Contract No. IST 2005-034891

Hydra

Networked Embedded System middleware for
Heterogeneous physical devices in a distributed architecture

D13.4 Plans for Contribution to Standardisation Work

Integrated Project
SO 2.5.3 Embedded systems

Project start date: 1st July 2006 **Duration: 48 months**

Published by the Hydra Consortium
Coordinating Partner: C International Ltd.

25. June 2007 - version 1.0

Project co-funded by the European Commission
within the Sixth Framework Programme (2002 -2006)

Dissemination Level: Confidential

Document file: D13.4 Plans for Contribution to Standardisation Work_internal_review.doc

Work package: [WP13 – Dissemination and Exploitation]

Task: [T13.2 Standards]

Document owner: [Atta Badii (University of Reading)]

Document history:

Version	Author(s)	Date	Changes made
0.1	Atta Badii, Adedayo Adetoye, Daniel Thiemert, Renjith Nair	06-06-2007	Structure defined, content added
0.2	Atta Badii, Adedayo Adetoye, Daniel Thiemert, Renjith Nair	20-06-2007	Content added
0.3	Atta Badii, Adedayo Adetoye, Daniel Thiemert, Renjith Nair	25-06-2007	Internal reviewers' comments incorporated
1.0	Atta Badii, Adedayo Adetoye, Daniel Thiemert, Renjith Nair	25-06-2007	Final version submitted to the European Commission

Internal review history:

Reviewed by	Date	Comments
Siegfried Bublitz	22-06-2007	Approved with comments
David Riou	22-06-2007	Approved with comments

Index:

1. Introduction

The Hydra project is researching and developing a middleware for heterogeneous physical devices in a distributed architecture. The middleware is a software layer between the operating system and the applications. The goal of the project is to develop an inclusive middleware. That means that it will be possible to enable any device, current and future devices, to be usable from Hydra enabled applications and devices. The project will deliver development tools such as a Software Development Kit (SDK) and a Device Development Kit (DDK) to allow developers and manufacturers to enable their products to be part of the ambient intelligence environment.

Standardisation plays an important role in order to make new products a success on the market. In this respect two aspects are considered to be important for standardisation work:

- Use of existing standards, and
- Contribution to standards or development of new standards.

Use of existing standards supports technology convergence in making a new product interoperable with existing technologies. Since this is one of the main goals that the Hydra project wants to achieve, i.e. interoperability and inclusiveness, the development of the middleware will also be based on existing standards in the different areas of the project, such as Grid, web services, and security. On the other hand use of existing standards also saves efforts and money since not every technology has to be newly developed from scratch if there are approved and widely used technologies or standards already in place that could be deployed or built upon.

The second pillar of standardisation work is contribution to existing standards or development of new standards. The Hydra project will contribute to standards where gaps have been identified and will develop new standards where those are missing completely. Increasingly in the context of ambient intelligence standardisation efforts should consider deeper levels of integrability that extent the baseline interoperability towards deeper semantic integrability including cooperativity between device agents which should find resonances in the Hydra RTDI agenda with a focus, e.g. on virtualisation including the semantics of Security Context in general and Semantic Resolution of security in particular.

The deliverable D13.4 “Plans for Contribution to Standardisation Work” will summarise the standards already used, the standards that are envisaged to be used, and will identify possible contributions to existing and new standards in the areas of Web Services, Security, Identity Management, Networking, and Grid.

2. Executive summary

The Hydra project is developing a middleware for heterogeneous physical devices in a distributed architecture. The project will develop an inclusive middleware to enable any device to be usable from a Hydra application. The outcome of the project will be a reference implementation, a Software Development Kit and a Device Development Kit.

Standards play an important role for the success of a project later on the market. To achieve interoperability the Hydra project has identified existing standards to be used and new standards to contribute to or develop.

Existing standards that are already used or will be used have been identified in the following main categories: Web Services, Security, Identity Management, Networking, Embedded AmI, Grid, SOA and MDA, Software Development Kits and others. The standards are briefly introduced and their deployment within the Hydra Framework Architecture illustrated.

Furthermore areas have been identified where the Hydra project aims to contribute to existing standards and specifications, e.g. in Identity Management/ Web Services, Construction Classification or Semantic Device Description. The contribution to these standards will take place towards the end of the project.

3. Preliminary Standardisation Work

To contribute to standardisation work knowledge about the process how to contribute is necessary, i.e. the type of organisation, the separate steps, etc. Many of the project partners have available this knowledge since they are already active in the standardisation areas.

- C-Lab for example is active in the standardisation of User Interface Modelling Language (UIML) through OASIS.
- The University of Reading and the Fraunhofer SIT are contributing in the area of semantic-cooperative virtualisation standards through the EU-funded SecurIST taskforce.
- Priway are already contributing to standardisation work in the field of RFID where they are promoting standards for incorporating security.
- Telefonica I&D is a member of the W3C Advisory Committee as well as the ETSI Steering Committee and OMG.

This ensures that the project partners have access to the respective organisations and standardisation bodies and are aware of the procedures of standardisation work.

4. Standards

4.1 Web Services Standards

The HYDRA middleware transparently exposes functionalities to consumers as abstract services using a Service-Oriented Architecture (SOA). Service-Oriented Architecture is simply a design paradigm where access to resources is exposed as services which can be consumed consistently and independently of particular implementations and details of the platform exposing the service. A particular instantiation of the Service-Oriented Architecture paradigm is the Web Services standards, which is a collection of core specifications for exposing services that facilitate machine-to-machine interaction over a network. In the following we highlight some of the key Web Services specifications that are (or potentially will be) used in the HYDRA middleware.

4.1.1 XML

Quick Summary	
HYDRA Usage	In current use (Middleware)
Standard Organisation	W3C
Plan to contribute	No

Extensible Markup Language (XML) is a simple but yet very flexible text format derived from the ISO 8879 SGML format. XML is a W3C standard and is the de-facto format used in Web Services for the exchange of data and messages and it is playing an increasingly important role as the standard data exchange format on the Internet. XML is used extensively in many areas of the HYDRA middleware. We do not plan to contribute to this standard.

4.1.2 SOAP

Quick Summary	
HYDRA Usage	In current use (Middleware)
Standard Organisation	W3C
Plan to contribute	No

SOAP, which stands for Simple Object Access Protocol, is a lightweight protocol for structured information exchange in distributed, decentralised and loosely coupled systems. It is the foundational messaging protocol used in Web Services implementations. SOAP relies on the XML standards to define an extensible messaging framework and messaging constructs that can be exchanged over a variety of underlying protocols. Furthermore, the SOAP protocol is designed to be independent of any particular programming model and other implementation specific semantics. This property is crucial in heterogeneous distributed systems that HYDRA addresses. SOAP is a W3C standard which we use in the implementation of Web Services in the HYDRA middleware, but we do not plan to contribute to this standard.

4.1.3 WSDL

Quick Summary	
HYDRA Usage	In current use (Middleware)
Standard Organisation	W3C

Plan to contribute	No

Web Services Description Language (WSDL) is an XML-based format for describing network services in a structured manner. The key aspect of WSDL is its abstract description or definition of services (also called endpoints) in a way that is independent of the concrete protocols and message formats used to realise those service endpoints. This feature makes WSDL well suited for use in the HYDRA middleware, and in particular for the description of services provided by sensors, actuators, and other HYDRA-enabled devices. WSDL is a very extensible description language, and it is often used in conjunction with protocols such as SOAP, HTTP GET/POST methods and MIME; however its usage is protocol independent. WSDL is a W3C standard and we currently have no intention to contribute to.

4.1.4 UDDI

Quick Summary	
HYDRA Usage	Potential (Middleware)
Standard Organisation	OASIS
Plan to contribute	No

UDDI, which stands for Universal Description, Discovery and Integration protocol is an OASIS standard that allows applications to dynamically find and use Web Services over the internet. It combines a number of technologies such as XML, HTTP and Domain Name System (DNS) to provide a searchable registry of services that allow dynamic integration of applications. UDDI is not used at present in the HYDRA framework, but there is a potential for its usage to allow HYDRA enabled devices to search for services of interest, such as locating and interacting with local resources when the device arrives at a new physical location.

4.1.5 WS-Security

Quick Summary	
HYDRA Usage	Potential (Middleware)
Standard Organisation	OASIS
Plan to contribute	No

WS-Security is a series of specifications which extend the basic Web-Services messaging infrastructure to provide message confidentiality and integrity. In other words, WS-Security ensures the security of message exchange during a Web Service transaction by preventing unwanted disclosure of messages and by ensuring that messages are not tampered with during transmission. The specification proposes a standard set of SOAP extensions that facilitate confidentiality and integrity of messages. This is achieved by using technologies such as PKI, Kerberos, SSL among many others. WS-Security is an OASIS specification. We do not plan to contribute to this standard.

4.2 Security Standards

A key aspect of the HYDRA framework is the integrated security layers which facilitate the enforcement of policies capturing users' security concerns. It is envisaged that the security policy interface will be easy to use. However, translating high level security policies to low level operational constraints will be nontrivial. In order to simplify the process of policy creation for the user, and the process of providing provable security guarantees an approach will be to define common security requirements as primitive policy constructs which the user can compose together into more sophisticated policies. These policy primitives will have been formally verified a priory and a policy advisor will be able to inform the user of the security guarantees that a given policy provides and the associated risks. In this area, HYDRA will be using standard security primitives such as standard cryptographic functions, standard security protocols and policy languages for expressing access control and privacy requirements as follows.

4.2.1 AES

Quick Summary	
HYDRA Usage	In current use (Security)
Standard Organisation	NIST
Plan to contribute	No

AES stands for the Advanced Encryption Standard, which is a symmetric block cipher that can encrypt and decrypt information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Being a symmetric-key cipher the same key is used for both the encryption and decryption of information. AES was published by the National Institute of Standards (NIST) under the US Federal Information Processing Standards (FIPS) Publications (FIPS PUBS 197). AES is used in the demonstrator implementations for encryption. We do not plan to contribute to this standard.

4.2.2 TDEA (3DES)

Quick Summary	
HYDRA Usage	In current use (Security)
Standard Organisation	NIST
Plan to contribute	No

TDEA stands for Triple Data Encryption Algorithm and is also known as Triple Data Encryption Standard (3DES). It is a block cipher based roughly on the repeated application of the Data Encryption Algorithm (DEA) algorithm. TDEA is slowly being replaced by the AES encryption standard as the latter offers a higher security level and is often faster either implemented as a software or hardware module. However, TDEA is still popular because of its use within the electronic payment industry. We use TDEA in demonstrator implementations and will be natively supported by the HYDRA middleware. We do not plan to contribute to this standard.

4.2.3 SHA

Quick Summary	
HYDRA Usage	In current use (Security)
Standard Organisation	NIST
Plan to contribute	No

SHA stands for Secure Hash Function, and it is a family of algorithms published by the National Institute of Standards for computing message digests. Members of this family include SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The key usage of message digests is for authentication purposes and for checking the integrity of transmitted information. SHA is used in many popular applications such as the Transport Layer Security (TLS) and the Secure Socket Layer (SSL) for protecting information exchange between two parties. We use the SHA algorithms in the HYDRA demonstrator implementations and will be natively supported by the HYDRA middleware. However, we do not plan to contribute to this standard.

4.2.4 MD5

Quick Summary	
HYDRA Usage	In current use (Security)
Standard Organisation	IETF
Plan to contribute	No

MD5, which stands for Message-Digest Algorithm 5, is a cryptographic hash function similar to the SHA family of functions. It is weaker than the SHA algorithms such as SHA-1 because of a non-fatal security flaw that it has. MD5 is an internet standard (RFC 1321) and we use it in the HYDRA demonstrator implementations. However, we do not plan to contribute to this standard.

4.2.5 XACML

Quick Summary	
HYDRA Usage	Potential (Security)
Standard Organisation	OASIS
Plan to contribute	Yes

OASIS currently has a version 2.0 of their XACML (eXtensible Access Control Markup Language), which is a standard policy language originally designed for access control but it has recently been extended with constructs for expressing privacy policies. The privacy aspect of the policy framework still has much scope for improvement at the moment and there is an opportunity to contribute in terms of very rich privacy constructs and semantics to the XACML standard. We plan to contribute to this standard. Some of the interesting research issues that are very relevant to the HYDRA framework, and whose inclusion in the XACML standard will be of benefit are the following:

- Abstract models of privacy and trust
- Metrics for trust and privacy
- Privacy guarantees and privacy level agreements (required to be provided by a service provider)
- Policy constructs and support for expressing rich privacy requirements
- Semantic bridges from (easy-to-use) high level secrecy policies to low level semantic enforcement
- Technical enforcement apparatus for secrecy policies. These should be able to notify concerned parties of policy violations and fulfil purposes including[1]:
    - notification of the user about what information is being collected about them
    - informing the user about the purpose for which the data is being collected
    - control of data flow to ensure that it is only being used for the purpose for which it is collected and such that data is not otherwise disclosed without the consent of the owner.

[1] Privacy Guidelines - Organization of Economic Cooperation and Development (OECD), 1980

An enforceable policy standard for privacy and security is a very important aspect of the HYDRA framework and support for this at the middleware level is very desirable. The XACML standard thus seems to have a lot of promise in this regards, in particular since it supports both access control and privacy as well. With respect to privacy policies, a similar effort is the Enterprise Privacy Authorization Language (EPAL) submitted to the W3C by IBM. It has been demonstrated that it is functionally a subset of the XACML standard[2]. Platform for Privacy Preferences (P3P) is also an effort along the lines of user-managed privacy policies. However, P3P is not enforceable and is currently defunct. For the purposes of completeness however we discuss the EPAL and P3P specifications next.

4.2.6 EPAL

Quick Summary	
HYDRA Usage	Not used
Standard Organisation	W3C
Plan to contribute	No

EPAL stands for Enterprise Privacy Authorization Language, which is intended as a formal language for writing enterprise privacy policies to govern data handling practices in IT systems according to fine-grained positive and negative authorization rights. It concentrates on the core privacy authorization while abstracting data models and user-authentication from all deployment details such as data model or user-authentication. Being a policy language for expressing privacy concerns, EPAL is clearly relevant to the HYDRA framework. However, EPAL has been shown to be a functional subset of the XACML standard; and, unlike XACML, EPAL is not yet a standard. We do not plan to contribute to EPAL.

4.2.7 P3P

Quick Summary	
HYDRA Usage	Not used
Standard Organisation	W3C
Plan to contribute	No

The Platform for Privacy Preferences Project (P3P) enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. The idea is that a user agent can make informed choice of whether to proceed with revealing confidential user data by first checking whether the data processing practices of the destination is compatible with the user's privacy requirements. While the idea behind P3P is good, it has received very little support in terms of implementation and adoption, in particular from web browsing software. Work is currently suspended on the P3P specification. We do not plan to contribute to P3P.

4.3 Identity Management

An important issue in the HYDRA framework is the secure management of identities. We plan to contribute to standardisation efforts in this area via experience gained from HYDRA RTD efforts. The relevant industry frameworks that we plan to contribute towards include the OASIS SAML standard, and the Liberty Alliance's Identity Web Services Framework (ID-WSF).

[2] See the Sun Microsystems' technical report at http://research.sun.com/techrep/2005/smli_tr-2005-147/TRCompareEPALandXACML.html

4.3.1 SAML

Quick Summary	
HYDRA Usage	Potential (Security/Identity Management)
Standard Organisation	OASIS
Plan to contribute	No

Security Assertion Markup Language is an XML-based OASIS standard for describing and exchanging security information, such as authentication, entitlements and other security attributes between on-line business partners. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The use of SAML falls under the secure management of identity information in HYDRA.

4.3.2 ID-WSF

Quick Summary	
HYDRA Usage	Potential (Security/Identity Management)
Standard Organisation	Liberty Alliance
Plan to contribute	Yes

The Liberty Identity Web Services Framework (ID-WSF) provides a framework for identity-based web services in a federated network identity environment. One of the key aspects of the ID-WSF is that it now supports the OASIS SAML for deploying and managing open identity-based applications. We plan to contribute to this standard through the HYDRA RTD efforts.

4.4 Networking Standards

The HYDRA middleware layer sits on top of, and transparently provides access to, various networking technologies via consistent interfaces which hide the complexity of the specific technology in use. We highlight below some of the networking standards that the HYDRA middleware supports.

4.4.1 IPv6

Quick Summary	
HYDRA Usage	Potential (Networking)
Standard Organisation	IETF
Plan to contribute	No

IPv6 stands for the Internet Protocol version 6, and is also known as the “next generation” Internet protocol. IPv6 is an IETF standard and is intended to be a replacement for the current version of the Internet Protocol standard (also known as IPv4). IPv6 is an improvement on IPv4 and solves the address space problem associated with the IPv4[3]. The address space size is very important in particular small mobile devices must be assigned with unique addresses like any other computer on the internet. It is envisaged that more and more mobile devices will use IPv6 in the future and hence the strategic importance of a native support of the IPv6 protocol by the HYDRA middleware.

[3] IPv6 addresses are 128 bits as opposed to the 32 bits used for IPv4 addresses.

IPv6 also has many other useful features that are relevant to HYDRA such as stateless auto-configuration of hosts, security and inbuilt multicast support. We however do not intend to contribute to this standard.

4.4.2 ZigBee

Quick Summary	
HYDRA Usage	Potential (Networking)
Standard Organisation	ZigBee Alliance
Plan to contribute	No

ZigBee is a set of high level communication protocols for low-power digital radios. These are mainly used for embedded applications which require low data rates and power consumption. The specification will be used for networking and no contributions are planned.

4.4.3 Bluetooth

Quick Summary	
HYDRA Usage	Potential (Networking)
Standard Organisation	Bluetooth Consortium
Plan to contribute	No

The Bluetooth technology is a short range communication technology commonly used for mobile devices. It provides wireless technology that is robust, has low power consumption and is available at low cost. The potential use of the specifications by the Hydra project is in the networking domain. No contributions are planned.

4.4.4 IEEE 802.11/b/g

Quick Summary	
HYDRA Usage	Potential (Networking)
Standard Organisation	IETF
Plan to contribute	No

IEEE 802.11 are the Wi-Fi standards for wireless LAN. The main difference between b and g is the data rate (b: 11 Mbit/s; g: 54 Mbit/s). The standard was originally published in 1997 but has been revised since then. In the Hydra project the standard will be used for communication purposes of devices. No contributions are planned.

4.4.5 IEEE 802.15.4

Quick Summary	
HYDRA Usage	Potential (Networking)
Standard Organisation	IETF
Plan to contribute	No

The IEEE 802.15.4 is the standard for low rate Wireless Personal Networks (WPAN). It is the basis for ZigBee and the first version was released in 2003. The standard will be used for low level personal devices within the Hydra framework. No contributions are planned.

4.4.6 RFC 793 – Transmission Control Protocol (TCP)

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

The RFC 793 is the fundamental TCP specification document. TCP is the core transport layer protocol used on the Internet. The RFC describes the TCP packet format, the TCP state machine and event processing, and TCP's semantics for data transmission, reliability, flow control, multiplexing, and acknowledgment. We do not plan to contribute to this RFC.

4.4.7 RFC 1323 - TCP Extensions for High Performance

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

This RFC defines TCP extensions for window scaling, timestamps, and protection against wrapped sequence numbers, for efficient and safe operation over network paths with large bandwidth-delay products. We do not plan to contribute to this work.

4.4.8 RFC 2581 – TCP Congestion Control

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

The RFC 2581 defines TCP's four intertwined congestion control algorithms: slow start, congestion avoidance, fast retransmit, and fast recovery. Additionally, it also specifies how TCP should begin transmission after a relatively long idle period, as well as discussing various acknowledgment generation methods. We do not plan to contribute to this work.

4.4.9 RFC 768 – User Datagram Protocol (UDP)

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

The User Datagram Protocol (UDP) provides a datagram mode for data transport over packet-switched networks, in particular those using the Internet Protocol (IP). The key objective of this protocol is to provide a data transmission mechanism with minimal protocol overhead and thus UDP is relatively lightweight when compared to the TCP protocol used for connection-oriented transport. UDP as opposed to TCP does not guarantee the order of arrival of packets, or whether packets will be delivered or not, or whether packets will not be duplicated. UDP is however useful for applications such as multimedia streaming, video or audio conferencing, and multicasting applications where packet losses can be tolerated. HYDRA supports UDP; however, we do not plan to contribute to this standard.

4.4.10 RFC 791 – Internet Protocol (IP)

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

The Internet Protocol (IP) is designed for use in interconnected systems of packet-switched computer communication networks. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses: 32 bit for IPv4, and 128 bit for IPv6 the fourth and sixth version respectively of the Internet Protocol. The IP is specifically limited in scope to provide the functions necessary to deliver a package of bits (an Internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. Hydra uses the IP protocol natively; however, we do not plan to contribute to the standard.

4.4.11 RFC 1519 – Classless Inter-Domain Routing (CIDR)

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

Classless Inter-Domain Routing (CIDR) is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme. It allows increased flexibility when dividing ranges of IP addresses into separate networks and thereby promotes more efficient use of increasingly scarce IPv4 addresses and because of its use of hierarchies in address assignments (also known as prefix aggregation) it lowers the overhead on inter-domain routing on the Internet. IPv6 uses CIDR routing technology and CIDR notation in the same way as IPv4 but as opposed to IPv4 its addressing scheme is designed to be fully classless. We do not plan to contribute to the CIDR standard.

4.4.12 RFC 4122 – Universally Unique IDentifier (UUID) URN Namespace

Quick Summary	
HYDRA Usage	Used (Networking/Middleware)
Standard Organisation	IETF
Plan to contribute	No

The RFC 4122 defines a Uniform Resource Name (URN) namespace for UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique IDentifier). A UUID is 128 bits long, and requires no central registration process. This is one of the key reasons for using UUIDs since no centralised authority is required to administer them. As a result, on demand generation of UUIDs can be completely automated. This is useful in a variety of contexts such as the generation of transaction IDs. UUIDs are of a fixed size (128 bits) which is reasonably small compared to other alternatives. This makes it well suited for sorting, ordering, and hashing of all sorts, storing in databases, simple allocation, and eases its use during programming in general. Since UUIDs are unique and persistent, they make excellent Uniform Resource Names. The unique ability to generate a new UUID without a registration process allows for UUIDs to be one of the URNs with the lowest minting cost. We do not plan to contribute to this standard.

4.4.13 RFC 4291 – IP Version 6 Addressing Architecture

Quick Summary	
HYDRA Usage	Used (Networking)
Standard Organisation	IETF
Plan to contribute	No

This RFC specification defines the addressing architecture of the IP Version 6 (IPv6) protocol. It includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 node's required addresses. We do not plan to contribute to this standard.

4.5 Embedded, Autonomic Ambient Intelligence Architecture

A key aspect of the HYDRA framework is the Ambient Intelligence capabilities provided at the middleware layer. These capabilities are realised via a semantic interpretation of abstract domains created from worlds describing the capabilities of the devices that constitute the worlds. These can be achieved via pre-programmed or dynamic rules and query languages (for example, by using rules frameworks such as JESS and query languages such as OWL-QL or SPARQL) to harvest domain properties and to reason about global capabilities.

4.5.1 RDF

Quick Summary	
HYDRA Usage	Potential (AmI)
Standard Organisation	W3C (Recommendation Status)
Plan to contribute	No

RDF stands for Resource Description Framework and is a general-purpose language for representing information in the Web. Formally, RDF is an assertion language in the form of subject-predicate-object with the intention of ascribing formal semantics or meaning to statements made about resources on the Web. RDF can be viewed as labelled, directed graphs useful for representing information such as personal information, social networks and metadata about digital artefacts. In this regards, it could be used as a data model in a knowledge management system or in ontological specifications. RDF is one of the specifications under the W3C Semantic Web activity. It currently has a recommendation status. We do not plan to contribute to this standard.

4.5.2 SPARQL

Quick Summary	
HYDRA Usage	Potential (AmI)
Standard Organisation	W3C
Plan to contribute	No

SPARQL is a recursive acronym that stands for SPARQL Protocol and RDF Query Language. As its name suggests, SPARQL is a query language for searching RDF graphs – which is a directed, labelled graph data format useful for representing information such as personal information, social networks, metadata about digital artefacts, as well as to provide a means of integration over disparate sources of information among many other uses.

4.5.3 ISO/IEC 15909

Quick Summary	
HYDRA Usage	Potential (AmI)
Standard Organisation	ISO
Plan to contribute	No

The ISO/IEC 15909 standards deals with definition of Petri nets, an interchange format for Petri nets (PNML- Petri Net Markup Language), and with Petri nets extensions. Petri nets are currently used for event handling within the middleware. There are no contributions planned to extend this standard.

4.6 Grid Technology

Grid Technology or Grid Computing is an infrastructure that allows for the integrated use of (geographical) distributed resources. The grid coordinates the resources to achieve a given goal.

4.6.1 OGSA

Quick Summary	
HYDRA Usage	Potential (Grid)
Standard Organisation	GGF
Plan to contribute	No

The Open Grid Services Architecture (OGSA) by the OGSA working group within the Global Grid Forum (GGF) describes an architecture for service oriented grid computing as it will potentially be used in the Hydra framework. The architecture is based on the on web service technologies such as WSDL or SOAP. The consortium does not plan to contribute to that specification.

4.6.2 WSRF

Quick Summary	
HYDRA Usage	Potential (Grid)
Standard Organisation	OASIS
Plan to contribute	No

The Web Service Resource Framework belongs (WSRF) to the OASIS-family of specifications for web services. WSRF provides functionalities that enable developers to transform web services, which are usually stateless, into stateful web services. It also provides functionality to address resources that should be used within a specific service request.

Stateful services are essential for session based interaction, e.g. in security mechanisms. Therefore it is likely that the Hydra project will make use of these standards. It is not planned to make contribution to this work.

4.7 Service Oriented Architecture and Model Driven Architectures

Service oriented Architecture and Model Driven Architecture are design principles used in Hydra. Whilst SoA is the main concept for the development of the middleware, MDA is used to realise the Software Development Kit (SDK), the Device Development Kit (DDK) and the Integrated Development Environment (IDE).

4.7.1 UML

Quick Summary	
HYDRA Usage	Used (Software Engineering)
Standard Organisation	OMG
Plan to contribute	No

The Unified Modelling Language is defined by the Object Management Group (OMG) to specify, visualise, construct and document software-intensive systems. UML is used in the in the software modelling and design stages of the Hydra project. No contributions are planned for this specification.

4.7.2 SOA

Quick Summary	
HYDRA Usage	Used
Standard Organisation	OASIS
Plan to contribute	No

Service Oriented Architecture (SOA) is not a standard but “a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.”[4] Since Hydra aims at developing a middleware for heterogeneous physical devices in a distributed architecture, the project will make use of the concepts of SOA. A contribution to the specification is not foreseen.

4.7.3 MDA

Quick Summary	
HYDRA Usage	Used
Standard Organisation	OMG
Plan to contribute	No

[4] See http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf for details.

Model Driven Architecture (MDA) by the Object Management Group) itself is not a standard but builds on existing specifications such as UML, Meta-Object Facility or Common Warehouse Meta-model (CWM). It aims at supporting platform independent architecture definition. The MDA approach will be used for realising the SDK, DDK, and IDE.

4.8 Software Development Kits

A key goal of the HYDRA framework is the development of Software Development Kits (SDKs) that can be used to develop innovative Model-Driven applications with embedded ambient intelligence using the HYDRA middleware.

4.8.1 Java Standards

Quick Summary	
HYDRA Usage	Used (SDK)
Standard Organisation	No
Plan to contribute	No

The Java programming language was released in 1995 by Sun Microsystems and has since then published several releases of J2SE (Standard Edition) or J2ME (Mobile Edition) which are used for this project. Java has not been standardised.

4.8.2 Microsoft .Net

Quick Summary	
HYDRA Usage	Used (SDK)
Standard Organisation	ECMA / ISO
Plan to contribute	No

The Microsoft .Net Framework is a software component to be included in the Microsoft Windows operating system. The Common Language Interface (CLI) and the programming language C# have been standardised in 2001 by ECMA (ECMA 334) and 2003 by ISO (ISO/IEC 23271 and 23270). The .Net Framework and .Net Compact Framework (CF) is used for implementation of web services as well as for realisation of the SDK and DDK.

4.8.3 ISO/IEC 9899

Quick Summary	
HYDRA Usage	Used (SDK)
Standard Organisation	ISO
Plan to contribute	No

The IS/IEC 9899 is the standard for the programming language C. It was published in 1999 but the latest version was made available in 2005. C is used for low level network and device programming.

5. Other Standards

5.1 Architecture Specification and Software and Systems Engineering

5.1.1 IEEE 1471

Quick Summary	
HYDRA Usage	Used (Architecture Design)
Standard Organisation	IEEE
Plan to contribute	No

The Recommended Practice for Architectural Description of Software-Intensive Systems is used by the Hydra project during the architecture design process. There are no contributions planned for this standard.

5.1.2 ISO 9126

Quick Summary	
HYDRA Usage	Used (Software Engineering)
Standard Organisation	ISO
Plan to contribute	No

The ISO Software Engineering Product Quality specification has been used to verify the quality of the requirements engineering results. No further contributions to the specification are envisaged.

5.2 Other

5.2.1 BSAB/ AMA

Quick Summary	
HYDRA Usage	Classification of devices
Standard Organisation	BSAB/AMA
Plan to contribute	Yes

BSAB is a common classification scheme for the Swedish building and construction industry while AMA is the common construction directives structured according to BSAB. The Hydra project envisages contributing to these schemes in order to add device classification facilities to the construction scheme.

5.2.2 Semantic based device interoperability

Quick Summary	
HYDRA Usage	Classification/interoperability of devices
Standard Organisation	W3C

Plan to contribute	Yes

The Hydra project will implement a middleware for interoperability of heterogeneous devices. This will be based on a semantic description of devices. Protocols for the bridging of such description have been identified missing or insufficient. Therefore the project will develop standards for interoperability of semantic descriptions in the final phase of the project.

6. Conclusion

This report has acknowledged the Standardisation in Hydra as encompassing two main planks of effort namely the deployment of existing standards, and, contribution to relevant standardisation including innovation of new standards as needed to ensure a confluence of technology interfaces to serve the future deeper semantic integration of technologies serving the emergent ambient intelligence.

Accordingly this deliverable has presented a summary of the standards already deployed in the project as well the standards that are envisaged to be used, and, has sought to identify possible contributions to existing and new standards in the confluent technology areas of Web Services, Security, Identity Management, Networking, and Grid. However, since existing standards are already mature enough to fulfil the demands of the project, only few contributions are planned.

7. Glossary of Acronyms and Abbreviations

AES	Advanced Encryption Standard
AmI	Ambient Intelligence
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
MDA	Model-Driven Architecture
MIME	Multipurpose Internet Mail Extensions
NIST	National Institute of Standards and Technology
OASIS	Organization for the advancement of Structured Information Standards
OMG	Object Management Group
PKI	Public Key Infrastructure
RDF	Resource Description Format
SDK	Software Development Kit
SGML	Standard Generalised Markup Language
SHA	Secure Hash Algorithm
SOA	Service-Oriented Architecture
SOAP	Simple Object Access protocol
SSL	Secure Socket Layer
TCP	Transmission Control protocol
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
WSDL	Web Services Description Language
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language