IoT Architecture

Section I: The Issue / Challenge

The Internet of Things domain will encompass an extremely wide range of technologies, from stateless to stateful, from extremely constrained to unconstrained, from hard real time to soft real time. Therefore, single reference architecture cannot be used as a blueprint for all possible concrete implementations. While a reference model can probably be identified, it is likely that several reference architectures will co-exist in the Internet of Things.

Architecture in this context is defined as a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

For example, the RFID Tag based identification architecture (using a tree naming mechanism) may be quite different from a sensor-based architecture, which is more comparable to the current Internet. There will also be several types of communications models such as: Thing to Application Server, Thing to Human or Thing to Thing communication.

The IoT architecture, like the Internet, will grow in evolutionary fashion from a variety of separate contributions, rather than from a grand plan. In this respect the group considered that current efforts regarding architecture models under development, such as the ITU-T model, the NIST model for Smart Grid, the M2M model from ETSI or the Architectural Reference Model from the EU IoT-A project and related work in other international fora such as the IETF, W3C etc., should be factored into future developments of the policy debate in Europe.

An area of overlap also exists between Identification and Architecture. It is not clear that a single addressing model will be applicable to the entire IoT, nor necessarily a single addressing format. The wide range of resources and computing capabilities available to IoT devices may require many optimized address formats, which need to be unified by a common ID-to-Address translation service. In the same way that DNS allowed the location of devices to be decoupled from their services a similar name resolution component of the IoT will be required to support mobile as well as resource constrained devices. Whether a single global addressing system for IoT will emerge is an open question at this stage.

There are also some factors derived from the current legal framework to be taken into account when dealing with IoT architecture, particularly those related to privacy and data protection issues that need to be considered since the preliminary steps of the development.

This document is intended to provide a preliminary view on some of challenges/objectives related to IoT architecture that are relevant form an EU public interest perspective.

Is the need for network autonomy and security stronger for IoT applications that can be considered extensions of physical infrastructures?

Depending on the application, the need for network autonomy and security can be different, and will depend on considerations of the impact of compromised security or dependence on a service or infrastructure that is temporarily not available. Whether or not an application is the extension of a physical infrastructure is therefore only a secondary consideration.

The Internet of Things involves an increasing number of smart interconnected devices and sensors (e.g. cameras, biometric and medical sensors) that are often non-intrusive, transparent and invisible.

Moreover, as the communication among these devices as well as with related services, is expected to happen anytime, anywhere, it is frequently done in a wireless, autonomic and ad-hoc manner. In addition the services become much more fluid, decentralized and complex. Consequently, the security barriers in Internet of Things become much thinner. It also becomes much simpler to collect, store, and search personal information and endanger people's privacy. Finally, concern is rising that control over personal information is increasingly out of the hands of people. Obviously, this goes beyond the risks people are currently used to, leading to new security requirements and to a general requirement / obligation of transparency and accountability when providing IoT services.

In general, applications with and without extensions to the physical infrastructure can have needs for strong security and autonomous operation. A database of nuclear secrets, computer-controlled brakes in a car, and a hospital patient monitoring system may all require significant care in these respects. But it is perhaps likely that with the advances in machine-to-machine networking, there will be more applications that have security or autonomy requirements. This is natural, as IT technology expands to additional application areas. The requirements from applications do differ, however, and there should be no forcing of all applications to comply with the toughest requirements providing that they are enough according to the identified risks.

Autonomous operation will be needed in many applications. It can consist of autonomous operation of individual devices and self-organizing network mechanisms. It is important to ensure that any individual device or even the entire network is not dependent on some remote service that may become unavailable at times. Naturally there are also many applications where the ability to communicate outside a single network is crucial, and such applications cannot be entirely independent of the rest of the worldwide networks.

Issues with security, configuration, and autonomous operation should be addressed through the normal technical mechanisms and proper network design. Some areas, such as autonomous operation, are still active research domains and the solutions for specific situations are evolving.

However, certain use cases where privacy-sensitive data and information are involved, such as in Healthcare, additional security measures, governance and possibly even patient consent models need to be taken into consideration for the developing models for architecture governance.

Is a centralised architecture a risk for security and do other options exist?

In the IoT the integration of data over many environments will be supported by modular interoperable components. Solutions will need systems that combine volumes of data from various sources to determine relevant features, interpret it to show relationships, compare it to historical data and give greater meaning and context, and present the data when, where, and how it's most useful to support decision making.

Architectures should be open and standards based and not constrain users into fixed, end-to-end solutions, but facilitate solutions where customers and users can choose, leverage or mix different applications, service offerings and devices.

As a starting point the IoT reference architecture: (http://www.iot-a.eu/public/public_documents/d1.2) can be considered. Other reference architectures, such as the ITU_T reference architecture, can also be considered albeit that for example this ITU_T architecture is typically being used for use cases where identification plays a major role.

The IoT Architecture should be flexibly designed to cater for use cases where identification is being used (RFID, tags), as well as intelligent devices, smart objects (hardware and software solutions), and where active and participatory communication is involved.

IoT security is a major pre-requisite in defining architectures. The risks of centralized/decentralized architecture need to be carefully evaluated and secured through standardized measures. Clarity needs to be given to the question of what is centralized/decentralized in the architecture and then discuss advantages and risks. Generally decentralized architectures are very often preferable from the security perspective (denial of service attacks), but it really depends on what is meant to be centralized and on particular use cases.

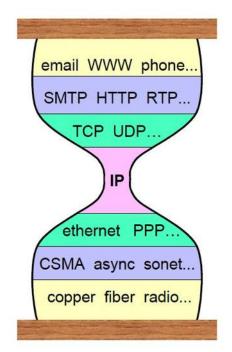
Governance of centralized vs decentralized architectures needs standardized ways for secure configuration and design of (ad-Hoc) solution networks, as well as secure operational functioning.

In deciding between centralized vs. decentralized IoT architecture designs, the development of reference architecture standards, or architecture ecosystems, should be considered; depending on specific domain use cases (e.g. identification, transaction, finance, healthcare etc.) leveraging applicable accepted international standards for the use case domain.

In short, for the IoT, a reference architecture is required that describes essential building blocks and that defines security, privacy, performance, and similar needs. Interfaces should be standardized, best practices in terms of functionality and information usage need to be provided leveraging as much as possible state of the art concepts and technologies.

How to manage the complexity deriving from the proliferation of networks (WAN, PAN, BAN, Ad Hoc Objects Networks, etc.), according to the type of architecture, interconnection and security levels?

Internet of Things technology can appear complex for variety of reasons. First, there is legitimate heterogeneity in the used networking technology and applications. This variation is necessary and useful, as for instance different applications and environments benefit from varying networking technology. The range and other characteristics of cellular, wireless local area networking, and RFID are very different from each other, for instance. There are literally thousands of different applications, and it is natural that they have differing requirements on what parties need to communicate with each other, what kind of security solutions are appropriate, and other aspects.



The answer to managing complexity in the face of this lies in layers of communication mechanisms. **Steve Deering's** hourglass model for IP communications is applicable here.

The hourglass model states that if there is a common waist of the hourglass, then all applications can work over all physical networking technology, ensuring widest possible coverage of networking applications. "Everything over IP and IP over everything."

Even if originally presented for very different protocols, the hourglass model provides some guidance for thinking about the Internet of Things architecture. First of all, it shows how we need common internetworking infrastructure (IP) to allow heterogeneous link media to work seamlessly with each other, and with the rest of the system. Secondly, there are various transport and middleware communications mechanisms that will probably become useful in the different IOT applications. For instance, today HTTP, COAP, XML, and JSON appear to be popular transport mechanisms and formats for a large class

of IOT applications, regardless of what specific link technology they run over.

But there can also be undesirable complexity and variation. Creation of alternative standards where one would have sufficed may be harmful (though it is important to leave room for competing technical solutions). Creating systems and communications mechanisms with unnecessary dependencies between different layers and system components limits our ability to migrate IOT systems to the most economic and efficient platforms, and limits our ability to connect as many "Things" as possible.

To summarize, complexity and alternative technologies can be very useful as a part of architecture, or can be problematic when it creates unnecessary competition and deployment barriers in the market place. The complexity will be addressed by regular technological evolution in the industry through underlying layers of bridging, tunneling, security etc. The Internet of Things framework should allow diverse technological solutions to resolve these issues depending on application requirements.

What about the neutrality principle in IoT? (e.g. for ensuring competition and innovation dissemination on all IoT market segments, for allowing new isolated players and small scale structures to propose and disseminate innovations on a large scale, for promoting innovation via new business models.)

Neutrality means transparency and lack of specific actions to promote one actor or perspective over others. In the development of the IoT, there are a number of dimensions to which neutrality should apply including forming, operating within, and the evolution of the IoT.

Neutrality also has an impact in terms of privacy and data protection as far as some specific actions can lead to expose personal data (e.g deep packet inspection).

Standards have an important role to play in forming the IoT and it is essential that all actors have equal access to the standards making process for the IoT. For a concept as vast as the IoT there will of course be many simultaneous standards making activities, distributed not only by technologies and applications but also geographically. Coordination of standards development, without constraining freedom to innovate, will promote efficient development of IoT infrastructure and consequently applications, services and devices. In the same manner that global coordination of M2M standards is being considered within the GSC, similar coordination may be applied to IoT standards.

Another perspective is that the IoT will in fact function as an infrastructure that a wide variety of applications and services will rely on. As a consequence access to this infrastructure [can][will] be important in order to develop and roll out new and innovative applications and services.

How to develop open standards instead of proprietary services/technologies? (e.g. object resolution services like the ONS.)

Interoperable modular solutions require the use of devices and smart objects that connect, communicate and operate according to standards. The preference is that they communicate through the use of international standards. European specific standards should only be considered where no other standard is available or where implementation of standards poses risks in terms of security, safety or privacy.

An architectural ecosystem should contain the necessary interfaces such that various parties can contribute in all layers, leveraging these international standards.

Today, large parts of machine-to-machine networking applications are specialized systems from a single vendor. Standards are needed to acquire the benefits of using commodity communications technology (such as cellular, wireless LAN, or Internet). Similarly, to support interoperable devices

and applications, standards are required not just at the physical and network interfaces, but also for application frameworks and data models.

We have to separate different aspects of such open standards, when examining the example of an object resolution services. Firstly, there are the technical standards themselves. Secondly, the architecture of those standards may support either a centralized or distributed implementation model. Thirdly, the information carried in these systems may be either centrally agreed or there may be different information in different deployments. Fourthly, the agreements about the standards or the information carried in the systems specified by the standards can be either openly agreed or provided by a closed process (such as through a company). An example may clarify these distinctions. For instance, there exists only one specification of the Domain Name System (DNS), but its architecture allows distributed operation. Indeed, the operation of the DNS root servers is replicated through the world in different organizations that run independently of each other. However, the actual data carried in the root is globally agreed. However, these agreements come through a process that is open to multiple different types of participants. In some applications -such as agreeing on name spaces that are globally accessible and should be the same regardless of your place of access -- it is necessary to have such a global agreement. The important aspects are that each step - standards, implementations, and possible agreements about information content -are open.

In general, open standards, information models, and other agreements can be developed when multiple parties co-operate to create these standards. The process has to be open to any type of a participant, and it is beneficial when the resulting standards are publicly and freely available. In today's networked world, global standards are typically more relevant than any local agreements. From an EU perspective, we recommend preferring open standard solutions over proprietary ones in government procuring, emphasizing the focus on global standards where EU can compete in the global business as opposed to internal EU standards, and setting policies that support getting sufficiently wide input on any standardization effort from a variety of types of participants.

Section II: Design Principles for IOT Architecture

This section previews possible extensions to the current work. It will require substantial effort to address the necessary level of details. It may require also splitting the work by market segments (i.e. Smart Grid, Smart home, healthcare, smart city, ITS...). Some of them have already been covered by European Mandates.

- 1. Application Support
- 2. Does IPv6 and IP technologies have a role to play within IOT?
 - a. Public and Private IP infrastructure:
 - b. Addressing mechanism
 - c. Security in IP networks
 - i. VPN
 - ii. Encryption
 - iii. Key management
 - d. Global IP perspective
 - i. IP in global markets i.e. Smart Grid
 - ii. Influential technologies i.e. 6LoWPAN
 - iii. Market making organizations i.e. WiFi Alliance, IPSO
- 3. Architecture performance
 - a. Resilience
 - b. Performance
- 4. Cloud computing / Virtualization
- 5. Innovation
- 6. Standards
 - a. Necessity for Open standards

It is likely that healthy development of IoT technologies and mandating the use of Open specifications will foster markets in Europe.

"Open specifications" that are considered applicable from a CEN/CENELEC/ETSI point of view comply with the following criteria:

- The specification is developed and/or approved, and maintained by a collaborative consensus- based process;
- Such process is transparent;
- Materially affected and interested parties are not excluded from such process;
- The specification is subject to RAND/FRAND Intellectual Property Right (IPR) policies in accordance with the "EU Competition rules";
- The specification is published and made available to the general public under reasonable terms (including for reasonable fee or for free).

b. Standardization Body ranking for the European IoT.

We have seen in recent EC mandates the need to establish a ranking of SDOs. Most of the well-established communication standards are from international organizations such as IETF and IEEE.

The selection of standards to be promoted in the development of the IoT should be based on the openness of the standards process and the technical relevance of the produced standards.

It is necessary to differentiate between infrastructure standards, especially where significant financial investment is required such a national M2M infrastructure, and device technology which may provide localized IoT communications or may connect to the infrastructure.

Competition in device technology is likely to promote rapid change and technical advancement that may not necessarily be compatible with the implementation and cost timescales of a substantial infrastructure.

The promotion of stable infrastructure standards, and their support by device technology, may be required to create the interconnection fabric necessary for the expected large-scale IoT application benefits to be realized.

7. Research

SECTION III: Objectives, Policy options and Impacts

Fair access to the infrastructure

"Another perspective is that the IoT will in fact function as an infrastructure that a wide variety of applications and services will rely on. As a consequence access to this infrastructure [can][will] be important in order to develop and roll out new and innovative applications and services."

Challenge / Issue description:

IoT applications rely on a communication infrastructure for exchanging information. It is important from a public policy point of view to ensure that IoT applications, which include healthcare, energy management, transportation, or any other innovative applications, will benefit from a fair access to this infrastructure.

The predictability of the development / deployment of such applications and the transparency in the service offering are key for the IoT success and its adoption by the European Union citizens.

Objectives to be achieved:

How can we characterize a fair access?

- It has to be **non-discriminatory**: not related to any types of applications or protocols.
- **Transparency of the tariff**: The tariff (including roaming charge if any) should be based on the real cost of carrying data packets or on the real cost of the implementation of the negotiated SLA (Service Level Agreement: QOS, bandwidth etc.). It should not be based on the types of applications or protocols (for example SMTP traffic versus HTTP, VoIP versus data...) or based on the geographical location.
- **Independence towards the infrastructure provider:** There should be no barrier whatsoever to move from one infrastructure service provider to another one (technical, price or contract).
- Ensuring practices in line with the legal framework on privacy and data protection issues.

Allow development and deployment of IOT applications across Europe with a predictable ROI (Return on Investment)

Avoid further problems equivalent to the non-regulated roaming charges of the cellular network. Maximize the impact of these technologies on the citizen life.

Permit independence from the infrastructure providers.

Policy Options:

- **Do nothing** and let the market decides based on the competition:

Impact:

Economic

- The advantage of such system is that it will promote the development of applications with a good business case and ROI as it leaves the initiative to commercial entities.
- The disadvantage is that it may impair the emergence of innovative applications and their deployment. We could see influence coming from large groups or corporations, which will dominate the market and leave almost no place to small and innovative companies.
- Social
 - o It may impact the neutrality principle as defined in this document as well as individual rights.
- Societal
 - We may see dominant position from large corporations.
- Environmental
 - o No specific impact

Binding law:

Tariff regulation may be a good example of a binding law but it may be difficult to adapt to each EU member state based on the differences that exist in the coverage of such infrastructure and the investment capacity of each state.

But binding laws may be the only viable solution to address the fair access challenge.

Impact:

- Economic
 - This will offer a clear economical view and will allow IOT application's business case to be based on real cost of services.
 - One disadvantage is that it may also impair the emergence of new business models not known at the moment of the elaboration of the regulation.
- Social
 - No specific impact
- Societal
 - Directives may be used to ensure the non-discriminatory aspect of the issue and a fair playing field for the stakeholders.
- Environmental
 - No specific impact

Non binding law:

Opinions and recommendations may be expressed to address the different aspects of the issue but the effectiveness may be discussed and probably will not be followed by facts.

Impact:

- Economic
 - o This option will have a limited economic impact as being only recommendation.
- Social
 - o No specific impact
- Societal
 - o Very limited
- Environmental
 - o No specific impact

Spectrum management

Issue description:

The IoT will have a very wide range of devices acting as data sources and a very wide range of services acting as sinks for IoT data. At the heart of the IoT is the notion of connecting mundane everyday devices – sensors & actuators, monitoring devices and appliances – and mining the flows of data they produce to synthesize information which fuels innovative services.

The issue of fair access to the infrastructure described above requires thought about connectivity technologies and policies to ensure that fair access is enabled in all aspects of the IoT infrastructure.

Connectivity technologies may be a function of the type of device and will operate over many different media e.g. fixed and mobile communications systems, powerline communications and most certainly wireless, especially short-range wireless, technologies. For optimum development of the IoT, the resources necessary for connectivity must be ubiquitous. Communications technologies for both fixed and mobile devices should enable low cost, reliable connectivity for even the simplest of devices.

Although spectrum regulation also applies to powerline technology, for wireless sensor devices, expected to form a significant portion of IoT source devices, radio spectrum is a critical resource. Correct spectrum depends on the application but must satisfy the demands of the propagation environment, provide adequate bandwidth for the application and the number of devices requiring service, and needs to be harmonized to allow large market development and support for mobile applications across regions or even globally. Europe is currently at a disadvantage to some other regions because of the lack of a 900MHz IS&M band (because of cellular deployments) such as is available in the USA, Australia and for some applications also in Japan. Opportunities from global economies of scale may be missed because of sub-optimal global spectrum policies. Where possible, opportunities for global harmonization (for example in the 915-921MHz band) should be strongly promoted.

These requirements align with the objectives of the first radio spectrum policy programme announced by the Council of the EU on 28 October 2011. The spectrum policy should

- 1) Ensure that adequate spectrum resources for device connectivity technology are mandated within the European Union.
- 2) Ensure spectrum access regulations promote equitable use of the spectrum resource
- 3) Satisfy the operating requirements of IoT devices and applications
- 4) Harmonize these resources across global regions as far as possible to promote technology interoperability leading to global scale efficiencies.

Supportive spectrum policies will stimulate innovation via investment in new device communications technologies, improved efficiency in medium use and increased reliability in communications leading to reduced device power consumption, increased device operational lifetime and reduction in total costs. Each of these factors has corresponding positive implications for human quality of life improvement via the IoT. Ubiquitous sensing devices

will be the powerhouse providing raw data to the IoT for myriad data mining applications including medical, transportation, environmental monitoring and human safety.

Inadequate spectrum resource resulting from poor spectrum policy implementation will severely limit the development of device technology. Regional differences in spectrum policies may lead to inequitable IoT development favouring those regions whose spectrum policies allow efficient device connectivity over those that do not. This may eventually lead to an IoT-divide where people in spectrum-wise regions experience significant advantages over those in less forward-looking regions.

Objectives to be achieved:

Uniform spectrum policy throughout the European Community to permit consistent operation of products and equal opportunities for market development and provision of IoT-based services in all Member States.

Spectrum resource designations which stimulate innovation and IoT device development and permit efficient implementation of IoT applications with reliable operation while ensuring efficient use of the scarce spectrum.

Regulation permitting adequate safe transmitted power levels, sufficient permitted duty cycle for small and large scale IoT application operation and addressing a range of frequency bands for the required signal propagation of IoT applications.

Promotion of Cognitive Radio techniques and other advanced spectrum sharing methods which minimize interference with other designated spectrum users and optimize use of available spectrum resources in time, space and frequency.

Policy Options:

Do nothing / Self regulation

This is not a viable option since spectrum is not something that the market place can self regulate. If no actions are taken then spectrum resources will remain as they are currently which is certainly inadequate for the predicted number of IoT operating devices.

Impact:

- Economic
 - Slow growth of IoT driven markets owing to limited performance of IoT communication owing to limited spectrum availability and restrictive Regulatory parameters
- Social
 - No specific impact
- Societal
 - No specific impact
- Environmental
 - No specific impact

Soft law

The advantage of soft law approach lies in the ability to allow different national markets to advance at their own rate. More advanced member states are already putting place IoT applications whereas less advanced member states will require investment to construct the necessary minimum infrastructure.

The disadvantage would be the fragmentation of the European IoT marketplace with inherent risks of divergent technology choice leading to poorer interoperability.

Impact:

- Economic
 - Growth in Member States that take positive initiatives on spectrum regulation for IoT devices, but limited by non-harmonised regional regulatory restrictions.
- Social
 - No specific impact
- Societal
 - No specific impact
- Environmental
 - No specific impact

Co-regulation

Co-regulation, or a mix of regulation and self-regulation, is probably the best near-term option where necessary spectrum decisions are taken by the regulatory authorities but national implementations are allowed to proceed in a manner consistent with local conditions. For example, different member states may have a variety of incumbent applications for any target spectrum identified for IoT use and therefore the time required to re-allocate or deprecate the existing spectrum usage will vary.

Impact:

- Economic
 - Direct impact on economies of Member Sates which instigate Regulatory
 policies to stimulate deployment of IoT-based public services owing to
 improved service efficiency, reduced costs, significant reduction in redundant
 and wasteful non-IoT supported systems. Improved general economic climate
 in technology-driven sectors with growth in SME creation and consequent
 employment driven by innovation.
- Social
 - Expected improvements in Quality of Life from IoT supported applications and services covering Healthcare, Security and environmental protection.
- Societal
 - Potential for major societal improvements via improvements in public service efficiency and individual oriented service enabled by deployment of IoT systems.
- Environmental
 - Potential for major environmental improvements enabled by fast response systems for monitoring and control coupled with new applications enabled by data mining large scale and continuous data sets of environmental measurements.

Binding law: prescribe spectrum use through regulation/directive

Eventually spectrum regulation must be harmonized and this will require binding law policies to be invoked. Applying this option too early will be very costly and potentially disruptive to incumbent applications and therefore binding law should only used for the longer term stable provision of necessary spectrum resources.

Impact:

- Economic

 Stabilised long term growth of IoT driven markets from innovation fuelled by stimulating spectrum resource availability and Regulatory environment

Social

 Wide scale social benefits from uniform availability of IoT devices and systems throughout the community.

Societal

 Levelling of societal advantages in Member States by harmonized spectrum environments allowing common deployment and operation of IoT supported societal applications.

Environmental

 Overall positive contribution to environmental improvements derived from deployment of smart communicating sensors systems for monitoring, control and support of environmental policies.

interoperability

Challenge:

It is the view of the group it is most likely that the architecture of the IoT will rather be described by a reference model than a single architecture and there will be many different – as yet unknown - technologies and applications that will connect to the IoT. This may be described by a layered model. In order to ensure a minimum level of interoperability, it may be necessary to define the interoperability requirements both from a communication and from a data perspective at one or more of these levels based on internationally agreed protocols.

From a public policy perspective [promoting an architectural model] ensuring a minimum level of interoperability may be considered relevant to

- Promote competition
- Help safeguard minimum standards for issues such compatibility, support for privacy and data security (may depend on application)...
- Support creating critical mass

Policy options:

1) Do nothing/Self regulation

The advantage of self-regulation is that the market will find the optimum. Stakeholders, whether or not assembled in international standardization bodies, will agree on the levels of interoperability and protocols. A potential disadvantage of this policy option may be the emergence of a large number of competing, incompatible or incomplete implementations, none of which will gain sufficient critical mass in the short to medium term.

2) Soft law

The advantage of setting possible requirements by soft law is that it will clarify to stakeholders what are the requirements to interoperability seen as desirable from a [public][societal] perspective whereas leaving it to the market to fit these into the IoT architecture. In a situation where the [public] requirements may not be very clear a priori, this option leaves the opportunity to guide the development of the IoT depending on actual developments.

Potential disadvantages of this policy option may be that – while it encourages aligned requirements and approaches – that in certain areas of public concerns requirements from different member states may diverge.

Also for this policy option it is required that there is clarity which [public][societal] requirements to the IoT architecture/protocols are already covered by existing regulations.

3) Co-regulation

The third option is co-regulation, where the regulator sets high-level objectives to be obtained and leaves it to recognized actors in the field. In this context it would be relevant to assess what would be which high level requirements should be posed related to interoperability in order to safeguard [public][societal] interest.

For this policy option it would also be relevant to assess to what extent existing regulation already addresses such high level [requirements][principles].

4) Binding law: prescribe architecture and protocols through regulation/directive

The risk of prescribing architecture and protocols through binding laws is that it will stifle innovation: At this moment it is not possible to predict which technologies and applications will be part of the internet of things. A further risk of prescribing interoperability at any level of detail is that it may disturb the working of the market and that there will be insufficient (commercial) incentive to develop and introduce new technology.

Object resolution (see also Identification sub-group paper)

Challenge:

The basic view of the group that an IoT architecture will probably best be described by a reference model than a single architecture and that there will be many different – as yet unknown – applications/services that will connect to the IoT applies also to object resolution mechanisms.

It would seem plausible at this early stage of technological and market applications development to make the following working assumptions:

- a) Different resolution mechanisms will apply to name spaces of varying sizes (in terms of sectorial/geographical footprint);
- b) The need for these resolution mechanisms to interoperate will vary (i. e. not all name spaces will have sufficient incentives to interact with every other) and, consequently
- c) A unique global meta-resolution mechanism (like the DNS for the Internet) may or may not emerge in the long-term.

The public interest element of different resolution mechanisms will therefore vary depending on their social relevance: the smaller the sectorial/geographical scale of a name space, the lower the public interest that needs to be addressed by public policies. By its very nature, public interest of any global mechanism will be best addressed at the international level, hence EU specific policy initiatives should aim at promoting such global agreements.

An additional dimension needs to be taken into account when evaluating the potential public interest at stake for a specific resolution mechanism. As described in the first part of this paper, each resolution mechanism may be thought of as composed of 3 interrelated elements: 1) Technical standards

- 2) Implementation models (centralized/distributed)
- 3) Information models (same info everywhere/portioned in each instance).

Processes to develop each element may have varying degrees of openness, from closed user groups (the case of proprietary solutions) to more inclusive ones where all interested stakeholders can participate to the process (open standards).

Policy options:

Do nothing/Self regulation

This option would seem appropriate for sector-specific and/or regional resolution mechanisms.

Interested stakeholders can develop services that best address their needs, and decision making processes can remain sufficiently flexible to be able to adapt to rapidly changing needs and technologies.

Soft law/co-regulation (Recommendation)

This option would address those resolution mechanisms with a more global dimension.

Policy makers would set high-level objectives to ensure that all the relevant parties do have an effective way to participate in the decision making process while leaving the detailed development of the solutions to the users.

Hard law (Directive/Regulation)

In highly dynamic technological context, trying to guide future development by law has invariably proved to be inefficient and stifled innovation. Our societies may find that some very high-level principles should be agreed to ensure technological developments are beneficial for all, but by definition they should be agreed at the global level.