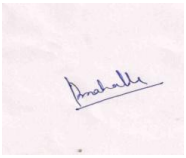
Doctoral Programme:	Wireless Communication
Project title:	Identity Management Framework for Internet of Things (IoT)
Name of PhD stud	Parikshit Narendra Mahalle
Email:	pnm@es.aau.dk
Education:	Master of Engineering – Computer Engineering
Institution:	Dr.D.Y.Patil College of Engineering, University of Pune, Pune ,India
Academic Supervisor:	Neeli R. Prasad, CTiF, AAU, Denmark
Co-supervisors:	Ramjee Prasad, CTiF, AAU, Denmark, Sudhir Dixit, Hewlett Packard labs, Bangalore, India
Department:	Electronic System
Date of enrolment:	15 Nov 2009
Expected date of Completion:	14 Nov 2012

Signature



08/07/2011 [Parikshit Narendra Mahalle]
Date PhD student

Study plan approved

Date	08/07/2011	Supervisor	Neeli R. Prasad **(Has reviewed by)**
Date		Head of Department	Børge Lindberg
Date		Head of Doctoral Programme	Gert Frølund Pedersen

AAU Ph.D. Degree
Updated 11 Month Study Plan

Title
Identity Management Framework for Internet of Things (IoT)

PhD Student
Parikshit Narendra Mahalle
(pnm@es.aau.dk)

Supervisor

Dr.Neeli Rashmi Prasad

(AAU, Denmark)

Co-Supervisor

Prof. Ramjee Prasad

(AAU, Denmark)

Co-Supervisor

Dr. Sudhir Dixit

(Hewlett Packard Labs, India)

AALBORG UNIVERSITET

Table of Contents

Section 1

Research Work Summary / Abstract

One of the most profound changes today is the increase in mobility of portable yet powerful wireless objects capable of communicating via several different kinds of wireless radio networks of varying link-level characteristics. Requirement for identity is not adequately met in networks, especially given the emergence of ubiquitous objects that are mobile and use wireless communications. Addressing identity problem requires changes to the architecture for addressing, trust establishment and authentication of objects. The uniqueness of research lies in creating identity management (IdM) framework for internet of things (IoT).

In IoT, the activities of daily life are supported by a multitude of heterogeneous, loosely coupled objects. The support of seamless collaboration between users, as well as between their objects, can be seen as one of the key challenges for this vision to come true. An object IdM is a central element of IoT. The purpose of this research is to describe framework for IdM which is scalable, trustworthy and generic.

The research evaluation will be mainly conducted in an advanced simulator. The device-level performance evaluation helps to find out the many suitable application situations.

The **expected outcome** of the PhD is to provide solution for the following features

1) Addressing of objects that holds identity
2) Establishing relation between trust management and IdM
3) Trust management and Circle of trust for ubiquitous objects
4) Authentication schemes for objects in IoT
5) Secure attribute exchange and selective disclosure of attributes inside IoT

Section 2

The Scientific Content of PhD Project

2. a Background

IdM refers to the process of representing and recognizing entities as digital identities in IoT. Authentication, which is an integral part of IdM, serves to verify claims about holding specific identities. IdM is therefore fundamental to, and always include, other security constructs such as addressing, access control and authorization. The major challenges and features of the future IoT are:

- **Objects** - Far from the dumb sensors that can be queried for simple data, the IoT of the future will include a wide array of objects, both virtual and real, ranging from smart devices with very high computing and communication capabilities to simple sensors that give out only one piece of data (e.g. temperature sensors).
- **Identities** - Identities are the windows as shown in figure 1 through which users interact with their devices and consume services in today's world. Before any service is delivered, it is customary to verify a digital identity of the user requesting that service (user identity) and also the identity of the entity offering the service (service identity). In the IoT world, this concept of identity extends to objects. Ensuring that the objects have a means to be identified is critical to assure users that their interactions with the objects are safe.
- **Interactions** - The ubiquitous nature of objects in the future will hugely impact the way in which users will interact with them in their daily life. Compared to today's world where interactions with devices and services are restricted by ownership and subscription (with very few exceptions), in the future, IoT users will be able to discover and use objects that are public, add objects temporarily to their personal space, share their objects with others, objects that are public can be part of the personal space of multiple users at the same time, etc.

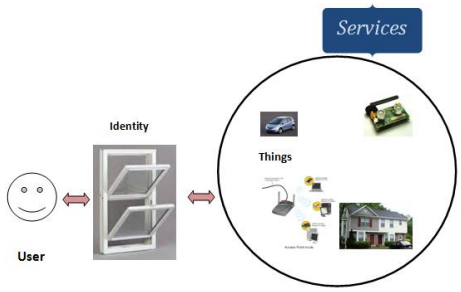


Figure 1: Object-User Interaction in IoT

To achieve IdM, the solution is to find new trust based IdM for objects, capability based addressing with context based authentication and secure attribute exchange of objects.

2. b Motivation

IoT is a service-oriented architecture and is mandatory subset of future Internet where every virtual and physical object can communicate with every other object giving seamless service to other entities. In ubiquitous networks not only user become ubiquitous but also objects and their context become transparent and ubiquitous. If all objects of daily life from animal to airplane are equipped with radio tags, they can be identified and managed by computers in the same way humans can. The IoT describes a world where humans are surrounded by objects that communicate with each other and can allow people to interact with the digital world. To succeed in this vision, it is not only the people who need an understanding of this multi-object environment, but also the network needs a representation of "who" the user is to achieve IdM with the help of new identities and identifier formats [1].

The purpose of this research is the development of a full working framework and architecture for IdM. Major factors of influence are the connectivity, power sources, form factor, security, geographical factors and cost of deployment and operation. Applications with different constraints on these factors will have different optimum architectures for integration. Many research proposals have already been presented but the proposed solutions are very basic, meeting only a partial range of identity requirements applicable only within closed trusted groups that support limited types of identities. Different IdM models will have different cost requirements in terms of time and space. The purpose of this research is to describe and study current approaches to identity management, and to provide light weight solutions for addressing, trust management, authentication and secure attribute exchange of objects.

2. c State of the Art

Current IdM solutions are mainly concerned with identities that are used by end users and services to identify themselves in the networked world (e.g. Liberty Alliance [2], OpenID [3], etc). These solutions provide user attributes and authentication as a service to relying parties. The main IdM solutions focus on the definition of IdM life cycle, definition of service integration with identity providers, the establishment of SSO mechanisms to define identity federations and exchange of authentication information and attributes with respect to end users and services. This is the case with solutions like Shibboleth [4], Liberty Alliance [2], OpenID [3] and WS-* [5]. The Internet players and the Telco industry have been developing their IdM solutions along different paths, to address different needs. In the Internet, the focus is more on providing solutions for end user to access services, while in the Telco world, it is more the case of identifiers and authentication, since deciding which entity is allowed to connect to the network is of paramount importance here. But with the convergence of the Internet and Telco worlds these paths are merging with each other more and more. Examples of efforts in this direction are the solutions developed in standardisation organisations like 3GPP (e.g. GAA [6]) or in European projects like FIDELITY [7], SPICE [8] (e.g. GBA-SAML), SWIFT [9] and PRIME [10]. The addition of things in this space requires that the concepts developed so far have to be extended and improved to include the scenarios made possible in IoT. Comparative summary of some of these IdM project is summarised in table 1.

Table 1. Comparative Summary of the State of Art for IdM

Features	OpenId[3]	Liberty Alliance[2]	Shibboleth[4]
Authentication(1:1)	No	No	Yes
Authentication(m:n)	No	No	No
Authorization	No	Yes	No
Single Sign On	Yes	Yes	Yes
Technologies	HTTP	SAML	SAML
Primary Focus	Distributed Identities	Trust Relations	Attribute Exchange
Device Identity	No	Partial	No
Interoperability	No	Yes	No
Federation	Yes	Yes	Yes
Lightweight	No	No	No
Scalability	Yes	No	No
Replay attack	Yes	Yes	Yes

The concept of identities and virtual identities in [11, 12, 13] are introduced for IoT but does not present concrete solution for IdM in IoT. An author presents the domain trusted entity where each identity is managed by a trusted entity of its corresponding home domain that keeps it under the preferences set by its holder. This approach is not suitable for futuristic IoT due to its dynamic topology and distributed nature. In [14,15], authors have not addressed the problem of how the wide range of entities can be organized in establishing a particular use or session. Author introduces identity framework by considering telecom infrastructure and ubiquitous objects are left unaddressed. Another proposal is Host Identity Protocol (HIP) [16] where identifiers are cryptographically generated using digest of RSA public key. Same mechanism of generating identifiers is not suitable for low memory and low battery objects like sensor nodes and other resource constrained objects. There is no identity protection in HIP, so HIP nodes can be easily tracked. In [17], author has described identity based mobility architecture relying on IdM system. It separates mobility into decision and action. This contradicts to the function of nomadic and uncertain IoT. Objects belonging to different owners in IoT , trust management [18] and circle of trust is crucial. In [19,20] , author presented trust based IdM and needs to be extended with dynamic trust management for IoT.

2. d Statement of the Research Objective

Things or entities like object, person that can request to access a resource in IoT. Objects get access by claiming an identity. Identities collate data in the form of attributes. A crucial function of IdM system is to authorize/deny access of subject to resources. Key elements of IdM system are authentication, authorization and policies that depend on proper authentication to regulate authorization. IdM solution is viewed as collection of identity definition and identifier format for object , storage of credentials , secure access and context oriented IdM framework.Research objectives for IdM in IoT can be enunciated as follows.

Identities: How does the concept of identity and identifiers translate into the world of IoT? How users' interactions with things affect the scope of identities inside IoT? Topics here include identifiers and attribute of users, services and objects, new concepts such identity aggregation, identity imprinting, private vs. public things, privacy aspects of identities and circles of trust.

Authentication of an identity: Topics here include methods for authenticating users, services and objects, multi-object single sign-on, authentication in case of identity imprinting and uncertainty.

Authorization and attribute exchange: attribute exchange protocols for users and objects, selective disclosure of attributes (privacy protection) and negotiation.
Trust Management: Trust management model for objects and circle of trust.

2. e Key Methods

IdM Solutions

1. **Centralised Solution**
   In centralised IDM solution, there is central entity called as server which is taking care of storing the identities of all stakeholders and all processing of these identities is carried out at this central server.. This solution is prone to single point of failure and causes a time inefficient solution for recovery
2. **Decentralised Solution**
   In decentralised solution, the processing and storage of identities is carried out in distributed manner where there is remotely all functioning is done.
3. **Hybrid Solution**
   In IoT, pervasive objects are going to mobile and depending on the scenario or context , IdM will vary with sometime centralised solution or decentralised solution. This is referred as hybrid solution suited and is best suited for IdM of ubiquitous objects in IoT.

The study will be based on theory-assisted design and application to generic practical situations. The main method for concept evaluation is an existing advanced simulation tool with performance being the main evaluation metric. This is because for the IoT, analysis and comparison through simulation are more desirable compared to fully theory oriented performance. The research will be based on a simple hybrid model with centralized/decentralised control. Resource and design constraints are going to be the crucial factors for designing IdM for IoT.

The aim of this research work is to build a generic framework for IdM in IoT. This research aims to find out:

- Defining measurement criteria for IdM in IoT environments.
- Performing a state of the art evaluation with respect to the defined criteria.
- Figuring out the vulnerabilities of the existing IdM solutions in IoT context.
- Building trust management model for IoT
- Working out remedies for these solutions.
- Researching capability based addressing in IoT
- In order to access a object or service, the user needs to provide an identity that can be authenticated giving need of Authentication algorithm
- Algorithms for attribute exchange between objects

2. f Potential Significance and Applications

The expected output of research is to provide efficient IdM strategies to fulfil fast evolving IoT. The IdM architecture will enable objects to communicate with other surrounding objects (perhaps belonging to other users) in environments with different security/authentication requirements. The authentication feature of IdM solution will cover the authentication of objects, where the relying parties may be services, other objects or users. This support is to be done such that it hides the specific characteristics of objects. At the end of the study, efficient algorithms for the access control, authentication privacy and trust negotiation is expected which can be easily deployed on the generic framework for IdM. Consider the smart home scenario in IoT which clearly describes the different communication which takes place between different objects .There are other applications like eHealth, pharmaceuticals where identity of objects plays an important role. These scenarios in IoT explain what operations take place when objects communicate with each other in smart home giving convenience and capability amplification and remote control. Different scenarios will be taken into consideration to design framework. In addition to benefits, IdM comes with risks, controversies, and

trade-offs giving birth to issues like privacy, authentication and authorization. Threats like spoofing, tampering, information disclosure and authentication needs to be considered for the design of IdM .

Applications

Applications areas will cover all sectors including Retail, Logistics, Pharmaceutical, Food, Health, Intelligent Home, Transportation, Military, etc. Intelligent homes, body area networks in eHealth as well as holistic and sustainable agriculture are prominent scenarios in the scope of the research field of IoT.

2. g Time Schedule for PhD Research Work

Milestones		Year 1				Year 2				Year 3			
1	Background Study												
2	Literature Survey												
3	Problem formulation												
4	Research direction and requirement												
5	Novel concept development												
6	Feasibility study												
7	Framework design and challenges												
8	Implementation												
9	Simulation and verification												
10	Result, conclusion, dissemination the PhD study												
11	Refinement and optimisations												
12	Attending PhD courses **												
13	Publication (Journal and conferences)												
13	Write of the Thesis												
14	Stay abroad *												

*3 months at AAU & 9 month at INDIA every year (Will be working with AAU supervisor & GISFI Indian supervisors)

** I am going to attend courses organized by Alborg University through video conferencing from India and courses related to my research area in well known institutes in India.

These are the milestones planning to achieve as part of my PhD with tentative months.

- **Milestone 1 (M3) :** Understanding literature of Identity management and IoT, security analysis and requirement
- **Milestone 2 (M3):** Determining motivations, questions and research challenges, direction and problem specifications.
- **Milestone 3(M6) :** Defining the functional requirements which will cover detailed study of risks and mitigations ,necessary extensions and novel developments and survey paper will be published in conference and journal.
- **Milestone 4(M7):** Researching on different addressing mechanism.
- **Milestone 5 (M9):** Design of optimized Cryptographic algorithms and trust management model.
- **Milestone 6 (M12):** Evaluating phases, defining of performance metrics and comparison with existing works and writing conference paper.
- **Milestone 7 (M15):** To do few courses during this 6 month period and submission of Journal Papers.
- **Milestone 8(M24):** Understanding literature of authentication methods**.** Developing algorithm, implementation and testing.
- **Milestone 9(M24):** Devising techniques and methods for attribute exchange of objects for management and building framework.

- **Milestone 9 (M24):** To finish the courses and complete 30 ECTS and submission of conferences/ Journal Paper.
- **Milestone 10 (M30):** To validate methods using system level simulation.
- **Milestone 11 (M32):** Submission of Journal Paper.
- **Milestone 12 (M34):** To start writing thesis and simultaneously do refinements towards finishing PhD, by the end of M34.
- **Milestone 13 (M36):** Wind up the PhD work, and publish the all the work done.

2. h Outline of the Content of Thesis

Thesis will be a monograph and below is the brief outline of the thesis.

Affidavit
Chapter 1 :Abstract

Chapter 2: Introduction
- Background
- Security Requirements for IoT
- Need for Identity Management
- Problem definition
- Thesis outline

Chapter 3: State of the Art in Identity Management

Chapter 4: Security Analysis, Evaluation and Verifications
- State of the Art - An Evaluation Report
- Analysis and verification
- Proposed Architecture
- Conclusions and Outlook

Chapter 5: System Model
- Design of Crypto Algorithms / Protocols
- Architectural Overview
- Conclusions and Outlook

Chapter 6: Addressing and Authentication of Objects
- Framework integration
- Design Methodology and algorithms
- Results and Comparison
- Conclusions and Outlook

Chapter 7: Conclusions and Future Work
- Conclusions
- Future work

Appendix (Reference)

2. i Publication Plan

The intention is to publish three journal papers, more or less one per year, in high quality security related journals such as Computer Networks, Computer communications, information security or Security and Privacy as given below.

Journal

- Bayu Anggorojati, Parikshit Mahalle, Neeli R. Prasad and Ramjee Prasad, "Capability based Context Aware Access Control (CCAAC) for Distributed Wireless Sensor Network" , in the Springer Journal **(Ready for Submission with Supervisor)**
- Parikshit Mahalle, Neeli Rashmi Prasad, Ramjee Prasad , "Identity Establishment and access control for Ad-hoc Wireless Networks" **(Working Title)**, Springer Wireless Personal Communication Journal
- Parikshit Mahalle, Neeli Rashmi Prasad, Ramjee Prasad , "Identity Management Framework for Internet of Things (IoT)" **(Working Title)**, Elsevier journal of Computer Communications on Information and Future Communication Security

Conferences

- Parikshit Mahalle , Neeli Rashmi Prasad , Ramjee Prasad ," Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges". Recent Trends in Network Security and Applications, Springer – Third International Conference,CNSA 2010, Chennai, India. Communications in Computer and Information Science, 2010, Volume 89, Part 2,430-429. **(Accepted & Published)**
- Sachin Babar, Parikshit Mahalle, A.Stango, Neeli Rashmi Prasad and Ramjee Prasad," Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)". Recent Trends in Network Security and Applications, Springer – Third International Conference,CNSA 2010, Chennai, India. Communications in Computer and Information Science, 2010, Volume 89, Part 2, 420-429. **(Accepted & Published)**
- Sachin Babar, Parikshit Mahalle, Neeli Prasad and Ramjee Prasad, " Proposed on Device Capability based Authentication using AES-GCM for Internet of Things(IoT)" , 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec) - Springer, May 17-19, 2011 - Aalborg, Denmark. **(Accepted & Published)**
- Parikshit Mahalle, Neeli Rashmi Prasad, Ramjee Prasad, "Proposed Decision Theory based Object Classification for Identity Management in Internet of Things", WPMC 2011. **(Submitted)**
- Parikshit Mahalle, Neeli Prasad, Ramjee Prasad and Sudhir Dixit, "Hierarchical Addressing with Clustering for Internet of Things (IoT) " – **(Working Title)**
- Parikshit Mahalle, Neeli Prasad, Ramjee Prasad and Sudhir Dixit, "Object Identification through Identity Mappings for Internet of Things (IoT) "– **(Working Title)**

Conference papers will be published as well along the three years of the PhD.

Section 3

Collaboration Agreements

Supervision Roles
Supervisor and co-supervisors has regular supervision through bi weekly Skype meetings along with the steering of the research. Since the candidate will be associated with research group and Indian Supervisor, research group and Indian co-supervisor will also help in supervision of PhD study.

Meetings
Regular supervision meetings will be held during the study period. Regular supervision meetings will be operated bi weekly, where both main supervisor and co-supervisors will be participating. An email distribution to all the supervisors documenting the achievements and planned activities will be carried out after the meeting. Moreover, irregular discussions would also take place, where participants exchange ideas on relevant interesting topics.

Work Plan
Detailed planning for work items, including specific tasks and corresponding due dates, are performed every half a year. Progresses will be tracked at the monthly supervision meetings.

Collaboration
As part of the collaboration It is planned to work along with research group of Hewlett-Packard Labs, India and it will be possible to access company internal documents. Some of the findings and results will be written in company internal documents and slides.

Section 4

Plan for PhD Courses adding up to 30 ECTS Points *

Name of the Course	Place/ Organizer (AAU)	Research related / General course	Status	ECTS
Introduction, What is IoT ? IoT application, Synergistic Technologies.	Neeli Prasad , Albena Mihovska , Zheng Tan, Ole Madsen ,Jens Erik Pederson	Research	Completed	1
Intellectual Property Rights	Lisbeth Tved Linde	General	Completed	2
Vehicle Communication	Tatiana Kozlova	Research	Completed	3
Air Interface Design for Future Wireless Systems – Towards Real 4G and Cognitive Radio	Ramjee Prasad, Frederikson, Suvra Das, Nicola Marchetti	Research	Completed	4
Sensors and RFID Networks	Neeli Rashmi Prasad	Research	Completed	3
Distributed source coding and Multiple descriptions	Jan Østergaard	Research	Completed	3
Seminar for scientists-patenting and commercialization	Nicolla Marchetti	Project	Completed	1
Analysis and design of high performance future internet infrastructure	Jens Myrup Pedersen, M. Tahir Riaz, Anna Tzanakaki	Research	Completed	2,0
Bayesian statistics, simulation and software -With a view to application examples	Kasper K. Berthelsen, Søren L. Buhl	General	Completed	3,0
Subtotal (Completed)				**22**
Writing and reviewing scientific papers	Jakob Stoustrup ,Jan Dimon Bendtsen	General	Registered	3,75
Special Courses for GISFI PhD Students / Conference / Tutorials*	I4CT, India	Research	Planned*	5
Subtotal (Planned)				**8,75**
Total (completed and planned)				**30,75**

* Will be decided in consultation with Supervisor. **Above list is based on the 2010 PhD Courses Catalogue. This list may change according to the courses available in India.

Section 5

Plan for Dissemination of Knowledge

- Most of the findings from the research work are going to be published in official conferences and included in the IEEE database according the standard proceedings.
- Furthermore, depending on the quality of the future results, other ways of dissemination -as newspaper articles, seminars, etc. will be considered.
- Depending on the solution and the application, some findings can be published as patents.

Section 6

Agreement on Immaterial Rights to Patent

All the rights about patents obtained during the PhD course will be shared between the university and the PhD student, following the standard procedures in AAU.

Section 7

Plan for External Collaboration

It is planned to work along with research group of Hewlett-Packard Labs, India.

Section 8

Financing Budget for the PhD

- CTIF, Aalborg University will provide the research facility.
- Expenses for tuition fee, lodging, boarding and travelling will be borne by STES, Pune (India)

Section 9

References

[1] G M Lee , Ning Kong , Noel Crespi , "The Internet of Things - Concept and Problem Statement" :draft-lee-iot-problem-statement-01.txt - 2011

[2] "The Liberty Alliance," Oct. 2007, (accessed 2008-08-15). http://www.projectliberty.org/

[3] "OpenID Authentication 2.0," Finalized OpenID Specification, Dec. 2007.

[4] Shibboleth project, http://shibboleth.internet2.edu/.

[5] Web Services Security Specifications Index Page on MSDN. http://msdn.microsoft.com /en-us/library/ms951273.aspx

[6] 3GPP TS 33.222- Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) - http://www.3gpp.org /ftp/Specs/archive/33_series/33.222/

[7] Federated Identity Management based on Liberty. EU CELTIC project.

[8] Service Platform for Innovative Communication Environment. EU FP6 project.

[9] The SWIFT (Secure Widespread Identities for Federated Telecommunications) Project, 2008

[10] Privacy and Identity Management for Europe (PRIME) - https://www.prime-project.eu

[11] Amardeo Sarma, Joao Girao," Identities in the Future Internet of Things". Wireless Pers Commun (2009) 49:353–363, © Springer Science+Business Media, LLC. 200 Tuesday,07 April 2009

[12] Antonio F. Gomez-Skarmeta, Pedro Martinez-Julia, Joao Girao, and Amardeo Sarma. Identity based architecture for secure communication in future internet. In Proceedings of the 6th ACM workshop on Digital identity management, DIM '10, pages 45-48, New York, NY, USA, October 2010.

[13] J. Guirao and A. Sarma. IDentity Engieered Architecture (IDEA). In Towards the Future Internet, pages 85-93. IOS Press, Amsterdam, 2010.

[14] Aguiar, R. L., Sarma, A., Bijwaard, D., Marchetti, L., Pacyna, P., & Pascotto, R. (2007).

Pervasiveness in a competitive multi-operator environment: The Daidalos project. IEEE Communications Magazine,45(10), 22–26.

[15] Amardeo Sarma, Alfredo Matos, Joao Girao, and Rui L. Aguiar. Virtual identity framework for telecom infrastructures. Wireless Personal Communications,45(4),521–543.

[16] R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture, 2006.http://www.ietf.org/rfc/rfc4423.txt.

[17] Alfredo Matos, Ricardo Pereira, and Joao Girao. Identity driven mobility architecture. In Future Network and Mobile Summit, Florence, Italy, June 2010. MS'10.

[18] Blaze, M.; Kannan, S.; Lee, I.; Sokolsky, O.; Smith, J.M.; Keromytis, A.D.; Lee, W.; , "Dynamic Trust Management," Computer , vol.42, no.2, pp.44-52, Feb. 2009

[19] Pacyna, P.; Rutkowski, A.; Sarma, A.; Takahashi, K.; , "Trusted Identity for All: Toward Interoperable Trusted Identity Management Systems," Computer , vol.42, no.5, pp.30-32, May 2009

[20] élix Gómez Mármol, Joao Girão, and Gregorio Martínez Pérez. Trims, a privacy-aware trust and reputation model for identity management systems. Computer Networks, 54(16):2899-2912, September 2010.