Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare

Project Acronym: **ASCLEPIOS**
Project Contract Number: **826093**

Programme**: Health, demographic change and wellbeing**
Call: **Trusted digital solutions and Cybersecurity in Health and Care to protect privacy/data/infrastructures**
Call Identifier: **H2020-SC1-FA-DTS-2018-2020**

Focus Area: **Boosting the effectiveness of the Security Union**
Topic**: Toolkit for assessing and reducing cyber risks in hospitals and care centres**
Topic Identifier: **H2020-SC1-U-TDS-02-2018**

Funding Scheme: **Research and Innovation Action**

Start date of project: 01/12/2018 Duration: 36 months

Deliverable:

Report on Cloud Computing Testbed

Due date of deliverable: 31/03/2020 Actual submission date: 30/03/2020

WPL: UOW

Dissemination Level: Public

Version: 1.0

1 Table of Contents

2 List of Figures and Tables

Figures

Tables

3 Status, Change History and Glossary

Status:	Name:	Date:	Signature:
Draft:	James DesLauriers	28/03/2020	James DesLauriers
Reviewed:	Antonis Michalas	30/03/2020	Antonis Michalas
Approved:	Tamas Kiss	30/03/2020	Tamas Kiss

Table 1: Status Change History

Version	Date	Pages	Author	Modification
v0.1	16.03.2020	all	G. Pierantoni	Skeleton
V0.2 – V0.5	25.03.2020	all	J. DesLauries	Editing input, writing content.
V0.6	29.03.2020	all	T. Kiss	Introduction, conclusion, review and updates.
1.0	30.03.2020	all	T.Kiss	Corrections after review

Table 2: Deliverable Change History

Glossary

ADT	Application Description Template
ASCLEPIOS	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare
API	Application Programming Interface
AWS	Amazon Web Services
DB	Database
EC2	Elastic Compute Cloud
GPU	Graphical Processing Unit
SGX	Intel Software Guard Extensions
TOSCA	Topology and Orchestration Specification for Cloud Applications
VM	Virtual Machine

Table 3: Glossary

4 Introduction

4.1 Scope of the Deliverable

The vision of the ASCLEPIOS project is to maximize and fortify the trust of users to cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. ASCLEPIOS is addressing these limitations by utilizing several modern cryptographic approaches to build a cloud-based eHealth framework that protects users' privacy and prevents both internal and external attacks. ASCLEPIOS also offers the ability to users to verify the integrity of their medical devices prior to using them while at the same time receiving certain guarantees about the trustworthiness of their cloud service provider. Furthermore, ASCLEPIOS offers a novel solution through which healthcare practitioners and medical researchers are able to calculate statistics on medical data in a privacy-preserving way.

To showcase these results, the project implements three real-life near production quality demonstrators provided by ASCLEPIOS healthcare partners. These demonstrators will be deployed in a heterogeneous cloud computing testbed and will illustrate how healthcare applications representing different application areas and user scenarios can take advantage of the secure ASCLEPIOS framework and its services. The role of Work Package 6 (WP6) in the project is to provide this cloud testbed and to develop and deploy the three ASCLEPIOS demonstrators.

The first step in this process is the creation of the cloud testbed that provides a suitable basis for the further demonstrator development work.During the design and setup of this testbed, various requirements and principles have been considered. First, the specific technical requirements of the demonstrator applications have been collected in order to assure that the provided cloud resources are suitable for serving their needs. Second, a heterogeneous cloud testbed has been designed and set up to assure that the developed solutions are agnostic to the underlying cloud infrastructure and can be deployed in a large variety of private and public cloud resources. The current testbed incorporates resources for the University of Westminster and NSE private clouds, and also from two leading international cloud providers, Amazon AWS and Microsoft Azure. Finally, the aim is to automate the deployment and run-time management of the applications in the created testbed and to provide portability between different clouds where it is possible. In order to achieve this objective, the demonstrators will be deployed in a cloud-native microservices-based infrastructure that is managed by the MiCADO (Microservices-based Cloud Application-level Dynamic Orchestrator) framework.

This deliverable describes the above listed three aspects of the ASCLEIPOS cloud computing testbed and explains how this testbed has been established.

4.2 Relationship with other Deliverables, Tasks and Work Packages

Deliverable D6.1 is part of WP6 – Demonstrators and Performance Evaluation and it is the outcome of Task 6.1 - Cloud Computing Testbed. This work package has four deliverables. D6.1 describes the creation and setup of the ASCLEPIOS cloud computing testbed, while the other three deliverables (outcomes of Tasks 6.2 - 6.4) will detail the deployment and operation of the demonstrators in this testbed. The cloud testbed is a fundamental requirement for the upcoming work within the work package and assures that the demonstrators have a suitable environment where these can be further developed and deployed.

Additionally, the testbed is relevant to the technical work packages (WP2-WP4) as the security services and components will also be deployed in this testbed as part of the demonstrators. Finally, it is also important for WP5 – Platform Integration and Finalization, as the testbed will host the final integrated ASCLEPIOS platform and will play a crucial role in its overall evaluation.

5 Description of the User Requirements towards the Cloud Testbed

5.3 Methodology of User Requirements Gathering

Technical requirements were collected from the three application demonstrators to ensure that an appropriate set of cloud resources were chosen for the ASCLEPIOS testbed. The technical requirements collected are four-fold: the software, compute, storage and networking specifications of each application. A collection form covering these four broad categories was circulated as a Google Form and as a free-entry Microsoft Excel Sheet to the use-case partners. The raw collected data (edited for clarity) can be seen in Figures 1-4 in the subsections below.

5.4 Testbed User Requirements

5.4.1 *Software Requirements*

Software Requirements					
Partner	**Demonstrator Name**	**Operating System Support**	**Application Language**	**External Dependencies**	**Licence Dependencies**
NSE	**Privacy-Preserving monitoring and benchmarking of antibiotics prescriptions**	Linux Windows MacOS	Java	MySQL DB, Openfire server, Play framework, web server (NGINX or Apache), misc. libraries	Open source / free software
AMC	**Acute stroke response & care**	Linux Windows MacOS	Python	None	None
CBMI & Charité	**Collaboration and analysis platform for inpatient and outpatient sleep medicine**	Linux	Java	Tomcat, PostgreSQL, NGINX, runtime environment for the pipelines	Open source licenses

Figure 1, User Requirements - Software

5.4.2 *Compute Requirements*

Compute Requirements					
Partner	**Nodes (virtual machine) required**	**CPU required for nodes**	**GPU support for nodes**	**RAM required for each node**	**Notes**
NSE	4	2.3GHz dual core	No	8GB	
AMC	1	Not known yet	1 GPU (not immediately required - see note)	16GB +	We intend to add a privacy analytics component for which we will need some computation power (GPU)
CBMI & Charité	2	Application container: 1 dedicated core; Pipeline container: at least 1 dedicated core; NGINX and Postgres can share resources	No	Postgres 2 GB; Tomcat 2GB; NGINX 2GB; pipeline container 2 GB	

Figure 2, User Requirements - Compute

5.4.3 *Storage Requirements*

Storage Requirements			
Partner	**Storage hosted alongside the application**	**How much storage is required per node?**	**Notes**
NSE	Databases or object/block storage should be hosted alongside the application	256GB	Smaller than the specified storage can still work fine.
AMC	Databases or object/block storage should be hosted alongside the application	~512 GB	Our Demonstrator is evolving into a complex system with privacy analytics, logs analysis etc. As we just started the web application itself, we do not have the storage requirements for the other components.
CBMI & Charité	At least 20 GB are required for storage of bio-signals: could be internal or external	Min. 4 GB for storage of one dataset & results + Matlab runtime environment (~2 GB)	

Figure 3, User Requirements - Storage

5.4.4 *Networking Requirements*

Networking Requirements	
Partner	**Additional Info**
NSE	In practice, as the nodes are connected through a Norwegian health network, it introduces restrictions on the communication between the nodes. Limited set of ports are opened on the nodes and all communication can only be initiated within a node. However, such limitations can be ignored for testing and prototyping.
AMC	N/A
CBMI & Charité	N/A

Figure 4, User Requirements - Networking

6 Description of the Cloud Computing Testbed

The aim of the ASCLEPIOS cloud computing testbed is to provide the necessary hosting and execution environment in order to support the development, deployment and benchmarking of the ASCLEPIOS demonstrators. The testbed will contain include three main building blocks:

- **Cloud deployments:** This represents the core cloud infrastructure that will be hosting the applicatons. To demonstrate the cloud independent nature and wide applicability of the ASCLEPIOS security solutions and the demonstrators, the cloud deployments will include both private (OpenStack) and public (AWS ans Azure) cloud resources.
- **MiCADO - automated deployment and autoscaling tool:** To facilitate the convenient deployment and portability of the demonstrators between multiple clouds, and to provide a cloud environment that is self-adaptive and automatically scales based on user defined policies, the MiCADO[1] framework is utilised in the testbed.
- **ASCLEPIOS services:** The testbed will also incorporate the various ASCLEPIOS security solutions and services that will support the demonstrators. However, as these services are not yet available, the first version of the testbed does not include such services. These components will be gradually integrated into the testbed and utilised by the demonstrators.

The high-level architecture of the ASCLEPIOS cloud computing testbed is shown in Figure 5. The next sections describe the first two components of the ASCLEPIOS Cloud Computing Testbed. The various ASCLEPIOS services are described in the deliverables of the technical work packages (WP2-WP4) and their integration into the testbed and utilization by the demonstrators will be covered in deliverables D6.3 and D6.4.

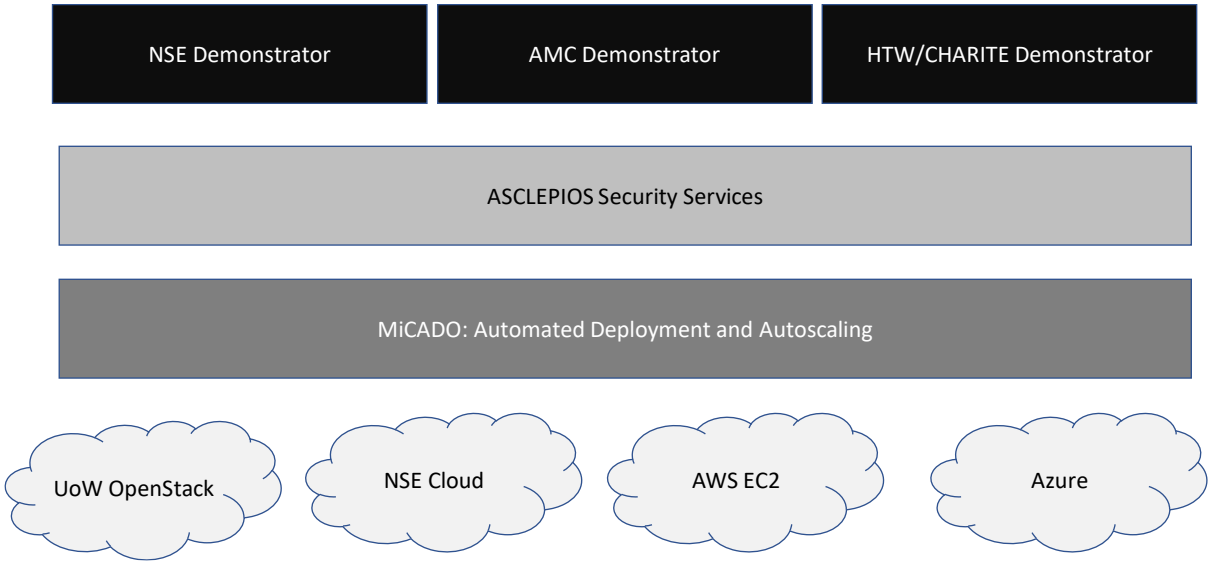

Figure 5, ASCLEPIOS Cloud Computing Testbed & Demonstrators

6.1 Cloud Deployments

The current cloud testbed incorporates resources from four cloud providers. There are resources offered from private clouds, as in healthcare setting, more secure private cloud computing offerings have specific importance. These private cloud resources are coming for the UoW OpenStack cloud and the NSE private cloud. Additionally, the testbed incorporates resources from two leading public cloud providers, Amazon AWS and Microsoft Azure. These

[1] https://micado-scale.eu/

two providers offer cutting edge solutions (e.g. trusted execution environments) that are crucial for prototyping some aspects of the results.

6.1.1 *UoW OpenStack*

The University of Westminster operates an IaaS (Infrastructure-as-a-Service) private cloud computing cluster intended for research use and teaching services provision. The cluster is an OpenStack Juno based infrastructure. The underlying software is based on LibVirt as the virtualising API and KVM as the hypervisor technology. This technology has been proven to be stable for several years and has become one of the virtualisation standards in both industry and the academic sector. The management works with the concept of tenants or projects. Defined by the cloud administrator, each tenant can use a defined number of resources set by the administrator. These resources include a number of CPUs, GB of RAM memory, disk space and Public IPs. Users manage the cloud resources either via EC2 and S3 APIs (Amazon compatible), the Nova API or the Horizon web interface.

Security is based on security groups that isolate the cloud instances (virtual machines running) from each other based on the users and/or projects they belong to. Inside each project, users can also define their own firewall rules and as many security rules as the administrator has allowed for them. Since the OpenStack cluster is running on the University's internal network, there are strict firewall rules in place that drop all incoming connections on all ports. This can be configured on a per-instance basis to allow external connections on certain ports, for example, to provide SSH access or access to the MiCADO Dashboard.

Computer force is based on 28 Dell C6105 doing a total of:

- 248 CPUs (AMD Opteron 4122 Processor (2.2GHz, 4C, 4x512K L2/6M L3 Cache, 75W ACP), DDR3 -1333MHz).
- 2376GB RAM memory (Dual Rank LV RDIMMs 1333MHz)

Storage is based on:

- 5 TB RAID1 based, local storage, 40 x (SATA 7.2k 2.5" HD Hot Plug)
- 12 TB RAID1 based, (PowerVault MD3620i External 10Gb iSCSI + PowerVault MD1220 Base extension)
- Huawei OceanStor 5500 (18 x 550GB SSD + 24 x 3 TB NL-SAS disks), replicated to Huawei OceanStor 5300 (24 x 3 TB NL-SAS disks)

Networking is based on:

- PowerConnect 8024F 10GbE optical fibre switches for VLAN and storage connectivity.
- Standard 100M ethernet switches for administration and live migration purposes.

6.1.1.1 Access to the UoW cloud:

Early access to the UoW cloud resources will be provided to the use cases in the form of pre-provisioned compute nodes of a desired specification. Access to these nodes will be granted via SSH, so the use-case is expected to provide a valid public key to authenticate against. The firewall will be configured on a per-instance basis to allow SSH access from outside the UoW network. Users will be given sudoer privileges so as to have full permissions for deploying and configuring a first test of the application on this cloud.

When MiCADO (see section 6.2) is introduced at the application level, MiCADO will take the role of provisioning and configuration of compute nodes at the infrastructure layer. To do so, MiCADO requires OpenStack credentials of a tenant able to provision resources within the project. The cloud orchestrators can then authenticate with and call the OpenStack API to create, destroy and configure virtual machines. Use-cases will only be given access to the MiCADO API and MiCADO Dashboard, but SSH access could be granted for debugging purposes.

Direct access to the OpenStack Web UI will be restricted to the project members at UoW responsible for provisioning and configuring the above cloud compute nodes for the use cases.

6.1.2 *NSE Cloud*

The Norwegian Center for E-health Research (NSE) operates a private cloud. The NSE has opted to keep the technical details of their cloud stack private. Access to the NSE cloud platform and its resources will be restricted to internal users of NSE only. As a result, this portion of the ASCLEPIOS cloud testbed will act as a secondary or tertiary resource for running the NSE application demonstrator only.

6.1.2.1 Access to the NSE cloud

As mentioned above, this cloud will remain restricted. Access to APIs, web interfaces and VMs will only be possible by the use-case partners at NSE.

6.1.3 *AWS EC2*

The University of Westminster holds a provision on Amazon Web Services (AWS), which is available to the ASCLEPIOS project. AWS operates a large number of public cloud services ranging from traditional cloud offerings such as compute and storage, to support for more recent workloads such as machine learning and IoT. The Elastic Compute Cloud (EC2) service is the main IaaS offering from AWS and supports provisioning CPU and GPU instances of various Linux flavours and sizes. The hypervisor varies depending on the instance family, but these are generally customisations based on KVM. Storage is offered by the S3 (object storage) and EBS (block storage) services, which are both well integrated with EC2. The S3 and EC2 APIs are extensively documented and extensively used. The EC2 service is an extremely popular choice in public clouds but can also be found underpinning private clouds such as OpenNebula and offering compatibility with open projects such as OpenStack.

Aside from the compute and storage services in AWS, ASCLEPIOS is also interested in Nitro Enclaves - hardware enclaves currently in a very early preview state which offer a TEE (trusted execution environment) or secure computing environment. Technical partners have a greater interest in enclaves than do the use-case partners of WP6. The ASCLEPIOS project is currently under consideration to gain access to some of these resources before a larger public preview.

Interacting with AWS EC2 is done via CloudFormation templates (proprietary Infrastructure-as-Code), the EC2 APIs, or the web interface. Both cloud orchestrators in MiCADO support AWS and they require access key and secret key credentials from a programmatic user defined in the AWS Identity & Access Management service.

6.1.3.1 Access to the EC2 cloud:

Use-case access to EC2 will primarily be through a single MiCADO Master machine. Use-cases will have access to the MiCADO API to deploy their applications and to the MiCADO Dashboard to monitor them. For special cases, bare Linux VMs could be provisioned, and access granted to the use-cases via SSH. Full user access to AWS is currently restricted to project members managing the testbed at UoW.

6.1.4 *Azure*

The University of Tampere is managing an Azure account – the public cloud offering from Microsoft. The Azure IaaS stack uses the Azure Hypervisor, which is based on Microsoft Hyper-V. Many different services exist under the Azure umbrella but of special interest to ASCLEPIOS are Windows virtual machines and SGX-enabled Linux instances. Windows virtual machines will be supported in MiCADO for those use-cases that offer Windows compatibility. SGX (*) is a form of hardware enclave from Intel acting as a TEE. Again, these SGX enclaves are important for technical partners outside of WP6.2.

Deploying cloud resources in Microsoft Azure can be done through the Azure web platform, with infrastructure-as-code in the form of ARM (Azure Resource Manager) templates, or via an API. Authenticating MiCADO with Azure will be done by assigning subscription-level privileges to an MSI (Managed System Identity) attached to the MiCADO Master virtual machine.

6.1.4.1 Access to the Azure cloud:

If use-case access to Azure is necessary, it will be through a pre-deployed MiCADO Master virtual machine. Azure Windows VM support is currently being added to MiCADO. Research is ongoing to determine whether generic support for running code in SGX can be added to MiCADO. Use-cases will have access to the MiCADO API to deploy their applications, and to the MiCADO Dashboard to monitor them. For special cases for testing SGX, bare SGX-enabled Linux VMs can be provisioned, and access will be granted to technical partners or the use-cases via SSH. Full user access to AWS is currently restricted to project members researching SGX-enabled instances at UoW and the University of Tampere.

6.2 MiCADO

MiCADO (Microservice-based Cloud Application-level Dynamic Orchestrator) is an orchestration framework for automated deployment and scalability of cloud applications, which was developed during the H2020 Project COLA[2]. The microservices architecture of MiCADO can be seen in Figure 6. MiCADO integrates widely used existing open source technologies, such as Kubernetes for managing containers (Container Orchestrator), Occopus and Terraform for deploying virtual machines (VMs) (Cloud Orchestrator), and Prometheus for monitoring the behaviour of the managed applications (Monitoring System). Additionally, COLA developed a custom MiCADO Submitter that receives and interprets a TOSCA-based[3] input configuration file, describing the application topology and the desired run-time management (auto-scaling and security) policies, a Policy Keeper that interprets these policies and enables the realisation of complex scaling rules, and an Execution Optimiser that uses machine learning based optimisation for autoscaling. MiCADO is an open-source but also a commercial product marketed by German company CloudSME[4] (that provides fully managed services on top of the open-source version). It is developed and maintained by the University of Westminster (with support from former COLA project partners).

The role of MiCADO in ASCLEPIOS will be to facilitate the automated deployment of the application demonstrators on the underlying cloud resources and ensure each application is executed alongside the security components of ASCLEPIOS in a portable and reusable way. A MiCADO Application Description Template (ADT) will describe the basic deployment of ASCLEPIOS components in a stable, working environment. This base ADT will then be extended for each of the respective application demonstrators and further extended for the desired cloud resources within the ASCLEPIOS testbed. MiCADO will then take care of the automated deployment of all VMs and containers required for the execution of both ASCLEPIOS components and the application itself, while enforcing the necessary security policies, and managing the execution of the application based on the scaling policies identified.

MiCADO will be customised and further developed based on the requirements collected from users and developers alike.

[2] https://project-cola.eu/
[3] http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html
[4] https://cloudsme.eu/

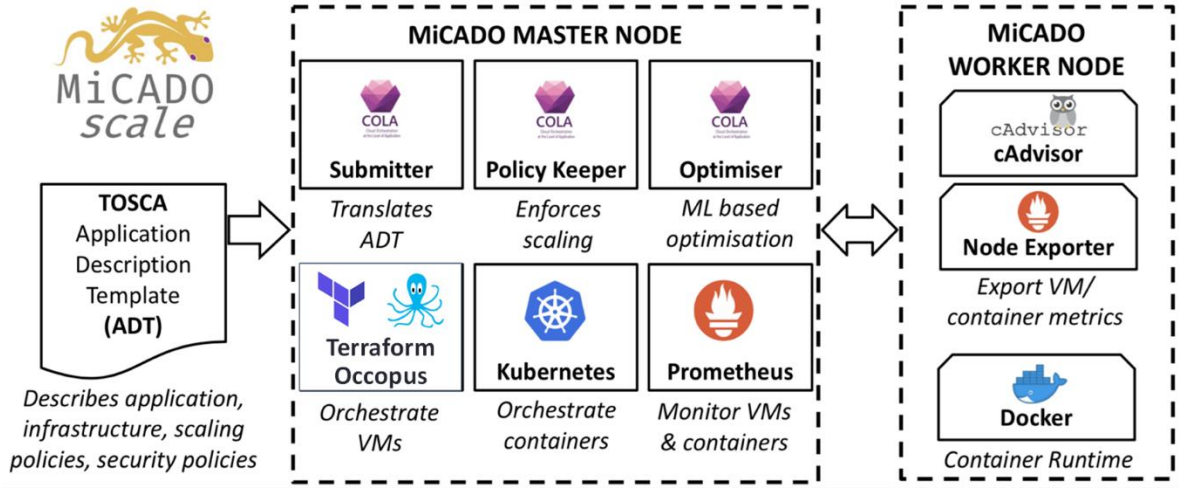

Figure 6, MiCADO Architecture Diagram

6.2.1 *MiCADO Developments to Support ASCLEPIOS (Modifications in M1-M12)*

Several modifications were made to MiCADO in the early months of the ASCLEPIOS project in order to better meet some general requirements of the project and use-case demonstrators. They are summarised below:

I. **Adding support for Terraform to support Windows and SGX VMs in Azure.** Terraform is a popular infrastructure-as-code tool that supports a much greater range of cloud providers and cloud resources than did Occopus – the previous cloud orchestration tool in MiCADO. Adding Terraform support in turn added support for provisioning cloud resources with Microsoft Azure, giving the project enhanced deployment and runtime orchestration of Windows VMs and SGX-enabled hardware.

II. **Making TOSCA ADTs more accessible and user-friendly for new use-cases.** A new approach to the ADT (Application Description Template) repository was developed, which enables metadata searches over previously developed templates for applications in MiCADO. At the same time, the TOSCA (Topology & Orchestration Specification for Cloud Applications) types used inside ADTs were refactored to support greater levels of abstraction. This serves to hide unnecessary complexity from the user at the level of the ADT.

6.2.2 *Planned developments in MiCADO to Support ASCLEPIOS*

Having collected specific technical requirements from the use-cases in M14 and with a better understanding of secure hardware enclaves, the following developments have been planned within MiCADO to support ASCLEPIOS.

I. **Adding support for generic execution of application code in enclaves.** Microsoft Azure supports SGX-enabled instances to provide enclaves for the secure execution of portions of code in isolated hardware. Currently, running a portion of application code in these enclaves requires specific instructions in the source code. This development would allow MiCADO support the deployment and runtime orchestration of both the secure and non-secure portions of code, in and out of the enclave, respectively.

II. **Adding support for running applications on GPU-enabled instances.** The AMC use-case demonstrator requires GPU based computing for performing complex computations in privacy analytics. This development will support running containerised applications in MiCADO so they may use GPUs.

6.3 Docker Container Registry

The feature set of MiCADO is much richer when orchestrating containers as opposed to simply virtual machines. Containers offer lightweight virtualisation for packaging and shipping software and are fast becoming standard in software engineering. MiCADO currently supports Docker[5] containers built from Docker container images, which can be stored in public or private Docker registries. MiCADO supports public registries such as the official public DockerHub, as well as private registries, which can be self-hosted, managed by a cloud provider, or subscribed to on the private DockerHub.

For open-source projects, the public DockerHub is usually sufficient, however, a private registry can be useful during the development phase. When working from within a private cloud with strict firewall rules, an internally hosted private registry can also be very beneficial for ease of access to container images. MiCADO and the ASCLEPIOS testbed are able to support both the official public and private DockerHub, and resources have been set aside within the testbed to self-host a private registry within the University of Westminster cloud on an as-needed basis.

[5] https://docker.com

7 Analysis of the adequacy of the testbed

7.1 MiCADO as a tool for deployment and runtime orchestration

To demonstrate the utility and efficacy of the security components and services that are developed as part of the ASCLEPIOS project, it is necessary to deploy them alongside a set of inherently different healthcare application demonstrators, and across multiple cloud service provider platforms. The MiCADO platform greatly facilitates this, by providing an abstraction layer on top of the testbed cloud infrastructure and by automating the deployment and runtime orchestration of each application demonstrator alongside an appropriate set of ASCLEPIOS services.

The ADT (Application Description Template) used to describe applications for MiCADO is TOSCA-based. TOSCA is an OASIS Standard for describing cloud applications which pays special attention to ensuring both portability across cloud platforms, and reusability of previous templates. The various components of an application's deployment can be described individually: each healthcare application demonstrator, the set of ASCLEPIOS security services and the compute and storage infrastructure in the ASCLEPIOS testbed. Additionally, policies describing the security, scalability and non-functional requirements of each application, ASCLEPIOS service or cloud platform can be defined to govern aspects of the deployed application at runtime.

These individual descriptions can be assembled into different ADTs, each describing the complete application infrastructure for one of the healthcare demonstrators – that is, the application proper, the bespoke set of ASCLEPIOS services for that application, the specific testbed resources from the chosen cloud service provider, and the desired set of policies for the deployment. On submission of the completed ADT, MiCADO will automatically provision the elected cloud resources, deploy the application and security components, and enforce the necessary set of policies.

An ADT can be modified to elect a different cloud service provider from within the testbed or extended to add new ASCLEPIOS services as they are developed. This approach enables simpler testing across platforms, facilitates staggered development of the various ASCLEPIOS components and encourages consistency between the different healthcare application demonstrators.

MiCADO is an open-source tool developed and maintained by the University of Westminster and other partners from the H2020 Project COLA (completed September 2019). Given that UoW is actively maintaining MiCADO, developments to support any aspect of ASCLEPIOS, be it a user requirement or developer request, are possible with a low lead time, making MiCADO an incredibly flexible choice for the project.

7.2 Selection of Cloud Service Providers

The ASCLEPIOS testbed is formed of four different clouds in an aim to provide a good cross-section of the available offerings on the market today. Both private (UoW & NSE) and public (AWS & Azure) clouds are considered, and all enjoy some measure of popularity and widespread use in the cloud communities. Both OpenStack and EC2 underlie a multitude of private and smaller commercial clouds, and their APIs and interfaces are fast becoming standard in the industry.

The UoW OpenStack cloud is a private cloud hosted on-premise at the University of Westminster and will serve as the primary cloud resource within the ASCLEPIOS testbed. It

is administrated by UoW staff and operated by UoW partners from WP6, and being on-premise, has no on-demand pricing associated with it, making it the most flexible resource within the testbed. A strict deep packet inspection firewall at the University offers very high levels of security, though sometimes to the detriment of network speed, and connectivity with external services and endpoints.

The AWS EC2 cloud offers a high network throughput and open connectivity with external services, making it an excellent resource for best scenario benchmarking and demonstrations of ASCLEPIOS services alongside each healthcare demonstrator. EC2 also offers a greater range of compute instances and storage solutions than does the UoW cloud, including access to GPU-powered instances which will be a requirement for at least one of the demonstrators.

Microsoft Azure offers several Windows environments for those application demonstrators whose code supports it and will act as the primary space for testing those applications alongside the developed ASCLEPIOS services. Additionally, Microsoft Azure is, at the time of writing, the only major cloud provider offering hardware-based security enclaves to act as trusted execution environments for sensitive code. This comes in the form of Intel SGX (Software Guard Extensions) and allows for the execution of sections of code in a specific, secure space in memory. SGX-enabled instances, and secure enclaves in general, are of interest to the ASCLEPIOS service developers and Azure provides access to them for testing over the course of the project.

The NSE cloud is a private cloud that forms part of the ASCLEPIOS testbed solely to support the NSE Antibiotics healthcare demonstrator. As the demonstrator requires a connection to physician offices, security and privacy at the infrastructure level are of the highest importance. The NSE cloud is administered and operated by NSE, offering complete control over the security of resources running within it and making it the best option for running this particular demonstrator.

Each of the four cloud platforms that make up the ASCLEPIOS test bed have their own advantages and together they are well suited to supporting the specific user requirements of the three healthcare demonstrators, as well as needs of the ASCLEPIOS service developers.

8 Conclusion and Future Work

This deliverable summarised the creation of the ASCLEPIOS cloud computing testbed. This testbed is crucial for the development, deployment and benchmarking of the ASCLEPIOS demonstrators and to showcase how the technical solutions developed in the project can be utilised in realistic user scenarios. The testbed has now been established and fully operational, fulfilling the requirements of milestone MS14 – Fully operational cloud computing testbed.

When creating the testbed, technical requirements of the ASCLEPIOS demonstrators were collected first, followed by the selection and definition of cloud computing resources and the scalable microservices-based deployment and run-time management framework (MiCADO).

As the testbed is now fully operational, future work is two-folded. First, the operation of the testbed will be assured by continuous maintenance and user support. Second, components of the testbed will be further developed and extended based on the specific requirements of the demonstrator applications. Most specifically, UoW will work on further developing the MiCADO framework in order to fully support the automated deployment, autoscaling and portability of the ASCLEPIOS demonstrators.

9 Appendix A – Technical Cloud Specifications

UoW Cloud	
General Configuration	
Description	**Private OpenStack cloud at University of Westminster**
Hypervisor	**KVM**
IaaS Service	**OpenStack Juno**
Monitoring	**none**
Access Methods	**Nova API, Web Interface, EC2/S3 (Amazon compatible)**
Connectivity	**Strict - deep packet inspection firewall**
Cloud-Interface	
Provisioning	**Web UI, MiCADO, Nova API**
Cloud Integration	**cloud-init, OpenStack HEAT, EC2**
Networking	**Web Console, API**
MiCADO Integration	**Integrated**
Storage	
Interfaces	**Swift (object), Cinder (block)**
Image Format	**QCOW2, RAW**
SSD Capacity	**-**
HDD Capacity	**2000GB**
Quota	**None**
Compute	
CPU (GHz/core)	**160 CPUs**
CPU Quota	**100 CPUs**
RAM (GB/VM)	**62.9GB**
RAM Quota	**100GB**
VM Quota	**50**
Linux Provision Time	**Slow (3min+)**
Win. Provision Time	**-**
Networking	
Internal bandwidth	**20GB per VM**
External bandwidth	**20GB per VM**
Inter-VM latency	**1ms**

NSE Cloud	
Description	**Private cloud at Norwegian Center for e-Health Research**

AWS Cloud	
General Configuration	
Description	**Public Amazon Web Services cloud**
Hypervisor	**Based on KVM**
IaaS Service	**Elastic Compute Cloud**
Monitoring	**CloudWatch**
Access Methods	**EC2/S3 API, Web Interface**
Connectivity	**Open, fully customisable**
Cloud-Interface	
Provisioning	**Web UI, MiCADO, EC2 API**
Cloud Integration	**cloud-init, OpenStack HEAT, EC2**
Networking	**Web Console, API**
MiCADO Integration	**Integrated**
Storage	
Interfaces	**S3 (object), EBS (block)**
Image Format	**AMI, OVA, VHD, VMDX, RAW**
SSD Capacity	**16TB**
HDD Capacity	**16TB**
Quota	**None known**
Compute	
CPU (GHz/core)	**-**
CPU Quota	**None known**
RAM (GB/VM)	**-**
RAM Quota	**None known**
VM Quota	**None known**
Linux Provision Time	**Fast (30secs)**
Win. Provision Time	**-**
Networking	
Internal bandwidth	**-**
External bandwidth	**-**
Inter-VM latency	**1ms**

Azure Cloud	
General Configuration	
Description	**Public Microsoft Azure cloud**
Hypervisor	**Based on Hyper-V**
IaaS Service	**Azure IaaS**
Monitoring	**Azure Monitor**
Access Methods	**Azure API, Azure platform Interface**
Connectivity	**Open, fully customisable**
Cloud-Interface	
Provisioning	**Web UI, MiCADO, Azure API**
Cloud Integration	**cloud-init, Microsoft ARM**
Networking	**Web Console, API**
MiCADO Integration	**Integrated**
Storage	
Interfaces	**(object), Azure Disk Storage (block)**
Image Format	**VHD, VMDX**
SSD Capacity	**64TiB**
HDD Capacity	**32TiB**
Quota	**None**
Compute	
CPU (GHz/core)	**-**
CPU Quota	**None known**
RAM (GB/VM)	**-**
RAM Quota	**None known**
VM Quota	**10**
Linux Provision Time	**Medium (90 secs)**
Win. Provision Time	**Medium (90 secs)**
Networking	
Internal bandwidth	**-**
External bandwidth	**-**
Inter-VM latency	**1ms**