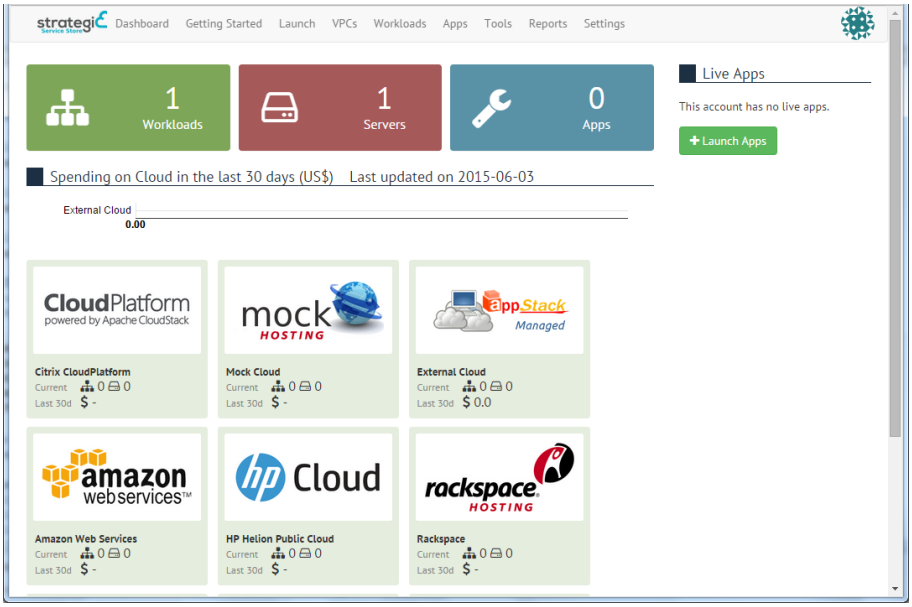

Figure 3: Landing portal of the STRATEGIC Marketplace

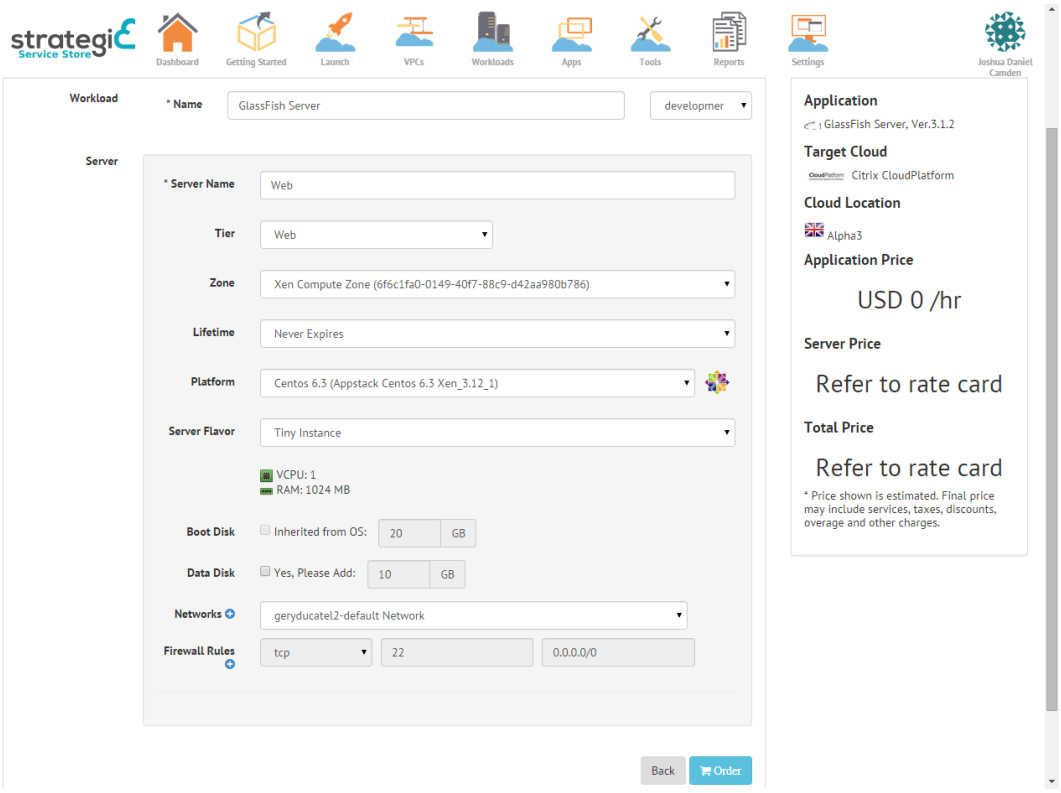

Figure 4: Application launch page

(The centre of the screen shows the technical specification page configuration. The right hand side shows the summary elements: application, target cloud, cloud location, application price, server price, and total price)

Integrated into the Service Store a monitoring system provides performance and availability information associated to the deployments, enabling the governance system to trigger actions related to the virtual resources that compose the service (instantiating new virtual images, decommissioning or migrating the resources).

The following components designed in the architecture are included in the first iteration of the STRATEGIC framework:

- ✓ STRATEGIC Web Console (see Figure 5)
- ✓ Application Repository/Marketplace (see Figure 5)
- ✓ Standardized Cloud Interface (STRATEGIC Core) (see Figure 5)
- ✓ Monitoring-As-A-Service Component (see Figure 5)
- ✓ Identity Management (see Figure 5)
- ✓ Accounting & Billing Component (see Figure 5)

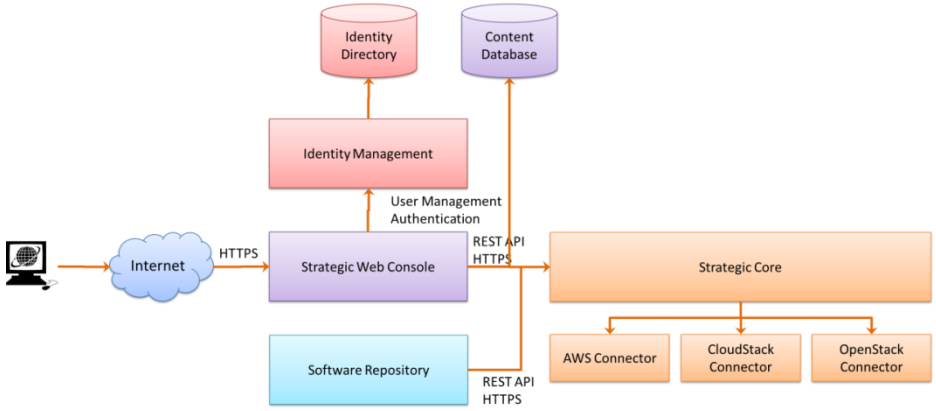

Figure 5: STRATEGIC Service Store Design

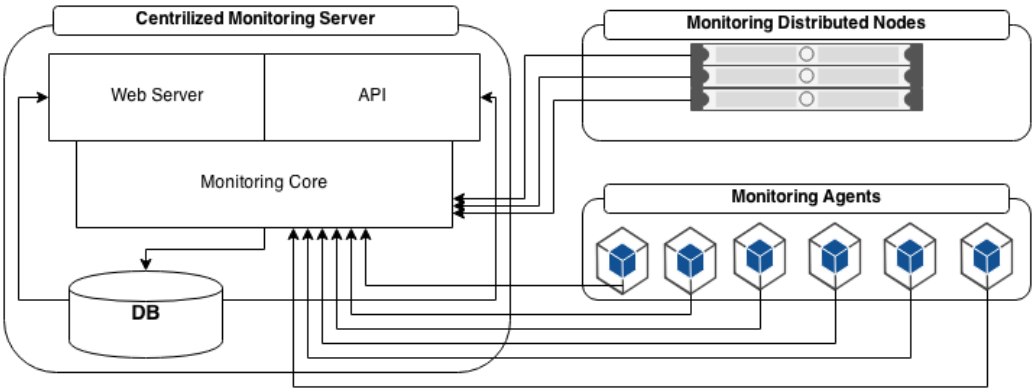

Figure 6: STRATEGIC Monitoring Service

Further information about the Service Store and the monitoring system is covered in document "D.4.1a STRATEGIC Cloud Broker and Marketplace" [7] and will be extended in D.4.1b [7] for the second iteration of the framework, which plans to include some enhancements as well as incorporate the horizontal security services into the STRATEGIC Service Store.

The marketplace runs from a Xen, or VMWare hypervisor. The server which runs these applications will have different specifications according to the expected usage. For the purpose of STRATEGIC, the Marketplace is made available from a single server with the following specifications:

- 8GB RAM
- 4vCPU's - AMD Opteron 2.3MHz (using 20%)
- 2 x HDD (250GB / 500GB)
- OS - Ubuntu 12.04.4 LTS

This can be considered to be a minimum specification. However, in production, these specifications can also be virtualized and made available globally across multiple data centers. Therefore, STRATEGIC offers physical deployment, or virtual hosting possibilities.

Both private clouds and public clouds can be supported in STRATEGIC. This includes:

- BT Cloud Compute (public)

- Amazon EC2 (public)
- Windows Azure (public)
- Racksphace (public)
- VMware vCloud Hybrid Service (private)
- CloudPlatform (private)
- Openstack (private)
- HP Cloud Helion (private)

STRATEGIC Marketplace allows application to be deployed onto one or multiple target clouds. The Marketplaces also synchronizes costs of IaaS with public clouds so as to provide aggregated deployment costs to customers. The Marketplace acts as a single point of control and security management for multiple cloud deployment.

2.2.3 Cloud Infrastructures Reference Implementation

Within STRATEGIC project, the cloud infrastructures are offered with the paradigm of IaaS cloud delivery model (see Figure 7). IaaS paradigm allows consumers to have control over operating systems, storage, applications and networking components while the control of the underlying cloud infrastructure is managed by a Service Provider, in our case managed by the STRATEGIC Service Store described above.

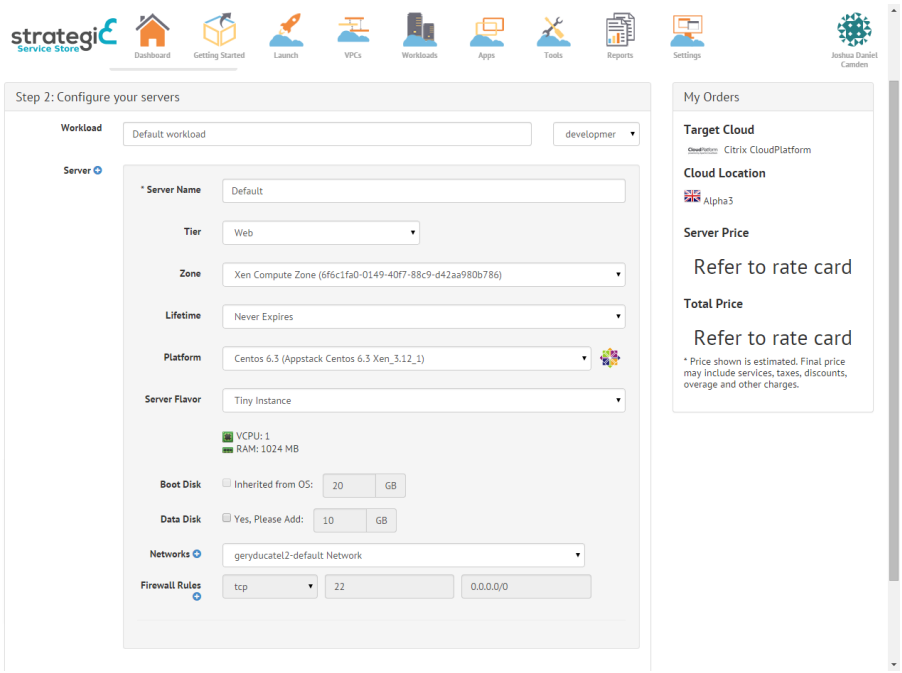

Figure 7: IaaS server configuration screen

(this allows users to control remotely hosted Virtual Machine providing the meta data required by the hosting platform (this screen shows a Cloud Platform Virtual Machine configuration))

The Service Store, released in the first iteration of the STARTEGIC framework, offers multi-provider support enabling the use of both private and public providers, as well as other cloud topologies that are based on the combination of the previous ones such as community or hybrid cloud topologies.

The deployment of the cloud infrastructures, which comprises the STRATEGIC framework, originally planned across all pilot sites have been installed in the premises of some of the technology partners (BT, SILO) for the first iteration of the framework, in order to support the early operation of the pilots. Afterwards each public body will evaluate the need to have their own cloud infrastructures installed in their own premises.

The installation and deployment of the cloud infrastructures have been divided in several phases to support the implementation and integration during the first year when the implantation of the reference implementation of the STRATEGIC framework takes place.

- *Phase1:* **Public Provider**

Initially a public provider has been used for the early validation of the first versions Service Store, each technology partner used their own accounts within Amazon Web Services (EC2, S3) to create toy examples for pilots as well as validate the functionalities offered by the first iteration of the STRATEGIC framework.

- *Phase2:* **Private Provider (OpenStack -- Havana)**

Additionally to the public provider described in phase1, a private cloud provider based on OpenStack has been installed in SILO premises to start the packaging of the pilot applications. This phase has been used to train pilot partners.

- *Phase3:* **Private Provider (OpenStack --Icehouse) + Cloudstack (BT Cloud) + Public Provider (AWS)**

The Private Cloud located in SILO premises have been upgraded to OpenStack 'Icehouse' to allow the integration of the private provider with the STRATEGIC Service Store which did not offers 'Havana' support at the time of the integration process.

In addition to the aforementioned private cloud, based on OpenStack, another private provider have been configured and deployed in BT premises. This second IP have been based on CloudStack and both have been registered within the Service Store to enable the deployments and tests from both technical and pilot partners. During the third phase the public provider deployed initially remains accessible from the Service Store converting our environment in a hybrid cloud.

Aiming to facilitate the inclusion of new infrastructure providers, especially from the pilot partners, and in order to deal with the administration complexity of the physical infrastructural elements a Metal-as-as-Service (MaaS) layer has been added. MaaS is responsible for the "Dynamic provisioning and Scaling" at the physical world through a simple web interface or API.

Further information about cloud infrastructures providers and the MaaS layer can be found in *"D5.1a – Cloud-Enablement of Distributed Services" [11].*

2.3 Interactions with STRATEGIC framework User Types

The framework built is structured in a modular way facilitating the scalability, adaptability, and maintenance of the overall framework. The resultant platform supports multi-tenancy allowing different interactions and user roles to on-board into the platform.

The STRATEGIC **end users** are usually citizens that want to use the applications deployed by public bodies in the cloud. They do not have direct access or control over the framework, but they are interacting and using the cloud based applications deployed through it. To on-board STRATEGIC as an end user, the citizens should be granted into the applications by the public organization that is managing the target application. The aforementioned user management is not part of the STRATEGIC framework, but managed within the applications that are using the framework.

The STRATEGIC **developers** or **ISVs** are persons or organizations responsible of the development and on-boarding of the applications offered by the STRATEGIC Service Store. In some cases those applications are implemented to be sell to other organizations, the platform developed in STRATEGIC allow to re-use the applications in order to be used by 3rd parties.

The **public bodies** are the main customers of STRATEGIC, they are responsible for the proper configuration, life-time management and deployment of the cloud based applications deployed and operated in STRATEGIC.

Both developers and public bodies may take advantage of the open meta-model proposed to package STRATEGIC applications, which is expressive enough to manage the life-time of the applications packaged as well as offers an intuitive way to abstract the configuration of the applications in order to allow their deployment and operation over different types of infrastructure providers. The meta-model used is encoded in JavaScript Object Notation (JSON) that is completely language independent but uses conventions that are familiar to programmers. The proposed meta-model is described in more detail under "D3.1 Specification of Cloud-Enablement and Migration Solutions and Services"[4].

The **STRATEGIC administrator** is responsible for the management of STRATEGIC Service Store, managing the product portfolio available through the marketplace. This role is granted for all the functionalities of the system allowing the management of other roles as well enable/disable framework functionalities, register cloud providers and on-board applications.

The **Cloud Infrastructure Provider** refers to the cloud hosting infrastructures needed to operate the cloud based applications. The STRATEGIC framework includes multi-provider support, enabling different cloud topologies to be used within STRATEGIC such us private, public, hybrid cloud topologies.

Further information about how to onboard new applications or infrastructures into STRATEGIC is fully covered in document "D3.2 Specification of Development and Governance Services" [5].

3 STRATEGIC Framework Validation

3.1 Framework Validation

The validation process performed in STRATEGIC aims to evaluate the framework and software components functionalities to assess those SW modules and systems operate as expected and effectively. Most of the test cases described below have been executed through the Service Store which is the main entry point for STRATEGIC deployments and operations.

The first iteration of the STRATEGIC framework, in an initial stage, has been validated against a public cloud provider, using Amazon EC2 and Amazon S3 cloud services for this purpose. Afterwards private cloud providers were included through the Service Store which allows us to double-check the test cases previously validated for the public provider against a private provider. The validation of the horizontal security services have been not included in the first iteration and consequently will be included in the validation of the second iteration, together with the validation of other framework enhancements.

Test Case Name	Description	Status	Comments
TC_UserRoles	Ability to offer multi-tenancy support.	☑	Within the Service Store different user roles can be configured.
TC_PublicProvider	Register AWS provider in the Service Store.	☑	Amazon AWS have been registered as public provider for the early validation of the Service Store functionalities.
TC_PrivateProvider	Register CloudStack provider in the Service Store.	☑	BT Cloud, based on CloudStack has been registered as private provider.
TC_HybridCloud	Register both private and public providers	☑	See previous TCs.
TC_Package_MonoliticAPP	Package cloud based application in a single-node using the Service Store.	☑	Several single-VM cloud based applications have been created from the applications available in the STRATEGIC marketplace. (RDBS,

Test Case Name	Description	Status	Comments
			Web Servers, Load Balancers, CMS, …)
TC_Pacakge_NTierAPP	Package N-tier complex applications using the Service Store.	☑	We created the typical 3-Tier workload to test Service Store functionalities. The 3-tier workload have been configured with an HA proxy as load balancer, MySQL as database back-end and Apache Tomcat as web server.
TC_ResellableAPP	Make the packaged appilcation re-sellable.	☑	In order to make applications re-sellable your user has to become APPSeller.
TC_ReusableAPP	Make the packaged application re-usable.	☑	Any cloud service configured from the Service Store could be instantiated many times.
TC_VM_Create	Create the cloud based workload virtual resources from the Service Store.	☑	Both single-node and N-tiered applications and their associated post-configuration hooks can be created.
TC_VM_Deploy	Deploy the virtual resources associated with the cloud service.	☑	Deployment capabilities have been validated in both public and private providers.
TC_VM_ReDeploy	ReDeploy the virtual resources associated with the cloud service.	☑	Redeployment capability has been validated; it implies the redeployment of all virtual resources of the service.

Test Case Name	Description	Status	Comments
TC_VM_UnDeploy	UnDeploy the virtual resources associated with the cloud service.	☑	Undeployment capability has been validated, the associated cloud service is not removed from the system and it could be used afterwards.
TC_VM_Delete	Delete the cloud based workloads from the Service Store.	☑	After deletion the cloud service cannot be used anymore.
TC_VM_MultiPlatform	Ability to deploy virtual resources with different operating systems.	☑	Several operating systems have been tested to validate multi-platform support (Debian, Ubuntu, CentOS and Windows distributions were tested).
TC_VM_MIGRATION	Migrate VMs between physical resources	☑	VMs can be migrated between physical nodes; the migration process can be triggered based on performance KPIs.
TC_Deployment_Monolitic	Deploy cloud based application in a single-node using the Service Store.	☑	Several single-VM cloud based applications have been deployed using the applications available in the STRATEGIC marketplace. (RDBS, Web Servers, Load Balancers, CMS, …)
TC_Deployment_NTier	Deploy N-tier complex applications using the Service Store.	☑	We deployed the typical 3-Tier workload to validate Service Store functionalities. The 3-tier workload have been configured with an HA proxy as load

Test Case Name	Description	Status	Comments
			balancer, MySQL as database back-end and Apache Tomcat as web server.
TC_MonoliticAPP_Monitoring	Ability to monitor monolithic applications.	☑	Performance and availability information measurements are collected by the monitoring system.
TC_NTierAPP_Monitoring	Ability to monitor N-tier applications.	☑	Monitored services can be identified in the monitoring system as they use the same monitoring path: "OrganizationName::Workload_Identifier::Image_Identifier"

Table 2: STRATEGIC Framework Test Cases

3.2 Cloud Infrastrucutre Validation

Test Case Name	Description	Status	Comments
TC_OnBoard_PrivateProvider	Register Private Provider through the Service Store	☑	Several private provider can be on-boarded into the Service Store (VCloud, Citrix Cloud Platform, OpenStack, CloudStack)
TC_OnBoard_PublicProvider	Register Public Provider through the Service Store	☑	Several public providers can be on-boarded into the Service Store (AWS, Microsoft Azure, Rackspace Cloud, HP Cloud, IBM Smart Cloud)
TC_OnBoard_MultiProvider	Register both Private and Public Provider through the	☑	The current configuration for the first iteration of the

Test Case Name	Description	Status	Comments
	Service Store		STRATEGIC framework includes both public and private providers (AWS, CloudStack, OpenStack)

Table 3: STRATEGIC Cloud Infrastructures Test Cases

3.3 Traceability

Requirement Number	Requirement Name	Short Description
CAMDEN_Req_1	Horizontal Security Services	Ability to protect the computing resources with Cloud based security solutions.
CAMDEN_Req_2	IaaS Diversity	Ability to use and manage public resources effectively from the STRATEGIC platform.
CAMDEN_Req_3	Auto-bursting capabilities / Elasticity	Ability to scale the service as and when required. Ability to Scale the portal as the number, size and download rate of datasets increases.
CAMDEN_Req_4	Limit in-house resources	Frees up internal Camden's internal computing resources for further internal innovation.
CAMDEN_Req_5	Re-usability / Re-sellability	Ability to publish and resell the application through STRATEGIC platform/marketplace.
CAMDEN_Req_6	Manageability	Ability to use and manage public resources effectively from the STRATEGIC platform.
CAMDEN_Req_7	Centralized Control	Provides centralised homogenous capability management.
CAMDEN_Req_8	Identify Management	Dedicated identity software maintenance and management.
CAMDEN_Req_10	Cost-efficiency	Ability to use cost-efficient public Cloud resources effectively from the STRATEGIC platform.
STARIGRAD_Req_1	Cost Optimisation	Reducing costs for infrastructure and applications via virtualized resources.
STARIGRAD_Req_2	Optimisation of resource utilization	Getting experience of cloud/virtualisation services' utilization.

Requirement Number	Requirement Name	Short Description
STARIGRAD_Req_3	Limit in-house resources	Frees up internal Stari-Grad's computing resources.
STARIGRAD_Req_4	Secure information exchange mechanism	Ability to protect the computing resources with Cloud based security solutions and offering citizens a secure and privacy aware mechanism of cross-border attributes exchange.
STARIGRAD_Req_5	Re-usability	Ability to publish and resell the application through STRATEGIC platform to other Serbian public bodies.
GENOA_Req_1	Cost-Optimisation	Reducing costs for infrastructure and applications via virtualised resources.
GENOA_Req_2	Unified Authorization	Unified authorization service and integration of central authorization service.
GENOA_Req_3	Secure information exchange mechanism	Ability to protect the computing resources with Cloud based security solutions.
GENOA_Req_4	Optimise develop-to-deploy cycle	Easy deployment of an innovative service.
PILOTS_Req_1	Requirements to operate Pilot site	• Deploy application • Manage application • Scale Application • Storage • Compute nodes • Network Bandwidth
PILOTS_Req_2	Requirements for data security	• Security tools to protect VM and data. • Support of Private Cloud IaaS for safe storage of the citizen private data. • Compliance with local requirements and restrictions. • Support for cross border authentication and data exchange.
PILOTS_Req_3	Requirements for network access	• Availability to deploy selected applications in private and protected networks accessible only via VPN connections. • Advanced network configuration.

Requirement Number	Requirement Name	Short Description
		• Public availability for selected applications. • Cryptographically secured connections for selected application
PILOTS_Req_4	Managerial Requirements	• Ability to deploy an application to a multitude of IaaS offerings, public or private. • Ability to use an easy to manage interface/ marketplace that allows the deployment of services. • Ability to publish new applications or reuse already published applications.
STRATEGIC_Req_1	Extend set of provisioned cloud services to public sector	Provision of cloud computing in public administrations is limited or in many cases even non-existent.
STRATEGIC_Req_2	SaaS, PaaS, IaaS support	Allow public and private solutions to on-board the cloud based applications into STRATEGIC.
STRATEGIC_Req_3	Interoperable Interfaces	Enabling the portability between providers, disaster recovery.
STRATEGIC_Req_4	Migration paths	Migration from existing solutions being interoperable.
STRATEGIC_Req_5	Security, Privacy and confidentiality	Guarantee security, privacy and confidentiality through cloud security services.
STRATEGIC_Req_6	Privacy-data protection	Compliance with EU and national directives.
STRATEGIC_Req_7	Identification of physical data location	Used for determination of jurisdiction and applicable law
STRATEGIC_Req_7	Legislation-aware services	To consider when to re-use cloud services from another countries.
STRATEGIC_Req_8	Costs estimation	Estimations of costs involved for migration to the cloud.

Requirement Number	Requirement Name	Short Description
Global_IdValidation_Req_01	User validation	The identity of the user SHALL be validated by the system.
Global_Notification_Req_01	Feedback	There SHALL be mechanisms to report both success and failures of information retrieval.
Global_UserConsent_01	Personal Information Access	The user SHALL take control about his personal information releasing.
Global_AccessProtection_Req_01	Sensitive information protection	Service providers and identity aggregators SHALL provide security mechanisms to protect the access to sensitive information from unauthorized access.
Global_Integrity_Req_01	Receive credentials securely	Whenever the user transmits his credentials to an authentication authority, the transmission MUST be secured.
Global_Privacy_Req_01	Avoid unnecessary access	Any unnecessary access MUST be avoided.
Global_Privacy_Req_02	Authentication only when required	The user MUST be asked for authentication only when the authentication is required for executing the accordant task.
Global_Privacy_Req_03	Only required attributes	Only these attributes of the user MUST be requested, that are required for executing the accordant task.
Global_Privacy_Req_04	Handle private data correctly	Components that handle user data MUST handle them correctly in that way they have specified, i.e., in accordance to process purposes.
Global_Privacy_Req_05	Inform user about purpose of authentication	The user SHALL be informed about the purpose of his authentication, i.e., why does he has to authenticate and what will be done with the authentication information.
Global_Privacy_Req_06	Process only requested attributes	When an attribute provider receives a request for attribute release, it MUST only process the requested attributes

Requirement Number	Requirement Name	Short Description
Global_Privacy_ Req_07	Use pseudonyms	As often as possible the system SHALL use pseudonyms for the user when requesting private data from different sources.
Global_Privacy_ Req_08	Use correct credentials	The user SHALL use the correct credentials when carrying out a login.
COR_Integrity_ Req_01	Receive approval securely	When the user approves the release of his private governmental data, the approval decision MUST be transmitted securely. Refines: Global_Integrity_Req_01
COR_Privacy_Re q_01	Only attributes required for certificate of residence	Only these attributes of the user MUST be requested at the Home Government, that are required for issuing the new certificate of residence Refines: Global_Privacy_03
COR_Privacy_Re q_02	Use correct credentials	The user SHALL use the correct credentials from his Home government eID when carrying out the login. Refines: Global_Privacy_08
COR_Privacy_ Req_03	Specify correct data sources	The user SHALL specify the sources of his residence information correctly at his Identity Aggregator in his Home Government federation. *Refines*: Global_Privacy_Req_09
CBA_Privacy_ Req_01	Explicit user consent required	User MUST be informed about the attributes to be exchanged and an explicit acceptance MUST be provided by the user before accessing user data.
CBA_Privacy_ Req_02	Minimal disclosure of data	Service MUST ask the minimum number of attributes needed, and the source of data MUST disclose only the attributes consent by the user.
CBA_Privacy_Re q_03	Second user consent	User can be optionally informed about the attributes values obtained that will be exchanged.
CBA_Security_ Req__01	Information integrity protected	Information exchange MUST be protected against changes.

Requirement Number	Requirement Name	Short Description
CBA_Security_02	Information protection	Protocols MUST use an encrypted channel to protect the information exchanged.
CBA_Security_Req_03	Traceability preserving user's privacy	Services MUST support the traceability of the electronic identification process preserving user's privacy.
CBA_Security_Req_04	Protection of international disclosure of national identifiers	National identifiers should be protected when required by local legislation.
CBA_Security_Req_05	Strong authentication based on eID	User MUST use Strong Authentication using one of the eIDs accepted in his origin country.
CBA_Security_Req_06	Trust relationship between components	Components in the environment MUST have a trust relationship based on digital signature.
CBA_Security_Req_07	Auditing	For the situations where it is intended, it MUST be possible to audit the system to trace fraudulent transactions.

Table 4: STRATEGIC Requirements

Module Tested / Pilot Tested	Test Case Name	Test Case Title
Camden-1	**TC_Camden-1**	Camden use case 1
Camden-2	**TC_Camden-2**	Camden use case 2
Camden-3	**TC_Camden-3**	Camden use case 3
Genoa-1	**TC_Genoa-1**	Genoa use case 1
Genoa-2	**TC_Genoa-2**	Genoa use case 2
Genoa-3	**TC_Genoa-3**	Genoa use case 3
Genoa-4	**TC_Genoa-4**	Genoa use case 4
Stari-Grad-1	**TC_Stari-Grad-1**	Stari Grad use case 1
Stari-Grad-2	**TC_Stari-Grad-2**	Stari Grad use case 2
Stari-Grad-3	**TC_Stari-Grad-3**	Stari Grad use case 3

Module Tested / Pilot Tested	Test Case Name	Test Case Title
Stari-Grad-4	**TC_Stari-Grad-4**	Stari Grad use case 4

Table 5: STRATEGIC Pilots Test Cases

Module/Pilot Tested	Test Case Name	Related Requirements
STRATEGIC Web Console, Identity Management	**TC_UserRoles**	CAMDEN_Req_6, CAMDEN_Req_9, STARIGRAD_Req_2, GENOA_Req_2,
STRATEGIC Web Console, Standardized Cloud Interface	**TC_PublicProvider**	CAMDEN_Req_2, STARIGRAD_Req_3, PILOTS_Req_3,
STRATEGIC Web Console, Standardized Cloud Interface	**TC_PrivateProvider**	CAMDEN_Req_4, STARIGRAD_Req_3, STRATEGIC_Req_3
STRATEGIC Web Console, Standardized Cloud Interface	**TC_HybridCloud**	CAMDEN_Req_2, CAMDEN_Req_8, STARIGRAD_Req_2, STARIGRAD_Req_3, PILOTS_Req_3, STRATEGIC_Req_1, STRATEGIC_Req_3
STRATEGIC Web Console, Application Repository/Marketplace	**TC_Package_MonoliticAPP**	GENOA_Req_4, PILOTS_Req_4, STRATEGIC_Req_2, STRATEGIC_Req_8
STRATEGIC Web Console, Application Repository/Marketplace	**TC_Pacakge_NTierAPP**	CAMDEN_Req_6, CAMDEN_Req_7, CAMDEN_Req_8, STARIGRAD_Req_2, GENOA_Req_4, PILOTS_Req_4, STRATEGIC_Req_2, STRATEGIC_Req_8
STRATEGIC Web Console, Identity Management, Application Repository/Marketplace, Accounting & Billing	**TC_ResellableAPP**	CAMDEN_Req_5, CAMDEN_Req_10, STARIGRAD_Req_1, GENOA_Req_1,

Module/Pilot Tested	Test Case Name	Related Requirements
Component		
STRATEGIC Web Console, Identity Management, Application Repository/Marketplace, Standardized Cloud Interface	**TC_ReusableAPP**	CAMDEN_Req_5, STARIGRAD_Req_5, GENOA_Req_4, PILOTS_Req_4 ,
STRATEGIC Web Console, Application Repository/Marketplace, Standardized Cloud Interface	**TC_VM_Create**	CAMDEN_Req_6, GENOA_Req_4, PILOTS_Req_1
STRATEGIC Web Console, Application Repository/Marketplace, Standardized Cloud Interface	**TC_VM_Deploy**	CAMDEN_Req_6, PILOTS_Req_1
STRATEGIC Web Console, Application Repository/Marketplace, Standardized Cloud Interface	**TC_VM_ReDeploy**	CAMDEN_Req_3, CAMDEN_Req_6, CAMDEN_Req_8, PILOTS_Req_1, STRATEGIC_Req_4, STRATEGIC_Req_7
STRATEGIC Web Console, Application Repository/Marketplace, Standardized Cloud Interface	**TC_VM_UnDeploy**	CAMDEN_Req_6, PILOTS_Req_1
STRATEGIC Web Console, Application Repository/Marketplace, Standardized Cloud Interface	**TC_VM_Delete**	CAMDEN_Req_6, PILOTS_Req_1
Standardized Cloud Interface	**TC_VM_MultiPlatform**	CAMDEN_Req_2, STARIGRAD_Req_3, GENOA_Req_4, PILOTS_Req_3, STRATEGIC_Req_1,

Module/Pilot Tested	Test Case Name	Related Requirements
		STRATEGIC_Req_3
Standardized Cloud Interface	**TC_VM_MIGRATION**	CAMDEN_Req_3, CAMDEN_Req_8, PILOTS_Req_1, PILOTS_Req_3, STRATEGIC_Req_4
Standardized Cloud Interface	**TC_Deployment_Monolitic**	GENOA_Req_4, PILOTS_Req_1, PILOTS_Req_4
Standardized Cloud Interface	**TC_Deployment_NTier**	CAMDEN_Req_6, CAMDEN_Req_7, CAMDEN_Req_8, STARIGRAD_Req_2, GENOA_Req_4, PILOTS_Req_1, PILOTS_Req_4
STRATEGIC Web Console, Monitoring-As-A-Service	**TC_MonoliticAPP_Monitoring**	CAMDEN_Req_2, CAMDEN_Req_8, PILOTS_Req_1, PILOTS_Req_4
STRATEGIC Web Console, Monitoring-As-A-Service	**TC_NTierAPP_Monitoring**	CAMDEN_Req_2, CAMDEN_Req_8, PILOTS_Req_1, PILOTS_Req_4
Camden-1	**TC_Camden-1**	CAMDEN_Req_1, CAMDEN_Req_2,
Camden-2	**TC_Camden-2**	CAMDEN_Req_3, CAMDEN_Req_4, CAMDEN_Req_5, CAMDEN_Req_6
Camden-3	**TC_Camden-3**	CAMDEN_Req_7, CAMDEN_Req_8, CAMDEN_Req_9, CAMDEN_Req_10
Genoa-1	**TC_Genoa-1**	GENOA_Req_1, GENOA_Req_2

Module/Pilot Tested	Test Case Name	Related Requirements
Genoa-2	**TC_Genoa-2**	GENOA_Req_2, GENOA_Req_3
Genoa-3	**TC_Genoa-3**	GENOA_Req_2, GENOA_Req_3
Genoa-4	**TC_Genoa-4**	GENOA_Req_2, GENOA_Req_3, GENOA_Req_4
Stari-Grad-1	**TC_Stari-Grad-1**	STARIGRAD_Req_1, STARIGRAD_Req_2, STARIGRAD_Req_3
Stari-Grad-2	**TC_Stari-Grad-2**	STARIGRAD_Req_4
Stari-Grad-3	**TC_Stari-Grad-3**	STARIGRAD_Req_1, STARIGRAD_Req_2, STARIGRAD_Req_3
Stari-Grad-4	**TC_Stari-Grad-4**	STARIGRAD_Req_3, STARIGRAD_Req_4, STARIGRAD_Req_5

Table 6: STRATEGIC traceability between test cases and requirements

4 Future Plans

The second iteration of the prototype implementation of the integrated STRATEGIC Framework is going to be delivered and the end of the second year of the project. The second release will include enhancement and fine-tuning from the previous version as well as includes horizontal security service into the platform.

The enhancements mentioned are going to be implemented based on pilot feedback, after the operation of their pilots use cases over the platform.

Additionally to the enhancements proposed by pilot partners, the second iteration will include security and trust mechanism. The following components/functionalities are going to be implemented and included in the second release:

- ✓ Application and host protection service
- ✓ Data protection service
- ✓ Cross-border attributes exchange
- ✓ Cross-border authentication engine
- ✓ Trust assessment

5 Conclusions

The STRATEGIC framework released for the first of two iterations accomplishes the project goals for this period, with no deviations from the annex.

Both, the framework and the cloud infrastructures are implemented, integrated and validated to facilitate the early commencement of pilot scenarios within WP5 and WP6.

Despite some security functionalities have been included in the first iteration, most of the horizontal security services will be released in the second iteration, as well as the trust and security functionalities that will be integrated to the STRATEGIC framework. Results from Task4.6, Application and Data protection as Service will be integrated in the second iteration of the deliverable, while the outcomes of Task.4.4. Trust and Security Solutions will be delivered within "D.4.3a, b Trust and Security Components" [9].

6 References

[1] STRATEGIC Deliverable 2.1, Report on Stakeholders Requirements
[2] STRATEGIC Deliverable 2.2, Pilot Scenarios, Use Cases and Pilot Operations Requirements
[3] STRATEGIC Deliverable 2.3, STRATEGIC Framework Architecture and Technical Specifications
[4] STRATEGIC Deliverable 3.1, Specification of Cloud-Enablement and Migration Solutions and Services
[5] STRATEGIC Deliverable 3.2, Specification of Development and Governance Services
[6] STRATEGIC Deliverable 3.3, Use of the STRATEGIC Framework solutions by the Pilot Sites
[7] STRATEGIC Deliverable 4.1a, STRATEGIC Cloud Broker / Marketplace
[8] STRATEGIC Deliverable 4.2a, Migration, Adaptation, Localization and Governance Tools
[9] STRATEGIC Deliverable 4.3a, Trust and Security Components
[10] STRATEGIC Deliverable 4.4b, Integrated STRATEGIC Framework and cloud
[11] STRATEGIC Deliverable 5.1a, Cloud-Enablement of Distributed Services