**IoT Architecture**

1. The Issue / Challenge

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

This document provides a very initial preliminary view on the challenges and objectives related to IoT architectures.

The RFID Tag based identification architecture (using 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 group observes that most of the current commercial efforts on IOT systems build around existing Internet and mobile network architectures. Additional models currently 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, should also be followed.

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.

**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 that compromised security or dependence from 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.

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 more applications that have security or autonomy requirements. This is natural, as IT technology advances to additional applications. The requirements from applications do differ, however, and there should be no forcing of all applications to comply with the toughest requirements.

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?**

Vertical application models do not work well for integrating data across distributed environments. Interoperable modular solutions are better. Solutions will need systems that combine 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.

Therefore IoT 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 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.

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.

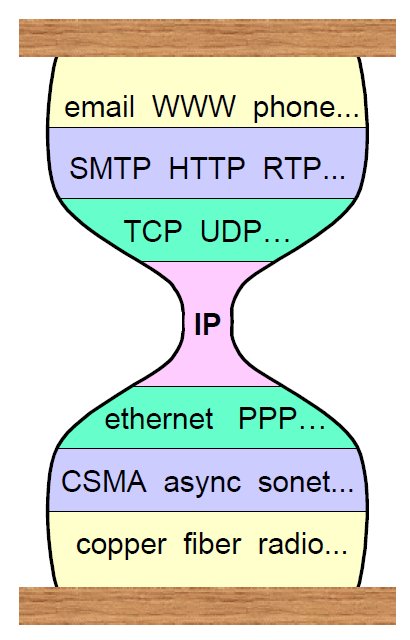
Governance of centralized vs decentralized architectures needs standardized ways for secure configuration and design of (ad-Hoc) solution networks, as well as secure operational functioning.

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 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 (Figure 1).

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 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 today's 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.

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 technologies? (e.g. distributed roots such as FONS.)**

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 can only be considered where no other standard is available or where implementation of standards poses security and safety risks.

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, given the example above about distributed roots. 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 into 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.

1. Objectives to be attained

In order to support innovation, fair access to technology and ensure the interoperability of IoT solutions, we need to support the development of open standards through worldwide coordination.

1. Policy options for reaching the objectives

The architecture sub-group has not yet reached the point to suggest some policy options to sustain the objectives. We see our role as support for the entire IoT expert team and work closely with other sub-groups like the identity, standard or privacy/security on defining these potential policies.