Project Acronym:	**OPTIMIS**
Project Title:	**Optimized Infrastructure Services**
Project Number:	**257115**
Instrument:	**Integrated Project**
Thematic Priority:	**ICT-2009.1.2 – Internet of Services, Software and Virtualisation**

D7.5.1.3 – Final Report on Standardisation Activities

Activity 7: *Business and Legal Activities*

WP 7.5: *Standardization*

Due Date:		M3
Submission Date:		14/06/2013
Start Date of Project:		01/06/2010
Duration of Project:		36 months
Organisation Responsible for the Deliverable:		British Telecom (BT)
Version:		1.0
Status		Final
Author(s):	Pramod Pawar Theo Dimitrakos	BT BT
Reviewer(s)	Karim Djemame Raj Muttukrishnan	University of Leeds City University London

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group specified by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	27/05/2013	Y3 updates	Theo Dimitrakos (BT)
0.2	09/06/2013	Y3 revisions based on input from partners	Theo Dimitrakos (BT)
0.3	06/06/2013	Version sent to reviewers	Karim Djemame (ULEEDS) and Raj Muttukrishnan (CITY)
0.4	13/06/2012	Update addressing comments from reviewers	Theo Dimitrakos (BT)
1.0	14/06/2013	Final version to submit	Ricardo Castaños (ATOS)

Table of Contents

EXECUTIVE SUMMARY **5**

1 INTRODUCTION **6**

1.1 Purpose 6
1.2 Glossary of Acronyms 6

2 SUMMARY OF EXISTING AND UNDER DEVELOPMENT STANDARDS **7**

2.1 WS-Agreement Negotiation 7
2.2 Simple API for Grid Applications (SAGA) 7
2.3 Open Cloud Computing Infrastructure (OCCI) 8
2.4 Open Virtualization Format (OVF) 9
2.5 Portable Operating System Interface (POSIX) 10
2.6 X.509 11
2.7 WS-Agreement 11
2.8 WS-* Standards 12
2.9 ENISA (European Network and Information Security Agency) 12
2.10 Cloud Security Alliance – Governance Risk and Compliance (GRC) stack 13
2.11 Open Grid Forum (OGF) 14
2.12 Distributed Management Task Force (DMTF) 15
2.13 Internet Engineering Task Force (IETF) 16
2.14 International Telecommunication Union 17
2.15 World Wide Web Consortium (W3C) 17
2.16 Information Security Forum – Information Risk Analysis Methodology (IRAM) 18
2.17 European Telecommunication Standards Institute (ETSI) – Cloud Standards Coordination (CSC) taskforce 18

3 EXISTING STANDARDS USED IN OPTIMIS **20**

3.1 Table of Standards 20
SLA negotiation, agreement factory 20
Core function of risk assessment 20
SP,IP Risk Assessment Tool 20
Core function of risk assessment 20
3.2 Standards and best-practices being Investigated / Monitored 22
3.2.1 Input to Cloud Standards roadmap and coordination by ETSI 23
3.2.2 Governance Risk and Compliance stack by Cloud Security Alliance 23
3.2.3 Input to ENISA expert group on European Cyber Security strategy for Cloud and Internet-based services 23
3.2.4 Other incubating standards that are being monitored 23

4 ACTIVITY OF MEMBERS IN VARIOUS STANDARDS **25**

4.1 WP2.2, WP3.4 25
4.2 WP5.4, WP6.2, WP 6.3, WP6.4 and Wp7.5 25
4.3 WP5.2 25

5 CONCLUSION **26**

6 REFERENCES **27**

APPENDIX A LICENSE CONDITIONS. **28**

Index of Tables

Table 1. Overview of the GRC stack by CSA 14

Table 2. Overview of the CSC task-force in ETSI 19

Table 3. Existing Standards Used in OPTIMIS 22

Executive Summary

Various standards are being used throughout the OPTIMIS work packages that shows the awareness of standardization and awareness of existence of various standards amongst the OPTIMIS partners. As the standards are being followed across all the work packages, usability of the standards makes the technology being developed across the work packages more acceptable in the industry. OPTIMIS partners are also involved and contributing to develop standards outside the scope of the OPTIMIS, which brings in the up to date knowledge for development of stable clouds. All the WP leaders have been contacted to get the input on standards being used in their WPs and to know the activity of their WP or WP partners in other standardization bodies.

Because of the ongoing development in the project, the list of standards being followed within project has been a living document that evolved as the project progresses. Some standards monitored by OPTIMIS partners have been incorporated in OPTIMIS. In other cases, OPTIMIS has made contributions to use-case definitions, guidance or incubating standards.

Furthermore, OPTIMIS has made contributions to open source reference implementations of Cloud infrastructures. Detail on such contribution is provided in separate deliverables on interoperability and therefore falls beyond the scope of this report.

1 Introduction

This deliverable documents the summary of existing standards. It mentions the areas within OPTIMIS toolkit that have been using standardization or have intension to do so and does the mapping with the existing standards. The WP has gathered the information on activity of OPTIMIS members in the existing and developing standards.

1.1 Purpose

The purposes of this deliverable of standardization are as follows:

- Identify the parts of the OPTIMIS toolkit, which could use existing standards in Overall Architecture Design.
- Documentation on understanding of the existing standards and their mappings to the work packages.
- Raise an alarm where usability of existing standards in the parts of OPTIMIS toolkit is questionable.
- Identify activities of members in different standardization bodies and contributions to various standards.

1.2 Glossary of Acronyms

Acronym	Definition
BLO	Business-Level Objective
D	Deliverable
DRS	Document Review Sheet
EC	European Commission
EMOTIVE	Elastic Management Of Tasks In Virtualized Environments
IP	Infrastructure Provider
PM	Project Manager
PO	Project Officer
QoS	Quality of Service
SLA	Service Level Agreement
SLO	Service Level Objective
SP	Service Provider
TREC	Trust, Risk, Energy, Cost
VM	Virtual Machine
WP	Work Package

2 Summary of Existing and under Development Standards

As can be seen in the table in Section 6.1 a number of standards or standards under development from different standards bodies are used in OPTIMIS. This section gives an overview on standards and standards bodies.

2.1 WS-Agreement Negotiation

WS-Agreement Negotiation is a proposed recommendation of the Grid Resource Allocation Agreement Protocol working group (GRAAP-WG [8] of the Open Grid Forum [7].

WS-Agreement Negotiation defines the Web Services Agreement Negotiation Specification (WS-Agreement Negotiation), a Web Services protocol for negotiating a valid agreement offer between two parties, such as between a service provider and consumer. A valid agreement offer may then be input to create an agreement using WS-Agreement (specified in the Open Grid Forum document GFD.192 [9]). WS-Agreement Negotiation can also be used to renegotiate an existing agreement that needs to be modified. Thus, WS-Agreement Negotiation provides an additional layer when creating agreements with WS-Agreement. WS-Agreement Negotiation provides an additional layer when creating agreements with WS-Agreement is using an extensible XML language for specifying the nature of the agreement offers, and agreement templates to facilitate discovery of compatible agreement parties and ease the process of creating valid agreement offers. Agreement templates conforming to the WS-Agreement specification including a negotiation context and a set of negotiation constraints are used for the negotiation. The specification consists of all schemas required for the negotiation and the necessary port types.

All information for creating, managing and monitoring an agreement, based on a valid negotiated agreement offer is not described in this specification but in the specification of WS-Agreement.

2.2 Simple API for Grid Applications (SAGA)

Simple API for Grid Applications (SAGA) [13] is a proposed recommendation of the Open Grid Forum.

This document specifies SAGA CORE, the Core of the Simple API for Grid

Applications. SAGA is a high-level API that directly addresses the needs of application developers. The purpose of SAGA is two-fold:

1. Provide a simple API that can be used with much less effort compared to the vanilla interfaces of existing grid middleware. A guiding principle for achieving this simplicity is the 80–20 rule: serve 80 % of the use cases with 20 % of the effort needed for serving 100 % of all possible requirements.
1. Provide a standardized, common interface across various grid middleware systems and their versions.

The SAGA API consists of a core specification that covers all requirements that are considered both urgent and sufficiently well understood to produce an API. Addressing the other the less urgent or well understood requirements is deferred to extensions of the SAGA API. Based upon this reasoning, areas of functionality (from now on referred to as packages) that are included in SAGA API (core) are the following:

- Jobs

- Files (and logical files)
- Streams
- Remote procedure calls
- Auxiliary API's for
  - Session handle and security context
  - Asynchronous method calls (tasks)
  - Access control lists
  - Attributes
  - Monitoring
  - Error handling

Possible SAGA extensions are:

- Steering and extended monitoring
- Possibly combining logical/physical files (read on logical files)
- Persistent information storage
- GridCPR [11]
- Task dependencies (simple work flows and task batches)
- Extensions to existing classes, based on new use cases

2.3 Open Cloud Computing Infrastructure (OCCI)

Open Cloud Computing Infrastructure (OCCI) [14] is a recommendation of the Open Grid Forum.

The Open Cloud Computing Interface is a RESTful [15] Protocol and API for all kinds of management tasks. OCCI was originally initiated to create a remote management API for IaaS model-based services, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling and monitoring. It has since evolved into a flexible API with a strong focus on interoperability while still offering a high degree of extensibility. The current release of the Open Cloud Computing Interface is suitable to serve many other models in addition to IaaS, including e.g. PaaS and SaaS.

In order to be modular and extensible the current OCCI specification is released as a suite of complimentary documents, which together form the complete specification. The documents are divided into three categories consisting of the OCCI Core, the OCCI Renderings and the OCCI Extensions.

- The OCCI Core specification consists of a single document defining the OCCI Core Model. The OCCI Core Model can be interacted with renderings (including associated behaviours) and expanded through extensions.
- The OCCI Rendering specifications consist of multiple documents each describing a particular rendering of the OCCI Core Model. Multiple renderings can interact with the same instance of the OCCI Core Model and will automatically support any additions to the model which follow the extension rules defined in OCCI Core.

- The OCCI Extension specifications consist of multiple documents each describing a particular extension of the OCCI Core Model. The extension documents describe additions to the OCCI Core Model defined within the OCCI specification suite.

The current specification consists of three documents. Future releases of OCCI may include additional rendering and extension specifications. The documents of the current OCCI specification suite are:

OCCI Core describes the formal definition of the OCCI Core Model [14].

OCCI HTTP Rendering defines how to interact with the OCCI Core Model using the RESTful OCCI API. The document defines how the OCCI Core Model can be communicated and thus serialised using the HTTP protocol (not yet published).

OCCI Infrastructure contains the definition of the OCCI Infrastructure extension for the IaaS domain. The document defines additional resource types, their attributes and the actions that can be taken on each resource type [16].

2.4 Open Virtualization Format (OVF)

The Open Virtualization Format (OVF) [11] is a standard defined by the Distributed Management Task Force (DMTF [12].

The Open Virtualization Format (OVF) Specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. The key properties of the format are as follows:

- Optimized for distribution

  OVF supports content verification and integrity checking based on industry-standard public key infrastructure, and it provides a basic scheme for management of software licensing.

- Optimized for a simple, automated user experience

  OVF supports validation of the entire package and each virtual machine or metadata component of the OVF during the installation phases of the virtual machine (VM) lifecycle management process. It also packages with the package relevant user-readable descriptive information that a virtualization platform can use to streamline the installation experience.

- Supports both single VM and multiple-VM configurations

  OVF supports both standard single VM packages and packages containing complex, multi-tier services consisting of multiple interdependent VMs.

- Portable VM packaging

  OVF is virtualization platform neutral, while also enabling platform-specific enhancements to be captured. It supports the full range of virtual hard disk formats used for hypervisors today, and it is extensible, which allow it to accommodate formats that may arise in the future. Virtual machine properties are captured concisely and accurately.

- Vendor and platform independent

  OVF does not rely on the use of a specific host platform, virtualization platform, or guest operating system.

- Extensible

OVF is immediately useful — and extensible. It is designed to be extended as the industry moves forward with virtual appliance technology. It also supports and permits the encoding of vendor-specific metadata to support specific vertical markets.

- Localizable

  OVF supports user-visible descriptions in multiple locales, and it supports localization of the interactive processes during installation of an appliance. This capability allows a single packaged appliance to serve multiple market opportunities.

- Open standard

  OVF has arisen from the collaboration of key vendors in the industry, and it is developed in an accepted industry forum as a future standard for portable virtual machines.

It is not an explicit goal for OVF to be an efficient execution format. A hypervisor is allowed but not required to run software in virtual machines directly out of the Open Virtualization Format.

2.5 Portable Operating System Interface (POSIX)

Portable Operating System Interface (POSIX) [17] is a standard defined by IEEE [18] and Open Group [19].

POSIX defines a standard operating system interface and environment, including a command interpreter (or "shell"), and common utility programs to support applications portability at the source code level. It is intended to be used by both application developers and system implementers.

POSIX comprises four major components (each described in an associated volume in [17]):

- General terms, concepts, and interfaces common to all volumes of POSIX.1-2008, including utility conventions and C-language header definitions, are included in the Base Definitions volume of POSIX.
- Definitions for system service functions and subroutines, language-specific system services for the C programming language, function issues, including portability, error handling, and error recovery, are included in the System Interfaces volume of POSIX.
- Definitions for a standard source code-level interface to command interpretation services (a "shell") and common utility programs for application programs are included in the Shell and Utilities volume of POSIX.
- Extended rationale that did not fit well into the rest of the document structure, containing historical information concerning the contents of POSIX.1-2008 and why features were included or discarded by the standard developers, is included in the Rationale (Informative) volume of POSIX.

The following areas are outside of the scope of POSIX.1-2008:

- Graphics interfaces
- Database management system interfaces
- Record I/O considerations
- Object or binary code portability
- System configuration and resource availability

POSIX describes the external characteristics and facilities that are of importance to application developers, rather than the internal construction techniques employed to achieve these capabilities. Special emphasis is placed on those functions and facilities that are needed in a wide variety of commercial applications.

2.6 X.509

X.509 is a standards developed by the International Telecommunication Union (ITU) [21]. Usually the X.509 profile [20] created by the Internet Engineering Task Force (IETF) [22] is used.

The IETF X.509 specification (RFC 5280) profiles the format and semantics of certificates and certificate revocation lists (CRLs) for the Internet PKI.

The RFC describes procedures for processing of certification paths in the Internet environment. Finally, ASN.1 modules are provided in the appendices for all data structures defined or referenced.

The standard described requirements for Internet Public Key Infrastructure (PKI), presents an architectural model and describes its relationship to previous IETF and ISO/IEC/ITU-T standards.

RFC 5280 describes profiles of the X.509 version 3 certificate, and profiles the X.509 version 2 CRL. The profiles include the identification of ISO/IEC/ITU-T and ANSI extensions that may be useful in the Internet PKI. The profiles are presented in the 1988 Abstract Syntax Notation One (ASN.1) rather than the 1997 ASN.1, syntax used in the most recent ISO/IEC/ITU-T standards.

Other topics described are Certification path validation procedures, which are based upon the ISO/IEC/ITU-T definition.

Procedures for identification and encoding of public key materials and digital signatures are defined in RFC 3279, RFC 4055, and RFC4491.

2.7 WS-Agreement

WS-Agreement is a full recommendation of the Open Grid Forum published as GFD.192 [9].

The Web Services Agreement Specification (WS-Agreement) is a Web Services protocol for establishing agreement between two parties, such as between a service provider and consumer, using an extensible XML language for specifying the nature of the agreement, and agreement templates to facilitate discovery of compatible agreement parties. The specification consists of three parts which may be used in a composable manner: a schema for specifying an agreement, a schema for specifying an agreement template, and a set of port types and operations for managing agreement life-cycle, including creation, expiration, and monitoring of agreement states.

The goal of WS-Agreement is to standardize the terminology, concepts, overall agreement structure with types of agreement terms, agreement template with creation constraints and a set of port types and operations for creation, expiration and monitoring of agreements, including WSDL needed to express the message exchanges and resources needed to express the state.

In a distributed service-oriented computing environment, service consumers like to obtain guarantees related to services they use, often related to quality of a service. Whether service providers can offer – and meet – guarantees usually depends on their resource situation at the requested time of service. Hence, quality of service and other guarantees that depend on actual resource usage cannot simply be advertised as an invariant property of a service and

then bound to by a service consumer. Instead, the service consumer must obtain state-dependent guarantees from the service provider, represented as an agreement on the service and the associated guarantees. Additionally, the guarantees on service quality should be monitored and service consumers may be notified of failure to meet these guarantees. The objective of the WS-Agreement specification is to define a language and a protocol for advertising the capabilities of service providers and creating agreements based on creational offers, and for monitoring agreement compliance at runtime.

An agreement between a service consumer and a service provider specifies one or more service level objectives both as expressions of requirements of the service consumer and assurances by the service provider on the availability of resources and/or on service qualities. For example, an agreement may provide assurances on the bounds of service response time and service availability. Alternatively, it may provide assurances on the availability of minimum resources such as memory, CPU MIPS, storage, etc.

To obtain this assurance on service quality, the service consumer or an entity acting on its behalf must establish a service agreement with the service provider, or another entity acting on behalf of the service provider. Because the service objectives relate to the definition of the service, the service definition must be part of the terms of the agreement or be established prior to agreement creation. This specification provides a schema for defining overall structure for an agreement document. An agreement includes information on the agreement parties and a set of terms. The terms MAY comprise one or more service terms and zero or more guarantee terms specifying service level objectives and business values associated with these objectives.

The agreement creation process typically starts with a pre-defined agreement template specifying customizable aspects of the documents, and rules that must be followed in creating an agreement, which we call agreement creation constraints. This specification defines a schema for an agreement template.

The creation of an agreement can be initiated by the service consumer side or by the service provider side, and the protocol provides hooks enabling such symmetry.

2.8 WS-* Standards

WS-* Standards [23] is a suite of standards for Web-services with SOAP/WSDL developed at the World Wide Web Consortium (W3C) [24].

Most commonly used in OPTIMIS are SOAP, WS-I Basic Profile, WSDL, WS-Addressing, WS-Policy, WS-ReliableMessaging, WS-Security. Detailed description can be found here [23].

2.9 ENISA (European Network and Information Security Agency)

ENISA is the EU's response to cyber security issues of the European Union. ENISA's objective is to create a hub for exchange of information, best practices and knowledge in the field of information security.

Main areas of activity of ENISA are,

Secure Applications and Services: The security of services and applications, ranging from cloud-based services, web applications to smartphones and smartphone apps.
Awareness Raising: Developing and maintaining cooperation models. The AR Community shares emerging good practice and discusses cutting-edge topics and key issues in the information security field.

Computer Emergency Response Team: Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more. They must act as primary security service providers for government and citizens. At the same time, they must act as awareness raisers and educators.

Identity, Privacy and Trust: Identity, Privacy and Trust are the parallel lanes of the road towards communication networks that safeguard the EU society. As society becomes increasingly dependent on information and communication technologies, the parallel lanes of the road towards communication networks safeguard the EU society.

Resilience of public Communication Networks and Services: Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on Internet, disruptions due to physical phenomena, software and hardware failures, and human mistakes all affect the proper functioning of public eCommunications networks. Such disruptions reveal the increased dependency of our society to these networks and their services.

Risk Management: This encompasses a variety of information pertinent to Risk Management and Risk Assessment but it also gives information about activities and events in that area.
Stakeholder Relations: Enables to identify emerging risks, to forge new insights into help Member States and private sector organizations better prepare themselves for challenges in a proactive and increasingly professional manner, and to build novel public and private sector partnerships as necessary.

In 2013 ENISA launched an experts group on Cloud Security and Resilience. The key objectives of this experts group for 2013 are:

- Cloud computing and EU cyber security strategy with core topics focusing on advice on:
  - How to implement incident reporting (as required in the EU strategy)
  - How can regulators best supervise security of Cloud and Internet-based services
  - How to analyse risks from a national perspective.
- Governmental Cloud computing focusing only on the use of cloud by the public sector and in particular the so-called governmental clouds. Core topics include:
  - An overview of existing governmental Cloud infrastructures and services, and
  - Identification of standard implementation approaches providing appropriate guidance on security and resilience.

BT and Atos follow this group and Dr Theo Dimitrakos is one of the experts contributing to the deliverables of the group.

2.10 Cloud Security Alliance – Governance Risk and Compliance (GRC) stack

Cloud Security Alliance (CSA) is the primary global industry forum focusing on Cloud Security with most of the major cloud providers and security vendors being members of CSA.

During the implementation of OPTIMIS, CSA has continued to produce guidance on cloud and virtualisation security as well as developing a certification programme on Cloud Security Knowledge (CCSK - Certificate of Cloud Security Knowledge) [29].

Furthermore, CSA produced the GRC (Governance, Risk and Compliance) stack – a toolkit enabling the assessment of security and security related risk in Cloud environments. The GRC stack includes the following elements [30]:

Stack Pack	Description	Resolves the question	Delivering
Cloud Trust Protocol (CTP)	Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from CSP	How do I know that the controls I need are working for me now (consumer)? How do I provide actual security and transparency of service to all of my cloud users (CSP)?	Continuous monitoring, with a purpose
Cloud Audit	Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments	How do I announce and automate my claims of audit support for all of the various compliance mandates and control obligations?	Claims, offers, and the basis for auditing service delivery
Consensus Assessment Initiative (CAI)	Industry-accepted ways to document what security controls exist	How do I ask about the control requirements that are satisfied (consumer) or express my claim of control response (CSP)?	Pre-audit checklists and questionnaires to inventory controls
Cloud Controls Matrix (CCM)	Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a CSP	What control requirements should I have as a cloud consumer, CSP?	The recommended foundations for controls

Table 1. Overview of the GRC stack by CSA

2.11 Open Grid Forum (OGF)

The Open Grid Forum (OGF) is a community of users, developers, and vendors leading the global standardization effort for grid computing. The OGF community consists of thousands of individuals in industry and research, representing over 400 organizations in more than 50 countries. Together they work to accelerate adoption of grid computing worldwide because they believe grids will lead to new discoveries, new opportunities, and better business practices.

The work of OGF is carried out through community-initiated working groups, which develop standards and specifications in cooperation with other leading standards organizations, software vendors, and users. OGF is funded through its Organizational Members, including technology companies and academic and government research institutions. OGF hosts several events each year to further develop grid-related specifications and use cases and to share best practices.

OGF is an open community committed to driving the rapid evolution and adoption of applied distributed computing. Applied Distributed Computing is critical to developing new, innovative and scalable applications and infrastructures that are essential to productivity in the enterprise and within the science community. OGF accomplishes its work through open forums that build the community, explore trends, share best practices and consolidate these best practices into standards.

The OGF community reflects the near universal interest in and applicability of distributed systems, and includes leaders and practitioners drawn from academia, enterprises, vendors and government organizations. OGF is open to everyone who is willing to participate, to discuss trends, share experiences, solve problems, and develop standards that accelerate the adoption, use and development of applied distributed computing technologies and environments.

Applied distributed computing environments include everything from distributed high performance computing resources (traditional 'Grids') to horizontally scaled transactional systems supporting Service Oriented Architectures to Clouds, across all scales and for all application domains.

Applied distributed computing environments take advantage of many technologies, e.g. virtualization, multi-Core, web services, SOA, etc. OGF will, where necessary, develop expertise in these areas in support of its mission, either through direct activity or through partnerships with other organizations.

By bringing a global community of vendors, researchers, architects and users together within an open forum, business and science requirements can be translated into best practices and, where appropriate, relevant and timely industry standards that enable interoperability and integration within and across organizational boundaries. This process is facilitated by regular meetings, ranging from large multi-track events held several times a year that bring the broad community together in workshops to smaller, more tightly focused group meetings. All OGF activity is underpinned by a web presence that enables communication within the various OGF working groups and the sharing of their work with the broader community.

Some of the well-known standards of OGF with many implementations are the Open Grid Service Architecture (OGSA), Simple API for Grid Applications (SAGA), Job Submission Description Language (JSDL), Distributed Resource Management Application API WG (DRMAA), Web Services Agreement (WS-Agreement).

Despite its name OGF is driving standards in the area of applied distributed computing where Grids are just one facet. OGF has also strong activities in developing standards for Clouds, like e.g. the Open Cloud Computing Interface (OCCI).

2.12 Distributed Management Task Force (DMTF)

DMTF's mission is to create standards that enable interoperable IT management. DMTF members and alliance partners represent all facets of the enterprise and computing sector, from major hardware and software vendors to companies specializing in the development of tools for managing the enterprise system. This widespread collaboration enables open development of standards critical to providing interoperable IT management.

The group spans the industry with 160 member companies and organizations, and more than 4,000 active participants crossing 43 countries. The DMTF board of directors is led by 15 innovative, industry-leading technology companies. They include Advanced Micro Devices

(AMD); Broadcom Corporation; CA, Inc.; Cisco; Citrix Systems, Inc.; EMC; Fujitsu; HP; Huawei; IBM; Intel Corporation; Microsoft Corporation; Oracle; RedHat and VMware, Inc.

With this deep and broad reach, DMTF creates standards that enable interoperable IT management. DMTF management standards are critical to enabling management interoperability among multi-vendor systems, tools and solutions within the enterprise.

Standards become even more crucial with increasing pressure to ensure that technology investments remain viable for years to come. Standards allow forward-thinking CIOs and IT managers to select the products that best suit their needs today–regardless of vendor–while helping to ensure that no proprietary constraints arise when new systems are put in place in the future.

DMTF members collaborate to develop IT management standards that promote multi-vendor interoperability worldwide. Together with a broad range of alliance partners, the group is at the center of the systems-management industry, developing standards that are continually improving the IT management landscape.

DMTF standards primarily serve:

- IT Personnel – DMTF provides increased choice, reduced cost and improved interoperability for heterogeneous IT management infrastructures.
- IT Solutions Vendors – DMTF standards reduce development and design costs by enabling companies to dedicate resources to growing their own business.

Some of the well-known standards of OGF with many implementations are Common Information Model (CIM), Web Services Management (WS-MAN , Open Virtualization Format (OVF).

2.13 Internet Engineering Task Force (IETF)

The goal of the IETF is to make the Internet work better.

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

Structure

The IETF's standards development work is organized into 8 Areas (http://www.ietf.org/iesg/area.html). Each Area has 1 or more Area Directors (ADs), which together comprise the IETF Engineering Steering Group (IESG). The IESG is responsible for technical management of IETF activities, the Internet standards process, and for the actions associated with entry into and movement along the Internet "standards track," including final approval of specifications as Internet Standards and publication as an RFC.

Within each Area there are multiple Working Groups (WG). Each WG has one or more chairs who manage the work, and a written charter defining what the work is and when it is due. There are more than 100 WGs. The WGs produce Internet Drafts (I-Ds) which often lead to the publication of an Internet standard as an RFC. See http://www.ietf.org/wg/ for WG charters and http://datatracker.ietf.org/wg/ for the list of the Areas, the current WGs and their chairs.

People interested in particular technical issues join the mailing list of a WG (http://datatracker.ietf.org/list/wg/) and occasionally attend one or more of the three IETF meetings held every year. See: http://www.ietf.org/meeting/ for meeting details.

Participation

The IETF is completely open to newcomers. There is no formal membership, no membership fee, and nothing to sign. By participating, you do automatically accept the IETF's rules, including the rules about intellectual property (patents, copyrights and trademarks). If you work for a company and the IETF will be part of your job, you must obviously clear this with your manager. However, the IETF will always view you as an individual, and never as a company representative.

2.14 International Telecommunication Union

ITU is the United Nations specialized agency for information and communication technologies – ICTs.

We allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide.

ITU is committed to connecting all the world's people – wherever they live and whatever their means. Through our work, we protect and support everyone's fundamental right to communicate.

Today, ICTs underpin everything we do. They help manage and control emergency services, water supplies, power networks and food distribution chains. They support health care, education, government services, financial markets, transportation systems and environmental management. And they allow people to communicate with colleagues, friends and family anytime, and almost anywhere.

With the help of our membership, ITU brings the benefits of modern communication technologies to people everywhere in an efficient, safe, easy and affordable manner.

ITU membership reads like a Who's Who of the ICT sector. We're unique among UN agencies in having both public and private sector membership. So in addition to our 192 Member States, ITU membership includes ICT regulators, leading academic institutions and some 700 private companies.

In an increasingly interconnected world, ITU is the single global organization embracing all players in this dynamic and fast-growing sector.

2.15 World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.

The following principles guide W3C's work.

- Web for All

  The social value of the Web is that it enables human communication, commerce, and opportunities to share knowledge. One of W3C's primary goals is to make these benefits available to all, whatever their hardware, software, network infrastructure, native language, culture, geographical location, or physical or mental ability.

- Web on Everything

The number of different kinds of devices that can access the Web has grown immensely. Mobile phones, smart phones, personal digital assistants, interactive television systems, voice response systems, kiosks and even certain domestic appliances can all access the Web.

- Vision

  W3C's vision for the Web involves participation, sharing knowledge, and thereby building trust on a global scale.

- Web for Rich Interaction

  The Web was invented as a communications tool intended to allow anyone, anywhere to share information. For many years, the Web was a "read-only" tool for many. Blogs and wikis brought more authors to the Web, and social networking emerged from the flourishing market for content and personalized Web experiences. W3C standards have supported this evolution thanks to strong architecture and design principles.

- Web of Data and Services

  Some people view the Web as a giant repository of linked data while others as a giant set of services that exchange messages. The two views are complementary, and which to use often depends on the application.

- Web of Trust

  The Web has transformed the way we communicate with each other. In doing so, it has also modified the nature of our social relationships. People now "meet on the Web" and carry out commercial and personal relationships, in some cases without ever meeting in person. W3C recognizes that trust is a social phenomenon, but technology design can foster trust and confidence. As more activity moves on-line, it will become even more important to support complex interactions among parties around the globe.

2.16 Information Security Forum – Information Risk Analysis Methodology (IRAM)

IRAM is the ISF's (Information Security Forum) information risk analysis methodology, it is designed to help organizations analyze business information risk and select the right controls to mitigate that risk.
It has been derived from good practice in leading organizations. These organizations network frequently to exchange information on good practice and the continued development of the IRAM approach to information risk analysis (including evolving software tools such as the IRAM Risk Analyst Workbench).
These organizations network frequently to exchange information on good practice and the continued development of the IRAM approach to information risk analysis (including evolving software tools such as the IRAM Risk Analyst Workbench).

2.17 European Telecommunication Standards Institute (ETSI) – Cloud Standards Coordination (CSC) taskforce

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

ETSI is officially recognized by the European Union as a European Standards Organization. ETSI is a not-for-profit organization with more than 700 ETSI member organizations drawn from 62 countries across 5 continents world-wide.

In 2013 ETSI established a Cloud Standards Coordination activity aiming to create a roadmap of existing and emerging standards in cloud computing, address conflicts and highlight need for further standardization

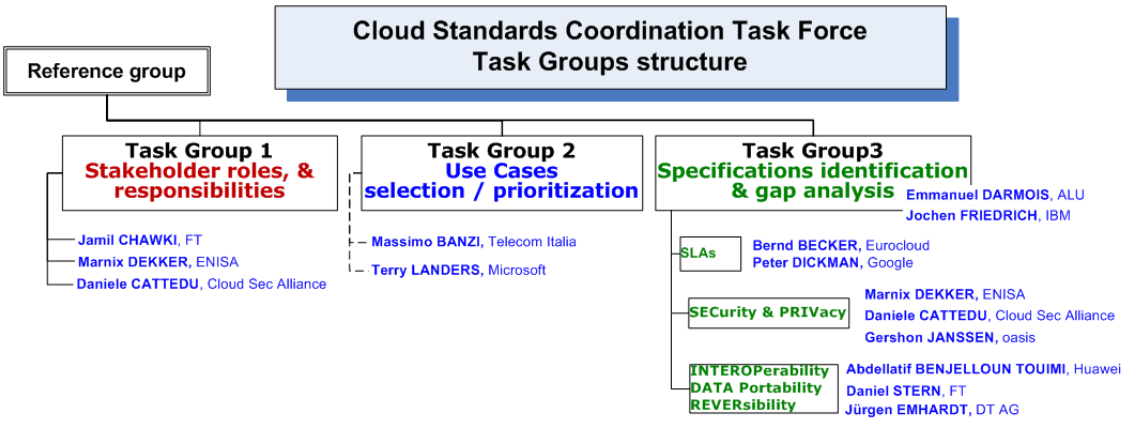

Table 2. Overview of the CSC task-force in ETSI

3 Existing Standards used in OPTIMIS

3.1 Table of Standards

Standards	WP	Component (optional)	Subcomponent (optional)	Relevance of the standard for the component	Standard status
Open Cloud Computing Interface (OCCI)	4.2	VMManager (EMOTIVE)		Interoperability inside OPTIMIS and interoperability of OPTIMIS IPs with other IPs	Existing standard
Open Virtualization Format (OVF)	2.1, 2.2, 3.1, 3.54. 2, 5.3, 5.3	IDE, Programming model Runtime ,Service Manifest, Agreement templates , VMManager, CO, Service Deployment Optimizer, Admission Control, Data Management	SP,IP Risk Assessment Tool	Interoperability inside OPTIMIS (SP and IP) and interoperability of OPTIMIS IPs with other IPs. Information on how the service is formed is specified in OVF format, in the Service Manifest. The manifest is generated by the IDE, and read by the Programming Model Runtime.	Existing standard with some custom extensions
Risk Management Standard(RMS)	3.4, 4.2	Risk Assessment Framework , Risk Assessor	SLA negotiation, agreement factory	Core function of risk assessment	Existing standard
Probabilistic Risk Assessment (PRA)	3.4, 4.3	Risk Assessment Framework , Risk Assessor	SP,IP Risk Assessment Tool	Core function of risk assessment	Existing standard
WS-Agreement	2.2, 5.1	WP2.2: WSAG4J framework WP5.1: SmartLM License Service		Interoperability inside OPTIMIS (SP and IP) and interoperability with other (external) SLA frameworks based on WS-Agreement	Existing standard

WS-Agreement Negotiation	2.2, 5.1	WP2.2: WSAG4J framework WP5.1: SmartLM License Service	SLA creation, agreement factory	Interoperability inside OPTIMIS (SP and IP) and interoperability with other (external) SLA frameworks based on WS-Agreement	Proposed standard with contribution from OPTIMIS partners
Simple API for Grid Applications (SAGA)	2.1	Programming model Runtime		Useful in order to work with different low level middlewares, with the same implementation of the runtime	Existing Standard
WS-* (SOAP, WS-I Basic Profile, WSDL, WS-Addressing, WS-Policy, WS-ReliableMessaging, WS-Security).	2.1, 3.3	Programming model Runtime, Trust Framework		Used for offering the new applications implemented with the programming model as services and invoking other web services required by these applications, interoperability inside OPTIMIS (SP and IP)	Existing Standard
For Certificates, X509 version 3 For Keys, PKCS#8 OPEN CA for Key store	5.4	Inter Cloud Services	VPN Overlay Component	Interoperability with in OPTIMIS	Existing Standard
IRAM, information security forum	5.4, 3.4	Threaten vulnerability tool		Interoperability with in OPTIMIS	Existing Standard
POSIX interfaces	5.2	Data management		For the VMs to be able to connect to the distributed file system and perform read/write operations	Existing Standard

SHA1, AES, SSL, HMAC	5.2	Data Management		Incorporated in the security and authentication management	Existing standard
Jersey implementation of the REST protocol	5.2	Data management		For the service interfaces	Existing Standard
NIST definition of security threats and assets	3.4	Risk Assessment		The security threats and assessment terminology definition of NIST is used in the IP risk assessment work.	Existing Standard
GRC by CSA and PCI DSS 2.0, HIPAA, NIST, SAS 70 and other standards for information assurance	5.4 & 6.4	Inter-Cloud Security and Broker Value-Added Services	Intelligent Protection Secure Cloud Storage	Detailed, auditable reports that document prevented attacks and policy compliance status Storage & Data Encryption and Key Management	Emerging (CSA-GRC) Existing (PCI DSS 2.0, HIPAA, NIST, SAS 70, etc.)

Table 3. Existing Standards Used in OPTIMIS

3.2 Standards and best-practices being Investigated / Monitored

OPTIMIS partners have been examining some more standards that were not directly used in the OPTIMIS components in order to investigate the possibility to incorporate them in future extensions of the OPTIMIS toolkit.

3.2.1 Input to Cloud Standards roadmap and coordination by ETSI

The European Telecommunications Standards Institute (ETSI) created in 2013 a task-force focusing on Cloud Standards Coordination.

OPTIMIS contributed, though the project coordinator Ana Juan Ferrer (Atos), input based on our experience through the Programming Model and Brokerage use-cases (WP6.2 and WP6.4 respectively) which was accepted by the ETSI task force and included in the consolidated report of ETSI on Use-Cases and Stakeholders. This consolidated input and in conjunction with results from other groups that analysed existing standards is now guiding the working parallel working groups on SLA, security and privacy, interoperability and data portability that aim to produce guidance on Cloud standards by July 2013, i.e. after the end of OPTIMIS project. Several OPTIMIS partners (e.g. SCAI, BT, etc.) are continuing to follow this activity via their representatives in the parallel groups of the task-force.

3.2.2 Governance Risk and Compliance stack by Cloud Security Alliance

The Cloud Security Alliance is another organization which will be closely monitored in order to identify opportunities for standardization. Particular attention has been placed on the GRC stack and in particular the CCM – Cloud Control Matrix. This aims to produce objective quantifiable metrics, to assure Information Security maturity in cloud, third party service providers, as well as internally hosted systems. **OPTIMIS partners have been continuously monitoring the development of this collaborative initiative; they have been directly contributing to its predecessor CAMM (Common Assurance Maturity Model) and indirectly to CCM.**

3.2.3 Input to ENISA expert group on European Cyber Security strategy for Cloud and Internet-based services

ENISA facilitates contacts between European institutions, the Member States, and private business and industry actors. **OPTIMIS partners are continuously monitoring ENISA development including OPTMIS members (e.g. Dr Theo Dimitrakos) participating in the ENISA expert group on Cloud Security and Resilience that is producing advice how to implement the European Cyber Security strategy for Cloud and Internet-based Services.**

3.2.4 Other incubating standards that are being monitored

IEEE has started activities on standardisation of Cloud computing aspects [27]. The IEEE Standards Association (IEEE-SA) has formed two new Working Groups (WGs) around IEEE P2301 and IEEE P2302.

IEEE P2301 will provide profiles of existing and in-progress cloud computing standards in critical areas such as application, portability, management, and interoperability interfaces, as well as file formats and operation conventions. With capabilities logically grouped so that it addresses different cloud audiences and personalities, IEEE P2301 will provide an intuitive roadmap for cloud vendors, service providers, and other key stakeholders. When completed, the standard will aid users in procuring, developing, building, and using standards-based cloud computing products and services, enabling better portability, increased commonality, and greater interoperability across the industry.

IEEE P2302 defines essential topology, protocols, functionality, and governance required for reliable cloud-to-cloud interoperability and federation. The standard will help build an economy of scale among cloud product and service providers that remains transparent to

users and applications. With a dynamic infrastructure that supports evolving cloud business models, IEEE P2302 is an ideal platform for fostering growth and improving competitiveness. It will also address fundamental, transparent interoperability and federation much in the way SS7/IN did for the global telephony system, and naming and routing protocols did for the Internet.

DMTF has had two active working Cloud-standards related working groups: Cloud Audit Data Federation Work Group' (CADFT) and Cloud Management working group (CMWG) [28].

Cloud Audit Data Federation Work Group will work to enable providers to increase security capabilities to address customer concerns over cloud provider security, one of the top inhibitors to the adoption of cloud deployment models.

The Cloud Management WG will focus on addressing the management interfaces between the Cloud service consumer/developer and the Cloud service provider. The working group will also address the security mechanisms required to enable interoperability. The CMWG will develop a set of prescriptive specifications that deliver architectural semantics as well as implementation details to achieve interoperable management of Clouds between service requestors/developers and providers.

Finally, the US-based National Institute of Standards and Technology (NIST) has set up a Cloud Computing Standards Roadmap Working Group [26], which worked on a survey of the existing standards landscape for security, portability, and interoperability standards/models/studies/etc. relevant to cloud computing, determine standards gaps, and identify standardization priorities. NIST is leading the development of a Cloud Computing Technology Roadmap. This roadmap will define and prioritize USG requirements for interoperability, portability, and security for cloud computing in order to support secure and effective USG adoption of Cloud Computing.

As one of the TREC factors, the risk factor is defined as part of TREC term language of WP2.2 which started discussing the TREC term language in the GRAAP working group of the Open Grid Forum in 2011. The outcome of the discussions was the decision to publish the TREC parameters in an informational document of the OGF first and see whether there is general interest. In a second step, the plan is to create a micro specification for the TREC parameters as a term language for WS-Agreement. There is also plan to continue this effort based on the state of the TREC parameters as defined in the OPTIMIS manifest. Moreover, currently there are Cloud SLA-related activities in other SDOs as well.

4 Activity of Members in various Standards

4.1 WP2.2, WP3.4

Members of this WP (SCAI) are member of the Open Grid Forum and leading the GRAAP-WG that developed the WS-Agreement recommendation and currently is developing the WS-Agreement Negotiation specification. The WP is also active in the OCCI working group. A member of SCAI is currently Area Director Applications in the Open Grid Forum.

WP2.2 members are also active in the Tele management Forum in the TR 128 cross SDO working group on end-to-end SLA management. The focus of this group is generating a use-case document for e2e SLA Management that takes into account the standards already available from the different SDOs (TMF, OASIS, DMTF and OGF). Our contribution is WS-Agreement and WS-Agreement Negotiation.

Other members of these WP (ULEEDS) are also members of standardization bodies within and outside the scope of OPTIMIS and they are actively contributing to the Reference Architecture and Taxonomy Group, Standards Roadmap Group, Security Group, Business Use Cases Group of NIST Cloud Computing Program.

There is a plan to propose the OPTIMIS based risk management framework (SP-IP profile evaluation, risk assessment, mitigation and negotiation) and methodology (e.g. cloud computing risk inventory) for cloud computing to the NIST Cloud Computing Program. TREC factors are defined as part of TREC term language of WP2.2, and there is strong interest in liaising with the GRAAP working group of the Open Grid Forum to publish the TREC parameters in an informational document to check general interest in its adoption (see section 3.2)

4.2 WP5.4, WP6.2, WP 6.3, WP6.4 and Wp7.5

BT who is a member of these WPs is contributing to Cloud Security Alliance (CSA) Governance Risk and Compliance stack and to ENISA expert group on Cloud Security and Resilience focusing on guidance for incident reporting as part of implementing the European Cyber Security Policy.

Furthermore Atos, BSC, BT and SCAI have contributed to the Cloud Computing standards roadmap that is being produced by ETSI as explained in section 3.2.1. See also [31].

4.3 WP5.2

WP5.2 has been taken standards under consideration and actively supports a variety of them, as shown in Table 1. In order to extend also the current Cloud standards, this WP has been involved in the definition of an XML schema that may be used by an IaaS provider to describe its capabilities and configuration to the external world (Cloud Provider Description Schema). More information on its structure may be found in D5.2.2.2 Scientific Report document. During its creation, standards have been taken under consideration in order to portray the necessary information that describes the provider's capabilities. Some standards that have been defined and used in the schema are ISO14000, Energy Star, OCCI, OVF, TOSCA, SOAP, REST and SPEC. These dictate the different standards that a CP can declare compatible to, and can be extended at will in the aforementioned schema.

Other standards that are used in the implementation of WP5.2 refer to SHA1, AES, SSL and HMAC for authentication. Furthermore, this WP will look into possible ways to standardize the way time series prediction information is exchanged between service oriented components, possibly through extending the PMML standard.

5 Conclusion

The use of standards in various OPTIMIS work packages combined with a parallel Interoperability task is contributing to making OPTIMIS output more acceptable by the cloud community. The document shows the awareness of various standards and their use in the various work packages of OPTIMIS.

Furthermore OPTIMIS partners have been involved in developing guidance and new industry standards which kept OPTIMIS development aware and up-to-date of the ongoing demand from cloud communities and users.

Finally, OPTIMIS has directly or indirectly contributed to wider impact global activities through NIST, ETSI, CSA and ENISA. These activities range from Cloud Standards Coordination to input on the impact of the European Cyber Security strategy and Directive on Cloud and Internet based services.

6 References

[1] http://www.dmtf.org/standards/ovf
[2] http://cdmi.sniacloud.com/
[3] http://www.snia.org/
[4] https://cloudsecurityalliance.org/
[5] http://common-assurance.com/
[6] http://www.enisa.europa.eu/
[7] http://www.ogf.org
[8] http://ogf.org/gf/group_info/view.php?group=graap-wg
[9] http://ogf.org/documents/GFD.107.pdf
[10] http://ogf.org/documents/GFD.193.pdf
[11] http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf
[12] http://www.dmtf.org
[13] http://www.ogf.org/documents/GFD.90.pdf
[14] http://www.ogf.org/documents/GFD.183.pdf
[15] http://www.ibm.com/developerworks/webservices/library/ws-restful/
[16] http://www.ogf.org/documents/GFD.184.pdf
[17] http://pubs.opengroup.org/onlinepubs/9699919799/
[18] http://www.ieee.org/index.html
[19] http://www.opengroup.org/
[20] http://tools.ietf.org/html/rfc3280
[21] http://www.itu.int/en/pages/default.aspx
[22] http://www.ietf.org/
[23] http://www.w3.org/2002/ws/
[24] http://www.w3.org/
[25] https://www.securityforum.org/iram/
[26] http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsRoadmap
[27] http://www.computer.org/portal/web/pressroom/20110404cloud
[28] http://dmtf.org/standards/cloud
[29] https://cloudsecurityalliance.org/education/ccsk/certification-board/
[30] https://cloudsecurityalliance.org/research/grc-stack/
[31] http://csc.etsi.org/Application/documentapp/documentlist/

Appendix A License conditions.

This is a public deliverable that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons http://www.creativecommons.org

This license allows you to

to copy, distribute, display, and perform the work

to make commercial use of the work

Under the following conditions:

Attribution. You must attribute the work by indicating that this work originated from the IST-OPTIMIS project and has been partially funded by the European Commission under contract number IST - 257115

No Derivative Works. You may not alter, transform, or build upon this work without explicit permission of the consortium

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

This is a human-readable summary of the Legal Code below:

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

"Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

"Licensor" means all partners of the OPTIMIS consortium that have participated in the production of this text

"Original Author" means the individual or entity who created the Work.

"Work" means the copyrightable work of authorship offered under the terms of this License.

"You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

For the avoidance of doubt, where the work is a musical composition:

Performance Royalties Under Blanket Licenses. Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

Mechanical Rights and Statutory Royalties. Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and

distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer. UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You distribute or publicly digitally perform the Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.