

Identity Management in Agent Systems¹

David R.A. de Groot and Frances M.T. Brazier

IIDS Group, Computer Science Department, Faculty of Sciences, Vrije Universiteit
Amsterdam, de Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands
{dra.de.groot, fmt.brazier}@few.vu.nl, <http://www.iids.org/>

Agent technology is a promising and enabling technology in open distributed environments. Agents are autonomous entities that interact with each other and with (web-) services, for which digital identity management (DIDM) is a prerequisite: the rights and obligations of all entities in an agent system need to be secured.

A framework for evaluation of DIDM in agent systems is proposed. Four computational entities in an agent system are distinguished: agent platforms, hosts, agents and services. These four entities are analysed with respect to four aspects of DIDM: representation, confidentiality, integrity and availability.

For each computational entity the following identity information is specified: a) name(s), b) address(es), c) look-up services, d) related principals, e) meta-data, and f) access regulation. *Names* are associated with each entity, e.g., unique identifiers and/or pseudonyms. *Addresses* specify an entity's point(s) of access and message delivery [2]. *Look-up services* provide information about other entities. *Related principals* are roles associated to a computational entity: Admin, Auditor, Creator, Developer, Owner, Publisher and User. These roles are often not explicitly represented. *Meta-data* describes the characteristics of an entity and its functions, e.g. information stored in a look-up service. *Access regulation* information, e.g. access rights.

The four aspects of DIDM of information stored and maintained in an agent system, are comparable to those found in other systems. A *representation* is a creation that is a visual or tangible rendering of someone or something. Representations are useful to store identity information. *Confidentiality* is related to information privacy. Any information that could possibly lead to the identification of a specific entity needs to be protected [3], e.g. user profiles, traces of transactions, and logs of interactions. In agent systems both the entities and their data need to be protected so that “only authorized entities

¹ The full version of this paper appeared in the Proceedings of the First International Workshop on Privacy and Security in Agent-based Collaborative Environments (PSACE), by Foukia, N., Seigneur, J., and Purvis, M. (editors) at the Fifth International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS-06), Future University, Hakodate, Japan, pp. 23-34

can see protected data” [3, 4]. Maintaining *integrity* includes [5]: a) Preventing unauthorized users from making modifications; b) Maintaining internal and external consistency; c) Preventing authorized users from making improper modifications. *Availability* can be defined as “ensuring that information and information processing resources both remain readily accessible to their authorized users” [5]. In agent systems, agents, for example, need to be able to find other agents and services. White- and Yellow page services can serve this purpose.

Two agent system development frameworks, JADE-S and AgentScape, are used to illustrate the potential of this framework with respect to analysis, evaluation, design and development of agent systems. The framework provides a basis for further consideration of issues concerning privacy, anonymity, traceability and accountability.

Acknowledgements

The authors thank Stichting NLnet and the Vrije Universiteit for their support and the Computer Law Institute of the Faculty of Law at the Vrije Universiteit (CLI) for their input. This research is conducted in the context of ALIAS project [6], in particular the project "The Virtual World requires New Bridges" (in Dutch: "De Virtuele Wereld vraagt om Nieuwe Bruggen"). In these projects legal implications of the use of software agents and agent systems are investigated from both a legal and technological perspective.

References

1. Luck, M., McBurney, P., Shehory, O., Willmott S. and the AgentLink Community (2005), "Agent Technology: Computing as Interaction - A Roadmap for Agent-Based Computing", ISBN 085432 845 9, <http://www.agentlink.org>
2. Tanenbaum, A.S. and Van Steen, M. (2002), Distributed Systems: Principles and Paradigms, Prentice Hall, New Jersey.
3. Subirana, B., Bain, M., (2005), "Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond", Springer's Integrated Series in Information Systems, Vol. 4, ISBN: 0-387-23414-4.
4. Pfleeger P. (1997), Security in Computing, international edition Prentice Hall, pp. 158, ISBN 0-13-185794-0
5. Mayfield, T., J. E. Roskos, S. R. Welke and J. M. Boone, (1991) "Integrity in Automated Information Systems". National Computer Security Center (NCSC), TR 79-91
6. <http://www.iids.org/alias>