4

Internet of Things Privacy, Security and Governance

Gianmarco Baldini[1], Trevor Peirce[2], Marcus Handte[3], Domenico Rotondi[4], Sergio Gusmeroli[5], Salvatore Piccione[6], Bertrand Copigneaux[7], Franck Le Gall[8], Foued Melakessou[9], Philippe Smadja[10], Alexandru Serbanati[11], and Julinda Stefa[12]

[1]*Joint Research Centre — European Commission, Italy*
[2]*AVANTA Global SPRL, Belgium*
[3]*Universität Duisburg-Essen, Germany*
[4]*TXT e-solutions S.p.A., Italy*
[5]*TXT e-solutions S.p.A., Italy*
[6]*TXT e-solutions S.p.A., Italy*
[7]*Inno TSD, France*
[8]*Inno TSD, France*
[9]*University of Luxemburg, Luxemburg*
[10]*Gemalto, France*
[11]*Sapienza University of Rome, Italy*
[12]*Sapienza University of Rome, Italy*

4.1 Introduction

Internet of Things (IoT) is broad term, which indicates the concept that increasingly pervasive connected devices (embedded within, attached to or related to "Things") will support various applications to enhance the awareness and the capabilities of users. For example, users will be able to interact with home automation systems to remotely control the heating or the alarm system.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 207–224.

The possibility of implementing "intelligence" in these pervasive systems and applications has also suggested the definition of "Smart" contexts, where digital and real-word objects cooperate in a cognitive and autonomic way to fulfil specific goals in a more efficient way than basic systems implemented on static rules and logic. While full cognitive and autonomic systems may still be years away, there are many automated processes and automated Internet process which we take for granted every day. So why should the Internet of Things (IoT) require special attention when it comes to privacy, security and governance? Doesn't the established Internet have these matters dealt with sufficiently already, given that through just about every smartphone anywhere there are already a wide variety of sensors capturing information which we share on the Internet e.g. photos, videos, etc.? Why is IoT any different?

Firstly IoT is different because it will be possible and likely that objects will autonomously manage their connections with the Internet or, this will be done upon the request of someone or something remotely. When someone shares a video or a photo taken on their mobile phone over the Internet they "call the shots". With IoT potentially someone else is in charge. For reasons largely similar to this, the topics of privacy, security and governance are very important if not vital to the success of IoT in order to establish and maintain stakeholder trust and confidence. Yes, there is a large overlap between IoT and Internet in many areas pertaining to trust however IoT brings many new specific dimensions too.

The adoption of IoT essentially depends upon trust. Moreover this trust must be established and maintained with respect to a broad group of stakeholders otherwise IoT will face, to some degree or other, challenges which may restrict adoption scope or delay its timing. Note that with social media you make the conscious choice to publish; some IoT applications may adopt the same or similar model but there may be other instances or applications where this will not be the case. This remote control is not essentially bad. For example if you were incapacitated due to an accident it could be advantageous that rescue services would be able to access objects in your environment to locate you or communicate with you. However if these devices were configured to automatically inform your children what presents had been bought or not bought this could spoil much of the excitement of receiving gifts. Facebook's withdrawn Beacon[1] service was accused of this when shoppers'

[1] http://en.wikipedia.org/wiki/Facebook_Beacon

purchases were automatically published on-line resulting in a public outcry and class-action in the US post-holidays (Christmas). There are also potential ethical issues if essential services oblige you to use IoT connected health monitoring devices. Also a number of Internet services are already struggling with the ethical issues of capturing and publishing information affecting 3rd parties where appropriate permissions have not been sought from the 3rd parties involved e.g. Street View.[2] Trust, privacy and governance aspects of IoT rely for the most part upon security [1]. Security in its broadest definitions includes health and wellbeing as well as other forms of protection. These aspects need to be viewed from the perspectives of the majority if not all the principle stakeholder groups and extended to include the relevant influencing and influenced elements of the general environment. Today from the European Commission's perspective the essential focus for security is the protection of health and, the avoidance of potential super-power control being established by enterprises. The objectives are not currently focused upon seeking specific IoT measures to deter cyber-crime, cyber-warfare nor terrorism. Without sufficient IoT security it is highly likely that some applications will more resemble the Intranet of Things rather than the Internet of Things (see [2]) as users seek to place their own proprietary protection barriers and thus frustrating broad interoperability. Many of the device connections to the Internet today more closely resemble the Intranet of Things which differs dramatically from the vision for the Internet of Things, the latter being a much more open and interoperable environment allowing in theory the connection with many more objects and with their multiple IoT compatible devices.

The future of IoT is not only influenced by users. The potential autonomy of IoT or lack of control over IoT by those it impacts will doubtless generate IoT adoption resistance potentially manifested by public protests, negative publicity campaigns and actions by governments. Indeed many IoT foundation technologies have been influenced during the last 10 years by the developing concerns which have been labelled as "threats to privacy". Privacy itself is multi-dimensional. Popular definitions focus upon individual freedoms, or the "right to be left alone". In reality privacy encompasses the interests of individuals, informal groups and including all forms of organizations and is therefore a complex multidimensional subject.

[2] http://en.wikipedia.org/wiki/Google_Street_View

In an age of social media it is interesting to see growing examples of how industry groups and governments begin to encourage greater individual responsibility for protecting our own privacy, defending our virtual representation in order to protect our identity and diminish the challenges of real-world or virtual-world authentications and authorization processes. Through IoT this may become an increasingly 'hard sell' as individuals begin to realize that any efforts individuals take to protect their own identities have almost no influence due to the amounts of information smart objects are collecting and publishing on the Internet. Ideally IoT would provision for flexibility enabling it to be suitably synchronized with the evolution of the development and use of the wider Internet and the general real-world environment.

One specific challenge in IoT is the control of the information collected and distributed by mobile devices which are increasingly small and pervasive like RFID or future micro-nano sensors, which can be worn or distributed in the environment. In most cases, such devices have the capability of being wireless connected and accessible. In this context, the challenge is to ensure that the information collected and stored by micro/nano-RFID and micro/nano sensors should be visible only to authorized users (e.g., the owner or user of the object) otherwise there could be a breach of security or privacy. For example, the owner of a luxury good may not want anybody to know that the luxury good is in a suitcase. The watch in the suitcase may be hidden from view, but it can be easily tracked and identified through wireless communication. In a similar way, the information collected by the body sensors applied to an elderly person should not be accessible by other persons apart from the doctor. Access control mechanisms for these wireless devices should be implemented and deployed in the market, but security and privacy solutions are not easy to implement in micro-nano devices because of the limitations in computing power and storage. At the same time, security and privacy should not hamper business development of micro-nano technologies. Keys management and deployment can also be complex to implement. Trade-offs should be identified and described. These are goals for research activity.

One aspect which often gets overlooked particularly frequently by those of us who entered adulthood before the year 1990 is the importance of the virtual-world. Today the virtual identities of children are as important to them if not more so than their real-world identities. Within the virtual-world there exists most if not all of the things we find in the real-world including objects,

machines, money, etc. IoT includes the real and virtual-worlds and indeed it is capable of establishing an important bridge between the two. This bridge is likely to grow and become more relevant in the life of citizen in the future. New devices like Google Glass or future Intelligent Transportation Systems (ITS) applications in cars will propose "augmented reality" where the integration of digital and real-word information is used to compose sophisticated applications. This trend highlights even more the need for security and privacy, because data breaches in the virtual-world can have consequences in the real-world. In some contexts and applications, security and privacy threats can even become safety threats with more dramatic consequences for the lives of the citizen. As a conceptual example, actuators in the real-world may be set remotely within a "smart house" to provoke fires or flooding.

4.2 Overview of Activity Chain 05 — Governance, Privacy and Security Issues

The European Research Cluster on the Internet of Things has created a number of activity chains to favour close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives. IERC Activity Chain 05 is a cross-project activity focused on making a valued contribution to IoT privacy, security and governance among the EC funded research projects in the area of Internet of Things. As described in [3], the three aspects are closely interlinked "Privacy, security and competition have been identified as the main issues related to IOT Governance, however those issues should not be discussed in a separate or isolated way" (from [3]). In the same reference, it was also highlighted the challenge to define a common agreed definition for Governance of IoT. In a similar way, the concepts of security and privacy do not have a uniform definition in literature even if there is a common agreement on these concepts. Overall, the main objective of the Activity Chain 05 is to identify research challenges and topics, which could make IoT more secure for users (i.e. citizen, business and government), to guarantee the privacy of users and support the confident, successful and trusted development of

the IoT market. In comparison to IoT initiatives in Europe or at a global level (e.g., IGF), Activity Chain 05 does not define government policies but focuses upon research (which could eventually be used to support policies or standardization activities). The following sections provide an overview of some contributions which European Commission funded projects associated with Activity Chain 05 have made to IoT privacy, security and governance.

4.3 Contribution From FP7 Projects

4.3.1 FP7 iCore Access Framework (iCore Contribution)

The iCore cognitive framework is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation in the "Internet of Things", which is called Virtual Object (VO). The virtual objects (VOs) are primarily targeted to the abstraction of technological heterogeneity and include semantic description of functionality that enables situation-aware selection and use of objects. Composite virtual objects (CVOs) use the services of virtual objects. A CVO is a cognitive mash-up of semantically interoperable VOs that renders services in accordance with the user/stakeholder perspectives and the application requirements.

The overall layered approach of the iCore project is provided in Figure 4.1.

The first cognitive management layer (VO level cognitive framework) is responsible for managing the VOs throughout their lifecycle, ensuring reliability of the link to the real world object/entity (e.g., sensors, actuators, devices, etc.). They represent for example, in a logistic related scenario, tracking temperature controlled goods transport, individual goods boxes are represented by VOs the container transported by a truck is a VO as is the truck itself. IoT related applications can interface for different service reasons each of these VOs separately.

The second cognitive management layer (CVO level cognitive framework) is responsible for composing the VOs in Composite VO. CVOs will be using the services of VO to compose more sophisticated objects. In our example, the combination of the truck and the transported goods is represented in the cognitive framework as a CVO.

The third level (User level cognitive framework) is responsible for interaction with User/stakeholders. The cognitive management frameworks will

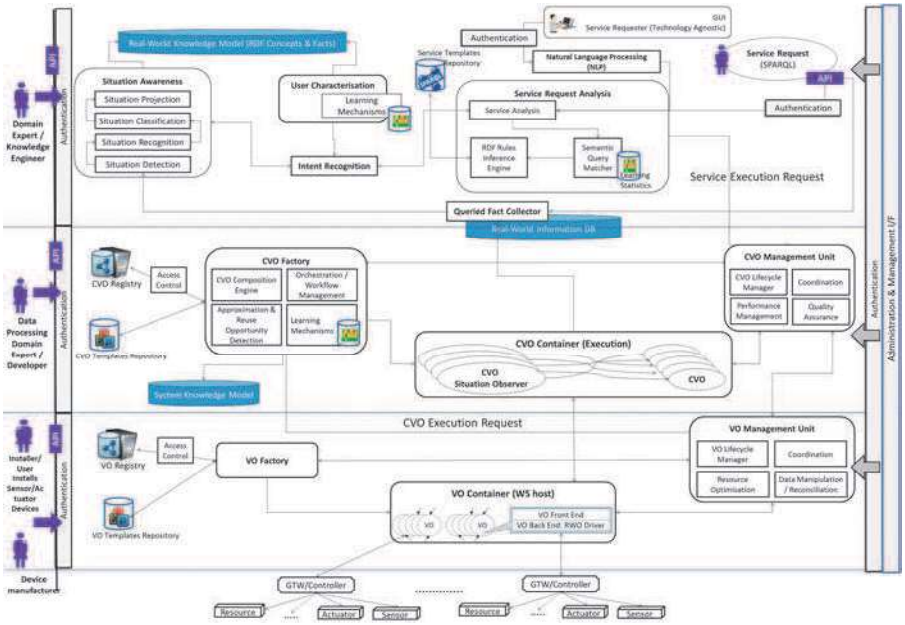

Fig. 4.1 iCore framework.

record the users needs and requirements (e.g., human intentions) by collecting and analyzing the user profiles, stakeholders contracts (e.g., Service Level Agreements) and will create/activate relevant VO/CVOs on behalf of the users.

4.3.2 IoT@Work Capability Based Access Control System (IoT@Work Contribution)

The Internet of Things (IoT) envisages new security challenges, including in the area of access control that can hardly be met by existing security solutions. Indeed, IoT is a more demanding environment in terms of scalability and manageability due both to the potentially unbounded number of things (resources and subjects), the expected most relevant need to support the orchestration and integration of different services, the relevance of short-lived, often casual and/or spontaneous interaction patterns, the relevance of contexts, etc.

In the following we shortly provide a description of the Capability Based Access Control (in the following referred to as CapBAC) system developed

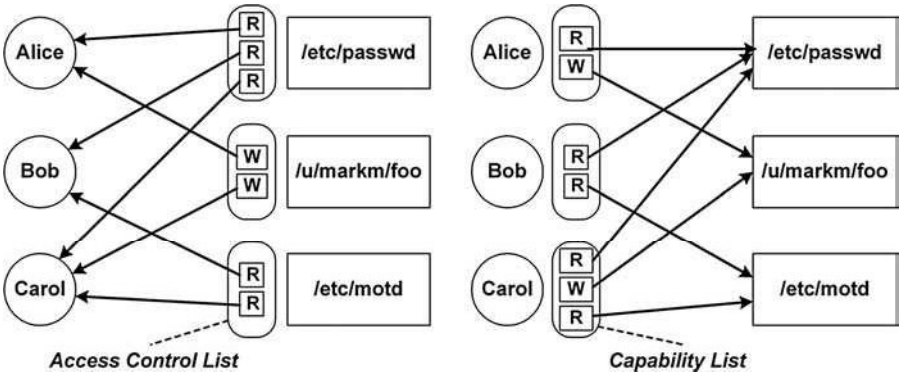

Fig. 4.2 ACL vs Capability-based authorization models.

within the EU FP7 IoT@Work project. The CapBAC is devised according to the capability based authorization model in which a capability is a communicable, unforgeable token of authority. This token uniquely identifies the granted right(s), the object on which the right(s) can be exercised and the subject that can exercise it/them. As depicted in Figure 4.2, a capability based system reverses the traditional approach being now the user in charge of presenting his/her/its authorization token to the service provider, while in a traditional ACL or RBAC system it is the service provider that has to check if the user is, directly or indirectly, authorized to perform the requested operation on the requested resource.

The CapBAC system borrows ideas and approaches from previous works (see [4]) extending and adapting them to IoT requirements and, specifically, the ones envisaged by the IoT@Work project. The CapBAC provides the following additional features that constitute the essential innovation over previous capability based techniques: a) Delegation support: a subject can grant access rights to another subject, as well as grant the right to further delegate all or part of the granted rights. The delegation depth can be controlled at each stage; b) Capability revocation: capabilities can be revoked by properly authorized subjects, therefore solving one of the issues of capability based approaches in distributed environments; c) Information granularity: the service provider can refine its behavior and the data it has to provide according to what is stated in the capability token. Figure 4.3 exemplifies the usage of a capability based access control approach to manage a simple situation: Bob has to go

on holidays and his house needs some housekeeping while he is away. Dave offered to take care of Bob's house for his holiday's period. Bob provides to Dave an access token that: a) Identifies Dave has the only subject entitled to use the token, b) States what Dave can actually perform c) States for how many days Dave can do these actions.

Bob and Dave do not need to establish trust relationships among their authentication and authorizations systems. Bob's house appliance recognizes the access token created by Bob and Dave has only to prove that he is the subject (grantee) identified by the capability token as entitled to do specific housekeeping activities for the holidays period. The above mechanism is very intuitive, easy to understand and easy to use. CapBAC is well suited to manufacturing contexts where there are many subjects, internal (e.g. workers, production supervisors) and external (e.g. suppliers, maintainers), that need access both directly (e.g. via mobile or desktop computing sets) or indirectly (e.g. via application services) to devices, data and services in the manufacturing plant. Most of, if not all, these elements require enforcement of strictly access control policies and finer-graded access control, and, at the same time, a management effort that has to be decoupled from the number of managed resources or subjects, especially when many subjects are external ones.

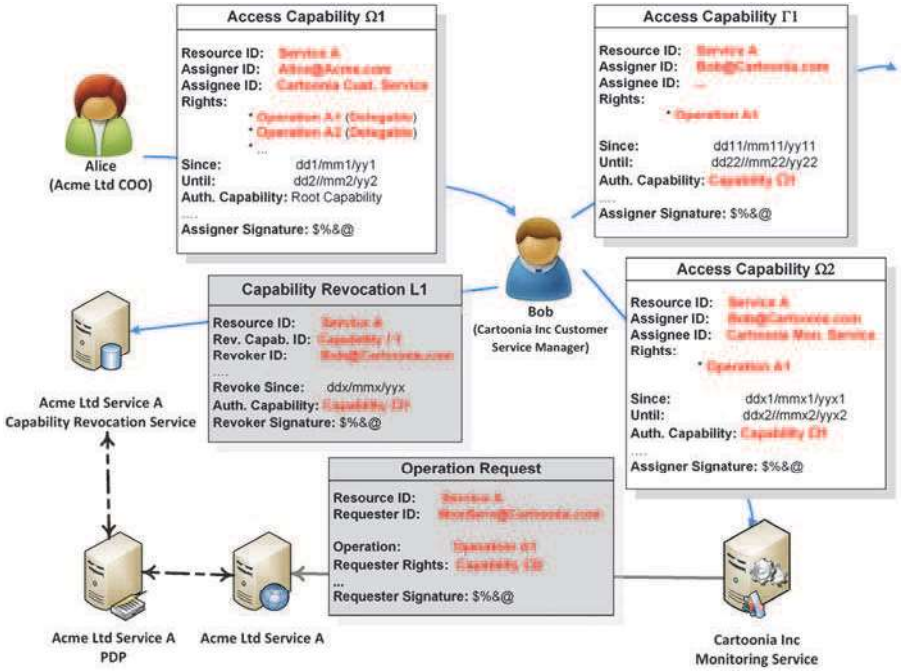

Fig. 4.4 Capability-based authorization architectural components and their interactions.

The CapBAC architectural elements can be shortly characterized as follows (see Figure 4.4):

- The resource object of the capability (Service A in Figure 4.4); it can be a specific data or device, a service or any accessible element that can be univocally identified and/or actable on (like resource);
- The authorization capability that details the granted rights (and which ones can be delegated and, in case, their delegation depths), the resource on which those rights can be exercised, the grantee's identity, as well as additional information (e.g. capability validity period, XACML conditions, etc.). An authorization capability is valid as specified within the capability itself or until it is explicitly revoked;
- The capability revocation is used to revoke one or more capabilities. Like a capability, a capability revocation is a communicable object a subject, having specific rights (e.g. the revoker must be an

ancestor in the delegation path of the revoked capability), creates to inform the service in charge of managing the resource that specific capabilities have to be considered no more valid;

- The service/operation request is the service request as envisaged by the provided service with the only additional characteristics to refer or include, in an unforgeable way, a capability. For example, for a RESTful service, an HTTP GET request on one of the exposed REST resource has to simply include the capability and its proof of ownership to use our access control mechanism;
- The PDP (Policy Decision Point) is a resource-agnostic service in charge of managing resource access request validation and decision. In the CapBAC environment it deals with the validation of the access rights granted in the capability against local policies and checking the revocation status of the capabilities in the delegation chain;
- The resource manager is the service that manages service/access requests for/to the identified resource. The resource manager checks the acceptability of the capability token shipped with the service request as well as the validity and congruence of the requested service/operation against the presented capability. It acts as an XACML Policy Enforcement Point (PEP) which consider the validation result of the PDP;
- The revocation service is in charge of managing capability revocations.

4.3.3 GAMBAS Adaptive Middleware (GAMBAS Contribution)

The GAMBAS project develops an innovative and adaptive middleware to enable the privacy-preserving and automated utilization of behaviour-driven services that adapt autonomously to the context of users. In contrast to today's mobile information access, which is primarily realized by on-demand searches via mobile browsers or via mobile apps, the middleware envisioned by GAMBAS will enable proactive access to the right information at the right point in time. As a result, the context-aware automation enabled by the GAMBAS middleware will create a seamless and less distractive experience for its users while reducing the complexity of application development.

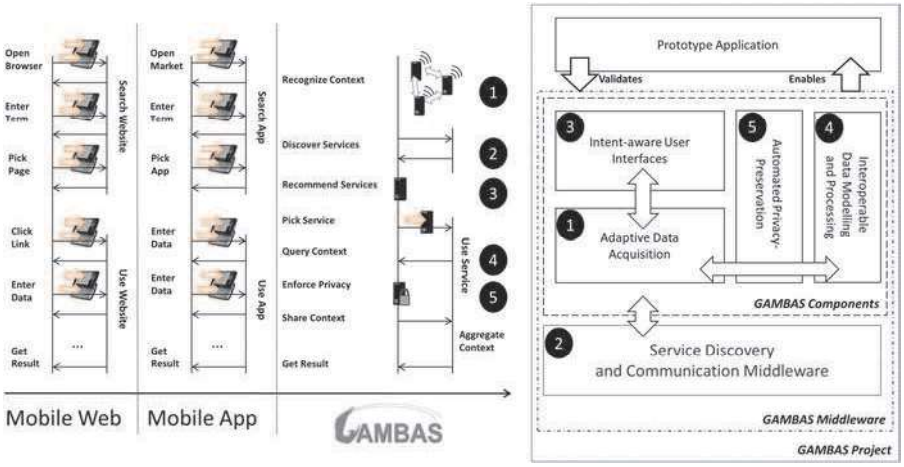

Fig. 4.5 GAMBAS middleware.

As indicated in Figure 4.5, the core innovations realized by GAMBAS are the development of models and infrastructures to support the interoperable representation and scalable processing of context, the development of a generic, yet resource-efficient framework to enable the multimodal recognition of the user's context, protocols and mechanisms to enforce the user's privacy as well as user interface concepts to optimize the interaction with behaviour-driven services.

From a security and privacy perspective, the developments in GAMBAS are centred on a secure distributed architecture in which data acquisition, data storage and data processing are tightly controlled by the user. Thereby, security and privacy is based on the following elements.

- Personal acquisition and local storage: The primary means of data acquisition in GAMBAS are personal Internet-connected objects that are owned by a particular user such as a user's mobile phone, tablet, laptop, etc. The data acquired through the built-in sensors of these devices is stored locally such that the user remains in full control. Thereby, it is noteworthy that the middleware provides mechanisms to disable particular subsets of sensors in order to prevent the accumulation of data that a user may not want to collect and store at all.

- Anonymised data discovery: In order to enable the sharing of data among the devices of a single user or a group of users, the data storages on the local device can be connected to form a distributed data processing system. To enable this, the GAMBAS middleware introduces a data discovery system that makes use of pseudonyms to avoid revealing the user's identity. The pseudonyms can be synchronized in automated fashion with a user defined group of legitimate persons such that it is possible to dynamically change them.
- Policy-based access control: To limit the access to the user's data, the networked data storages perform access control based on a policy that can be defined by a user. In order to reduce the configuration effort, the GAMBAS middleware encompasses a policy generator tool that can be used to derive the initial settings based on the user's sharing behaviour that he exhibits when using social services.
- Secure distributed query processing: On top of the resulting set of connected and access-controlled local data storages, the GAMBAS middleware enables distributed query processing in a secure manner. Towards this end, the query processing engine makes use of authentication mechanisms and encryption protocols that are bootstrapped by means of novel key exchange mechanisms that leverage the existing web-infrastructure that is already used by the users.

4.3.4 IoT-A Architecture (IoT-A Contribution)

Security is an important cornerstone for the Internet of Things (IoT). This is why, in the IoT-A project, we deemed as very important to thoroughly address security and privacy issues in various aspects. A set of requirements based on the input of external and internal stakeholders was used as a basis for the identification of the mechanisms and functionalities that guarantee user data privacy and integrity, user authentication, and trustworthiness of the system.

These functionalities were analysed and orchestrated in Functional Groups (FG) and Functional Components (FC) in the frame of WP1. High-level PS&T specifications were integrated in the frame of the IoT-A Architectural Reference Model (ARM) and then passed to vertical WPs dealing with communication protocols (WP3), infrastructure services (WP4) as well as hardware

aspects (WP5). Due to the highly heterogeneous environment provided by the IoT and the huge number of connected, (autonomous) devices foreseen by analysts, a strong focus was placed on scalability and interoperability.

The ARM document [5] paves the way for understanding and adopting the open architecture of IoT-A, as well as provides the overall definition of IoT security, privacy and trust design strategies that we adopted. Then, in WP3 we analysed the security of communication in the peripheral part of the IoT and its impact on the overall communication architecture. In this context we investigated HIP and HIP-BEX protocols, as well as considered issues like mobility, collaborative key establishment, and securing network entry with PANA/EAP.

Then, within the framework of WP4 [6] we developed a secure resolution infrastructure for IoT-A. It ensures privacy and security for the resolution functions as well as offers the basis for other security functionalities outside the resolution infrastructure. It controls the access to IoT resources, real world entities, and to the related information including their respective identifiers. In addition, the resolution infrastructure provides also support for pseudonymity: A user does not need to reveal his/her identity when using an IoT resource or a higher-level service. To achieve all this, various security components were developed (see Figure 4.6). They deal with authorization and authentication, key exchange and management, trust and reputation, and identity management.

Finally, WP5 deals with privacy and security at device level. In particular, it describes the mechanisms needed to authenticate RFID devices and to provide confidentiality of the communication between reader and tag. The PS&T features of the IoT-A architecture will be tested in the forthcoming IoT-A eHealth Use Case.

4.3.5 Governance, Security and Privacy in the Butler Project (Butler Contribution)

The goal of the BUTLER project is the creation of an experimental technical platform to support the development of the Internet of Things. The main specificity of the BUTLER approach is its targeted "horizontality": The vision behind BUTLER is that of a ubiquitous Internet of Things, affecting several

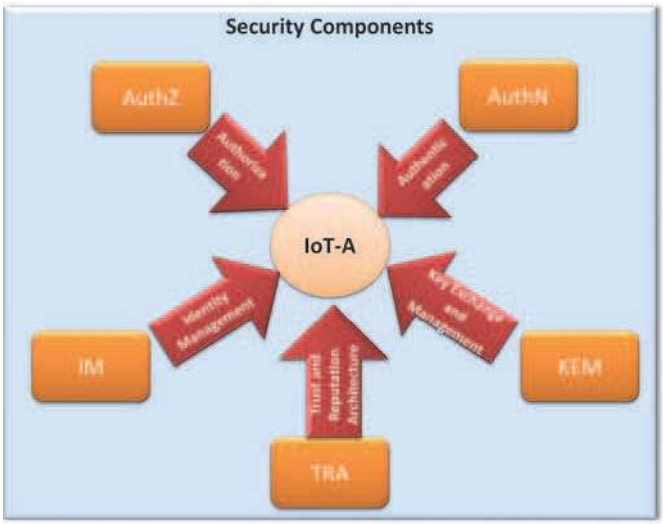

Fig. 4.6 Components for privacy and security in the IoT-A resolution infrastructure.

domains of our lives (health, energy, transports, cities, homes, shopping and business) all at once. The BUTLER platform must therefore be able to support different "Smart" domains, by providing them with communication, location and context awareness abilities, while guaranteeing their security and the privacy of the end users. The issue of security and privacy is therefore central in the BUTLER project and develops in several requirements, the main requirements relate to:

- Standard issues of data security, both at data storage level as at data communication level exists in IoT application. The diversity and multiplicity of the "things" connected by the internet of things, and of the data exchanged further amplifies and complicate these requirements.
- The application enabled by the Internet of Things may pose additional privacy issues in the use that is made of the data. From the collection of data by the applications (which should be conditioned by an "informed consent" agreement from the user), to the profiling, exchange and sharing of these data necessary to enable true "context awareness".

Data technical protection[3] mechanisms include two major aspects. One is the protection of the data at data storage, the other one the protection of the data at communication level. The protection of data at communication level is one the major area of research. Many communication protocols implement high level of end-to-end security including authentication, integrity and confidentiality. At communication level, the major issue is the deployment process of the security keys and the cost of the required hardware and software environment to run the security algorithms in efficient and secure way.

However, Privacy and Security do not only refer to security of the exchange of data over the network, but shall also include: (a) Protection of the accuracy of the data exchanged, (b) Protection of the server information, (c) Protection of the usage of the data by explicit, dynamic authorization mechanisms, (d) Selected disclosure of Data and (e) The implementation of "Transparency of data usage" policies.

The BUTLER project also addresses the Security and Privacy challenges from the point of view of their implication on business models. To specify the horizontal IoT platform envisioned in BUTLER, the project started from the gathering and analysis of the requirements from up to 70 use cases. The analysis of these use case not only produced requirements for the specification of the platform but also valuable information on the potential socio-economic impact of the deployment of an horizontal IoT and on the impact on the associated business models.

If treated accordingly, the ethics and privacy issues transforms from a threat to an opportunity. Better understanding of the service by the user increase acceptance and create trust in the service. This trust becomes a competitive advantage for the service provider that can become a corner stone of his business model. In turn the economic interest of the service providers for ethics and privacy issues, derived from this competitive advantage, becomes a guarantee for the user that his privacy will be respected. The BUTLER project research on the implication of the Ethics, Privacy and Data security on the business models and socio economic impact will be published in Deliverable 1.4 (May 2013) and Deliverable 1.3 (September 2014).

[3] An exhaustive study of the security enabling technologies is available in "D2.1 Requirements, Specification and Security Technologies for IoT Context-aware network". http://www.iot-butler.eu/download/deliverables

The involvement of end users in proof of concepts and field trials is another specificity of the BUTLER project. The end user involvement is key to validate not only the technical qualities of the BUTLER platform (technology feasibility, integration and scaling) but also to assess the perception of end user and their acceptance of the scenario envisioned for the future "horizontal" IoT.

However the involvement of end user in the scope of the project requires handling their data and privacy concerns carefully. The detailed specification of the field trials and proof of concept is described in Deliverable 1.2, (scheduled for end of May 2013). The following issues must be considered in the organization of end user involvement: (a) Technical security mechanisms must be set up to ensure the security and privacy of the participants. This involves secured data communication and storage, and in the scope of the BUTLER project is addressed by the enabling security technologies developed and integrated in the BUTLER platform; (b) The participants must be well informed of the scope and goal of the experiment. In the case of BUTLER, this involves specific efforts to explain the scope and goal of the project to a larger public; (c) The consent of the participants must be gathered based on the information communicated to them. The consent acknowledgment form must remind the participants of their possibility to refuse or withdraw without any negative impact for them; (d) finally both a feedback collection and a specific complaint process have been designed to offer the possibility to the participants to raise any issue identified.

4.4 Conclusions

IoT applications and supporting stakeholders can all mutually benefit from the establishing of a trusted IoT. Trust means establishing suitable provisions for privacy, security and governance. To put in place and maintain trust means fulfilling today's needs while providing sufficient future provisions to meet naturally evolving stakeholder requirements and expectations. Consensus necessary for the formation of successful standards and guidelines can only come through dialogue. Activity Chain 05 provides such a platform for information exchange and mutual understanding as well as in providing valued leadership. The research projects within Activity Chain 05 all contribute to advancing IoT adoption, some having universal IoT application value while others provide significant enhancements to specific IoT application groups. Making this

landscape clearer, identifying the gaps for further research as IoT develops and, assisting the progression of research towards standardization and adoption remain the principle challenges for Activity Chain 05. Another role for Activity Chain 05 is raising awareness and promoting adequate consideration of IoT privacy, security and governance within the other Activity Chains of the IERC and the wider stakeholder community.

References

[1] Roman, R., Najera, P., Lopez, J., "Securing the Internet of Things," *Computer* , vol. 44, no. 9, pp. 51, 58, Sept. 2011.

[2] Zorzi, M., Gluhak, A., Lange, S., Bassi, A., "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 44, 51, December 2010.

[3] Final Report of the EU IOT Task Force on IOT Governance. Brussels, November 14, 2012.

[4] Gusmeroli, S., Piccione, S., Rotondi, D., "IoT Access Control Issues: A Capability Based Approach," in *Proceedings of 6th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2012)*, pp. 787–792, July 2012.

[5] Carrez, F. (ed), Converged architectural reference model for the IoT, available at http://www.iot-a.eu/public/public-documents. Last accessed 10 May 2013.

[6] Gruschka, N., Gessner, D. (eds.), Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, available at http://www.iot-a.eu/public/public-documents. Last accessed 10 May 2013.