Future Internet **2012**, *4*, 1016-1025; doi:10.3390/fi4041016

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Supporting Trust and Privacy with an Identity-Enabled Architecture

Amardeo Sarma * and Joao Girao

NEC Laboratories Europe, Kurfürstenanlage 36, 69115 Heidelberg, Germany;
E-Mail: joao.girao@neclab.eu

* Author to whom correspondence should be addressed; E-Mail: sarma@neclab.eu;
Tel.: +49-6221-4342-144; Fax: +49-6221-4342-155.

Received: 1 September 2012; in revised form: 24 September 2012 / Accepted: 25 October 2012 / Published: 19 November 2012

Abstract: Cost reduction and a vastly increased potential to create new services, such as via the proliferation of the Cloud, have led to many more players and "end points". With many of them being new entrants, possibly short-lived, the question of how to handle trust and privacy in this new context arises. In this paper, we specifically look at the underlying infrastructure that connects end-points served by these players, which is an essential part of the overall architecture to enable trust and privacy. We present an enhanced architecture that allows real people, objects and services to reliably interact via an infrastructure providing assured levels of trust.

Keywords: identity; privacy; trust; virtual identity; virtual infrastructure session; identity aggregator; cloud

---

1. Introduction

A typical current development is the move to the Cloud, driven by the goal of saving cost or substantially enhancing the number and kinds of services offered. While the existing players can reduce cost, new entrants use services with a rich set of capabilities that they could not afford before. This commoditization of services has led to an increasing number of active players, including so-called "prosumers". A whole new community seeks to provide new and niche services. At the same time, we have seen a whole range of new network architectures and approaches appear.

This has however come at a cost: moving computation and storage outside the domain of the company, or even from the average user's home, means that we need to "trust" that those running these services behave as is expected and do not misuse the outsourced resources. There will be a wide range of trust levels, including both established players with a track record and initially untrusted new entrants, who may come and go quickly. Even these must have an opportunity to succeed in the future digital environment. New architectures to handle trust in a heterogeneous environment will be needed. In this context, Security, privacy, trust and identity are strongly interrelated.

The paper presents an enhanced security, privacy and trust architecture supporting the flexible integration of independent third parties building upon work done in the EU projects SWIFT [1] and Daidalos [2], in particular its concepts of Virtual Identity and Identity Aggregator or Broker, but going beyond using new approaches which support stronger notions of trust. It deals with both infrastructure and service aspects. The architecture supports an identity-enabled Future Internet and encompasses both control and management functions. The target of the architecture is to make real people, objects (things), as well as services the end-points of communications. The heterogeneous infrastructure, to which these end-points are connected, should support awareness and control of trust levels, as well privacy, and thus support the privacy and trust levels of services and applications.

People are now used to using digital identities to access networks and services, either via user name and password combinations, or via (U)SIM cards. Not quite as common is the use of digital certificates. With the upcoming Cloud environment, the number of distributed digital identities per person is exploding and becoming unmanageable. This is accompanied by a fragmentation both regarding the technologies used and underlying methods of use. From the usability point of view, we need to allow applications using a specific identity solution and technology to connect to applications and domains that use different identity technologies. These issues have been addressed e.g., by the identity aggregator approach in SWIFT.

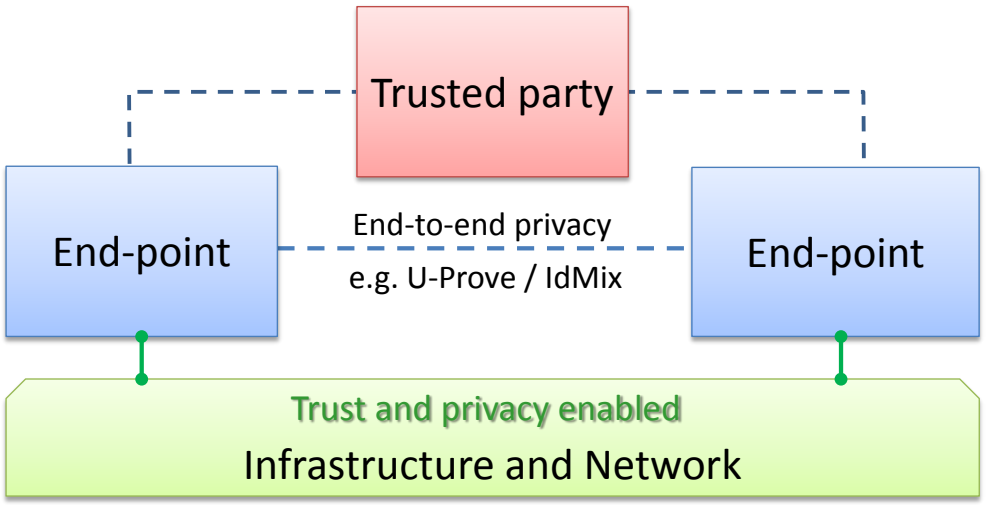
The paper is structured as follows. Section 2 shows the general problems that exist today and shows link to how related work has addressed the problem. Section 3 shows the proposed architecture. Section 4 illustrates an example scenario. Section 5 concludes the paper with a summary.

2. State-of-the-Art and Related Work

To be able to ensure reliable and trusted communication and use of services, we need to be able to control what happens both in the infrastructure and for the end points, services for example. Regarding the infrastructure, trust has been focused on security measures, e.g., dealing with securing individual channels via IPSEC or through end-to-end SSL encryption. Network Address Translation (NAT) has addressed network autonomy and security by decoupling the internal network from the Internet [3]. Approaches such as HIP (Host Identity Protocol) have separated identification and identities from the addresses (locators) that point to where a device is attached. HIP uses cryptographic host identifiers with a global name space between the IP and transport layers [4]. The EU FP6 Ambient Networks project is based on such a separation of locator, identifier and administrative domains [4,5]. Related approaches are PONA [6] and MILSA [7]. Some have suggested completely eliminating layering [8] to overcome layering violations of the TCP/IP architecture. Others adopt a content- or information-centric approach [9,10] connecting information consumers with information producers. Building on this work,

our goal on the infrastructure side is to enable reliable Virtual Infrastructure Sessions (VIS) connecting two or more end-points of the communication, represented by virtual identities as defined in SWIFT and Daidalos, to support privacy, with an architecture that allows us to control and understand trust related to the infrastructure and the end-points. We have not specifically addressed solutions, such as U-Prove and IDMix from the EU projects ABC4Trust or Prime/Primelife. These address privacy in the context of services and applications, not the network or the infrastructure. They may thus be seen as complementary or orthogonal approaches to the one described here, see Figure 1.

Figure 1. Supporting trust and privacy via the infrastructure.



Much work including in standards has been done on the identity side of things. ITU-T Recommendation (X.1250) on global identity management [11] defines identity as the "Representation of an entity (or group of entities) in the form of one or more information elements, which allow the entity(s) to be uniquely recognized within a context to the extent that is necessary (for the relevant applications)." For privacy, we need to handle (and restrict) Personally Identifiable Information (PII), which is "the information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person)" [12]. More on the application and end-point side, federated identity management systems are based on the SAMLv2 [13] Liberty Alliance [14] and Shibboleth [15] models, that support identity management, authentication and authorization. We differentiate between an identifier and an identity that includes attributes of the entity to enable communication between endpoints based on identifiers, possibly pseudonyms, as well as attributes, such as connecting with any entity with the property representative of bank x (not necessarily human). The use of pseudonyms and attributes help making identification more difficult.

3. Proposed Architecture

The Internet was designed as a support infrastructure to allow people to communicate freely when the computer was on its way to become the preferred tool to handle all sorts of information about people, public records, enterprise data, medical, things. Barriers to finding information have been torn

down, and the Internet has moved to the center of business, social, educational, cultural and global issues.

Along the way, we have neglected why we needed an Internet in the first place: for people to communicate. The Internet became the storage place for information, the infrastructure to where one plugs to and, inevitably, the bottleneck of our communications infrastructure. Because we see this Internet as an abstract entity to where one "plugs-in", it has become increasing difficult to scale services to the billions of users and their digital entities that the Internet will hold and serve.

We propose a different approach to the Internet based on previous work [16–19]. If we go back to how we started this discourse, the Internet is for people to communicate. They may be communicating in real-time or over-time. They may be using writing, speech, video, pictures, documents which include graphs and tables. They may be doing so in a business context, social context, for entertainment, for medical reasons. They even may be doing all these things at once, but all the information, data, they put in will only make sense in two contexts: their own and whoever receives it. Our approach is to design a Next Generation Internet, one which conceptually starts at the user consuming a service, identified and addressed by a virtual identifier acting as a portal to all the services the current Internet supports, and more. Our approach is to create a scalable digital communication infrastructure which mirrors the structure we have always had in the real world: people talking to people, objects, and in general digital identities communicating with each other.

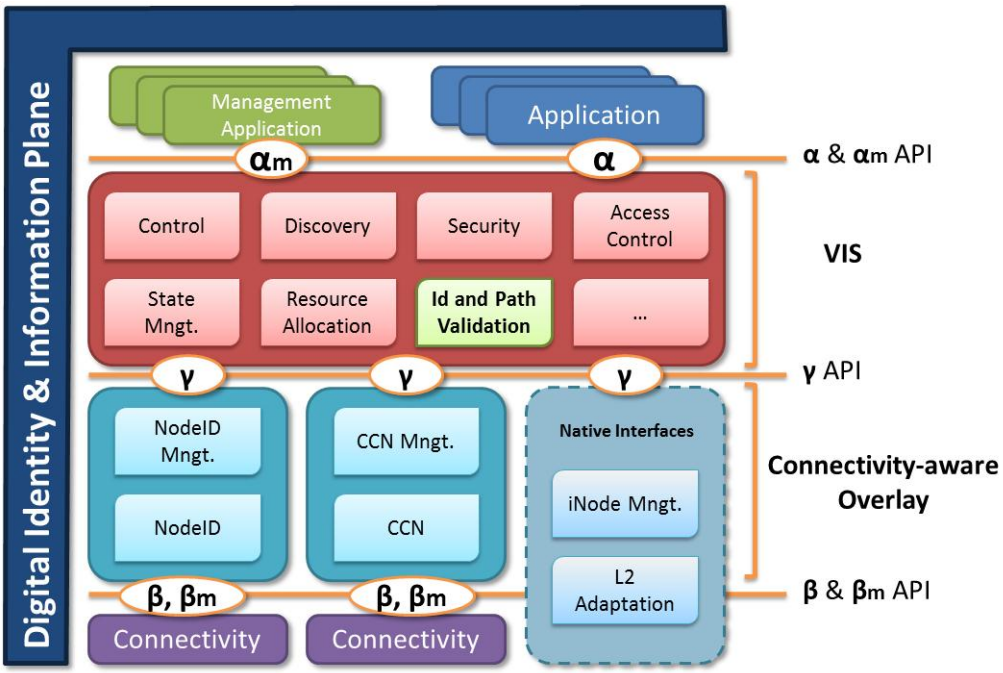
To bind these concepts together, we have created a concept called Virtual Infrastructure Sessions (VIS). A VIS is a channel over which one or more (virtual) identities communicate. It encompasses all the levels from application to transport necessary to transmit bits from one identity to the other and also the purpose for that communication. We distinguish between three parts: the virtual identities, which mark the endpoints and support privacy, the intent, which determines the purpose for the communication and the VIS, which is the channel over which communication is achieved. The intent is an abstraction of what some entity wants to do, such as a user wanting to make a phone call to some other user, or a user wanting to download some specific information, which brings the virtual identity and the VIS together for a specific purpose.

In most ways, the VIS can be seen as having the same properties as an identity. It can be identified, most times differently depending on the administrative domain and the level at which it is being addressed, it can be manipulated by a control layer, which permits functions such as connection establishment, the addition of identities to the communication and the query of parameters of the communication to be performed and it aggregates the same properties of security and privacy normally attributed to identities: authentication, authorization, minimum disclosure and trust.

3.1. Architecture Description

For us to get a better understanding of how the concepts of Identity and VIS can be instantiated in the existing Internet architecture, we propose the following separation of functions into three levels: Application, VIS and connectivity. Figure 2 describes the proposed alignment for these interfaces or APIs, which builds on ideas developed for MANA [20].

Figure 2. Future Internet identity architecture using Virtual Infrastructure Sessions.



The first step for session establishment is the discovery of the identity or identities we want to communicate with. Much like the Internet today, one can assume that discovering the domain name of a service endpoint can be done through the use of search engines or through assumed prior knowledge (e.g., google.com). The domain can then be used to identify a specific identity in the domain using a lookup mechanism such as a directory. We believe that for the purposes of the architecture, such mechanisms can be varied and heterogeneous, which is also why we do not offer further details about its instantiation in this paper. It is important at this stage that the result obtained from the lookup be compatible with the Identity Management (IDM) system. This is usually not a problem since most IDM systems are identifier agnostic. Once the identifier is obtained, a second discovery mechanism, at the connectivity layer can be used to find a path or route to the endpoint based on the context of the communication.

3.2. Virtual Infrastructure Session

The VIS is created as soon as the endpoints and intention are known. It offers a distributed querying and control layer distributed across the different domains which functions like an Identity Management system. Identifiers are mapped according to the domain and layer of the request. A URL might become an IP or a MAC address depending on the layer at which the data is indexed. The advantage of this system is that it is agnostic to the protocols offering a general purpose API to deal with data about a communication at all levels. In sum, a VIS has an identity of its own. Below is a description of the interfaces and their main functions:

Application (Alpha) API: The alpha API provides applications with the controls to create new VISs, populate them and use them to transport data at an application level. The API uses the identities and intents, together with the context of the access to provide discovery and session setup.

Control (Gama) API: This API provides VIS with a mechanism to interact with domain specific control layer. For example, it could be used to setup QoS or pinholes to allow for traffic to traverse across domains. Since our architecture could potentially use many different types of transport, the API ensures compatibility between Internet, Content Centric Networking, NodeID, *etc.* In some extreme cases, there might be no Beta API since the transport layer supports this architecture natively.

Transport (Beta) API: In cases where transport is not native, this API ensures the communication and abstraction between the different control layer protocols and the actual transport.

Each of these APIs vary from simple to complex depending on the functions to be supported, and are designed to be open for future extensions. The intention is to reuse existing protocols and standards as far as possible and only extend these when needed. The overall architecture may thus also be seen as a framework that encompasses the existing state of the art.

3.3. Privacy and Trust Support

One of the key motivations behind this architecture has been to enable privacy and trust. This done via two means:

Identity Validation Component: The VIS has an identity validation component owned by specific provider that validates identities, which may not go as far as identification, but may be content with the validation of attributes or claims that the end-points must fulfill. The provider is thus able to assess whether or not the end-points are valid, thus providing an important barrier to phishing attacks. Of course, this depends on the provider itself being trustworthy and certified. This validation component will communicate via the Alpha API, is designed to communicate with a wide range of Identity Management systems, and is open to enhancements to cope with new developments in Identity Management. Validations are performed using Identity Management protocols that guarantee privacy e.g., using pseudonyms. To each identity in a domain, a different local identifier is used and mapped at the borders using a name resolution mechanism built into the IDM platform. A partial recovery of the data and identification of the user can be perform by the correlation of the pseudonyms at the different domains, which allows for legal interception and fulfills other regulatory requirements without compromising privacy on the day to day operations. Attribute based access control will support the setting up of connections.

Path Validation Component: Not all the routers and nodes that are used by the VIS are necessarily owned by the provider of the VIS. This component will communicate via the Gamma API and need to check the identity of the nodes and their trustworthiness. As above, Identity Management protocols will be used to negotiate the security parameters related to the VIS for each particular communication. Identities of the network entities of a VIS, and their policies, are parameters that will need negotiation. Based on these results, the setup of the VIS will adjust which nodes have access to the transported data including end-point addresses, and which do not. As the internal end-points of the VIS themselves may not be (fully) trusted, the user will be notified about the level of trust that should be assumed and what levels of assurance exist.

For both the trustworthiness of end-points of a communication, e.g., services, as well as for the trustworthiness of internal nodes and routers, hierarchical schemes, such as via certification authorities, as well as reputation systems may be used, such as those proposed in [21]. Security functions will

ensure the necessary privacy, and prevent an uncontrolled disclosure of identity data. Cryptographic techniques regarding private information retrieval may be applied [22,23].

While we have focused on the privacy and trust components, others will be supported, see Figure 1, such as dealing with access control and resource allocation, both of which are not dealt with here.

3.4. Security Enforcement

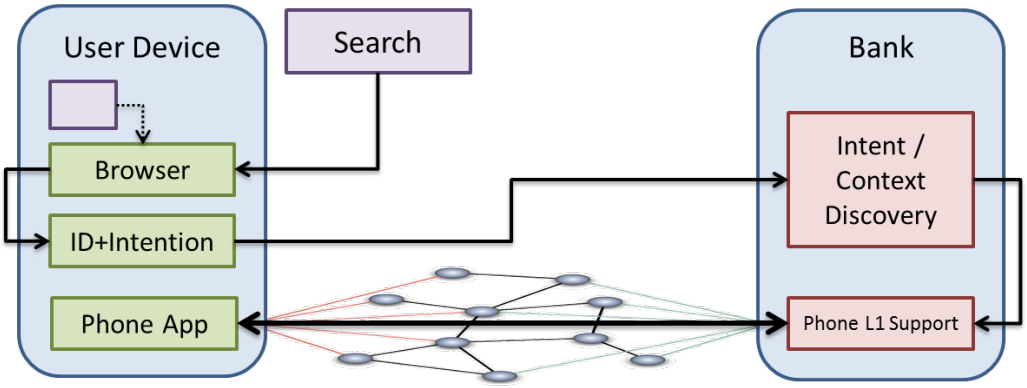
The VIS provides the interfaces both for the network, service and discovery components. In this architecture design privacy is intrinsically dealt with by creating the separation, or in some cases distributed, of the knowledge of identities, intents, networks and service operations. In this architecture, different layers behave independently but share a VIS. In addition to its role of providing a privacy layer, the VIS is also a point for policy enforcement and allows for fine grain control on discovery and access to information about the VIS based on identity or intent information. For example, the VIS can be setup in a way that the separation of data ensures the communication between participants remains anonymous; while preserving the right to be part of the VIS through the identity layer (and associated credentials).

4. Illustration of the Architecture Using a Simple Scenario

Let us imagine the simple scenario depicted in Figure 3, where a user would like to contact his bank. Currently, this would entail searching for the bank URL, navigating the site, browsing the website for the correct contact information and then starting a new application to contact either via email or phone. With our proposed architecture, the following steps would be taken after the user declares his intentions and communication partner:

1. The identity of the bank is discovered using a search engine or through prior knowledge of a domain name or URL. Thanks to the link between the user's identity and the context of the communication, the bank identity might actually be retrieved from the user's profile. In this case, the user would only have to reference "bank" or any other generic identifier for the endpoint.
2. The bank domain is contacted by the discovery process to resolve the contact endpoint based on the context and intention: e.g., if the intention is to perform a voice call, the identity of the closest branch level 1 support would be returned.
3. The VIS is created and the identities of the endpoints, together with a set of local domain identifiers, are provided at the domain level of the communicating entities.
4. At the domain level, routes or paths are configured to connect to the next domain until the identifier corresponding to the other endpoint is reached. Each step involves the VIS APIs to ensure the data is accessible by all levels and domains (depending on authorization).
5. The endpoints establish a secure channel based on the keys corresponding to the identities and, if necessary, using the IDM system as a trust bridge.
6. Now the service is ready to be provisioned and the VIS can be adjusted to support any number of future applications or identities related to the intent.

Figure 3. Simple scenario.



In a similar way, this mechanism can be used to contact any other number of entities simultaneously focusing on the endpoints and on the channel for the communication as a part of the identity of the participants. Also, the approach is not restricted to the entities being human. Objects or things may want to set up a communication completely without human intervention, with "intentions" that have been programmed into them. The same applies for autonomous software entities and services.

5. Conclusions

A large amount of effort has been put into identity management and the federation of such systems, and a large number of solutions exist today. However, some of the fundamental problems related to being able to trust both the infrastructure and the end-points at the other end remain inadequately addressed. For many applications and scenarios, this may be the blocking factor that differentiates success from failure. We have presented an architecture based on Virtual Infrastructure Sessions (VIS) that allows for a flexible build-up of a trusted connectivity between 2 or more end-points. The architecture provides a more controlled way of ensuring reliable connectivity without linking a lot of the data or identities, supporting privacy, while at the same time ensuring via security mechanisms that control the VIS that the sessions can be trusted and are not susceptible to be hijacked via man-in-the-middle attacks. Thus both privacy and trust are supported.

This paper has consolidated some of the findings of the EU projects SWIFT and Daidalos and enhanced the architectures developed there to cope with supporting trust and privacy from the infrastructure. It goes well beyond the contributions of these projects, since it takes a more consistent view on how identities can be used beyond the endpoints, and establishes a perspective on how communication can be perceived both from the endpoints and the nodes in between. Potentially, this approach can lead to more intelligent networks with reduced control messaging and a more coherent cross-application protocol stack. We will work on validating this architecture via new projects, such as EU FP7 ATTPS, which will be building the infrastructure for trials. In this context, we will also need to focus on a range of possible attack scenarios to ensure that the claim of support of privacy and trust is actually validated.

Acknowledgments

We express our thanks to the partners of the SWIFT and DAIDALOS projects, where a lot of the groundwork was done. We also thank the colleagues with whom we have collaborated with in writing several EU Call 8 proposals, where we gained useful insight into the challenges of providing privacy and trust of the Future Internet. In particular, we would like to thank Antonio Skarmeta, University of Murcia, for many fruitful discussions in the context of developing such new architectures.

References

1. SWIFT Project. Available online: http://www.ist-swift.org (accessed on 8 November 2012).
2. Daidalos Project. Available online: http://www.ist-daidalos.org (accessed on 3 May 2011).
3. Srisuresh, P.; Holdrege, M. IP Network Address Translator (NAT) Terminology and Considerations. Available online: http://tools.ietf.org/html/rfc2663 (accessed on 29 October 2012).
4. Moskowitz, R.; Nikander, P. Host Identity Protocol (HIP) Architecture. Available online: http://tools.ietf.org/html/draft-ietf-hip-rfc4423-bis-04 (accessed on 29 October 2012).
5. Ahlgren, B.; Arkko, J.; Eggert, L.; Rajahalme, J. A Node Identity Internetworking Architecture. In *Proceedings of 25th IEEE International Conference on Computer Communications*, Orlando, FL, USA, 23–29 April 2006.
6. Paul, S.; Jain, R.; Bowman, M. A Vision of the Next Generation Internet: A Policy Oriented Perspective, British Computer Society International Conference on Visions of Computer Science. Available online: http://www.cs.wustl.edu/~jain/papers/ftp/bcs08.pdf (accessed on 29 October 2012).
7. Pan, J.; Paul, S.; Jain, R. MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet. In *Proceedings of Global Telecommunications Conference*, New Orleans, LA, USA, 30 November–4 December 2008.
8. Braden, R.; Faber, T.; Handley, M. From protocol stack to protocol heap: Role-based architecture. *ACM SIGCOMM Compt. Commun. Rev.* **2002**, *33*, 17–22.
9. Jacobson, V.; Smetters, D.K.; Thornton, J.D.; Plass, M.F.; Briggs, N.; Braynard, R. Networking Named Content. In *Proceedings of Fifth ACM International Conference on Emerging Networking EXperiments and Technologies*, Rome, Italy, 1–4 December 2009.
10. Ahlgren, B.; D'Ambrosio, M.; Dannewitz, C.; Marchisio, M.; Marsh, I.; Ohlman, B.; Pentikousis, K.; Rembarz, R.; Strandberg, O.; Vercellone, V. Design Considerations for a Network of Information. In *Proceedings of ACM International Conference on Emerging Networking EXperiments and Technologies*, Madrid, Spain, 9–12 December 2008.
11. Baseline Capabilities for Enhanced Global Identity Management Trust and Interoperability; ITU-T: Geneva, Switzerland, 2009.
12. ITU-T. NGN Identity Management Framework. Available online: http://www.itu.int/rec/T-REC-Y.2720-200901-I (accessed on 29 October 2012).
13. OASIS SAML 2.0 profile of XACMLv2.0. Available online: https://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf (accessed on 1 November 2012).

14. Liberty Alliance Project. *Liberty ID-WSF Web Services Framework Overview*, Version: 2.0. Available online: http://www.projectliberty.org/specifications__1 (accessed on 8 November 2012).
15. Nanda, A.; Jones, M.B. Identity Selector Interoperability Profile v1.5. Available online: http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2/Identity_Selector_Interoperability_Profile_V1.5.pdf (accessed on 10 July 2008).
16. Sarma, A.; Girao, J. Identities in the Future Internet of Things. In *Wireless Personal Communication*; Springer: Berlin, Germany, 2009; pp. 353–3664.
17. Girao, J.; Sarma, A. IDentity Engineered Architecture (IDEA). In *Towards the Future Internet*; IOS Press: Amsterdam, The Nertherlands, 2010; pp. 85–93.
18. Gomez-Skarmeta, A.F.; Martinez-Julia, P.; Girao, J.; Sarma, A. Identity based Architecture for Secure Communication in Future Internet. In *Proceedings of the 6th ACM Workshop on Digital Identity Management*, Chicago, IL, USA, 8 October 2010; ACM: New York, NY, USA, 2010; pp. 45–48.
19. Martinez-Julia, P.; Gomez-Skarmeta, A.F. Using identities to achieve enhanced privacy in future content delivery networks. *Comput. Electr. Eng.* 2012, *38*, 346–355.
20. Galis, A.; Abramowicz, N.; Brunner, M. Position paper Management and Service-Aware Networking Architectures (MANA) for Future Internet, System Functions, Capabilities and Requirements. Available online: http://www.future-internet.eu/fileadmin/documents/madrid_documents/sessions/MANA-Position_Paper-V5.0.pdf (accessed on 1 November 2012).
21. Gomez Marmol, F.; Martínez Pérez, G. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Comput. Stand. Interfaces* **2010**, *32*, 185–196.
22. Yoshida, C.; Sekino, T.; Shigetomi, R.; Otsuka, A.; Imai, H. Practical Searching over Encrypted Data by Private Information Retrieval. In *Proceedings of IEEE Global Telecommunications Conference*, Cape Town, South Africa, 6–10 December 2010.
23. Pinkas, B.; Reinman, T. *Oblivious RAM Revisited, Advances in Cryptology (CRYPTO)*; Springer: Berlin, Germany, 2010; Volume 6223, pp. 502–519.