Computational Trust to Further Reduce the Complexity of the Higher Education Common Space

Jean-Marc Seigneur[1], Pierpaolo Dondio[2], Stephen Barrett[2], Stefan Weber[2]

Abstract *— First, we review why the Higher Education Common Space is of challenging complexity to any stakeholders as well as the current management instruments and their shortcomings. Then, we emphasize that humans have used the notion of trust to manage complexity in the real world and that computational models of the human notion of trust have recently been researched to manage complexity in the digital world. We propose to integrate computational trust engines to the information system of each Higher Education stakeholder to further reduce the complexity of the Higher Education Common Space. To evaluate our approach, we detail how the SECURE trust engine can be applied to aspects of this problem: to decide which online course or host institution should be chosen; to select the best visitor student candidates; and to allow foreign engineer students to access lab experiments.*

Index Terms - Higher Education Common Space, complexity barrier, information technology, computational trust.

INTRODUCTION

Since the ratification of the first European Cultural Convention, signed in Paris in 1954 [7], the European Community has pursued its aim of creating a common framework for Higher Education. Several conventions and declarations were signed during the last 20 years to delineate guidelines and common actions: mobility programs were established; grant schemes, dedicated institutions and proper instruments were defined. These official acts were the first step to manage the complexity of the Higher Education Common Space (HECS).

The HECS can be seen today as a network of educational stakeholders, administrative offices, alumni, national or EU institutions, and students' information that are stored in departmental accounts. Each of these entities takes its own decisions, interacting with the others parties in the network. On one hand, the students should seek to choose the most appropriate online courses or host University; on the other hand, the educational stakeholders should choose the best suited candidates for admission.

As we shall present in the next section, this decision space has an inherent complexity which makes it difficult to manage. It is built upon autonomous institutions over 40 countries, with an increasing number of students and proposed courses (especially if we consider lifelong learning), with different legacy approaches, social and economic issues. In particular, the huge quantity of information, the dynamic and decentralized nature of the common space, the shortcomings of the current supporting instruments have led to a situation where it is difficult to make trustworthy and correct decisions for any of the education stakeholders.

Humans have used the notion of trust to manage complexity in the real world and computational models of the human notion of trust have recently been researched that seek to manage complexity in the digital world. Our assumption is that the information system of any of these stakeholders will be equipped with our SECURE computational trust engine to facilitate their decision process. Our solution is not only an application of computational trust to the HECS network, but also an effort to improve the quality assurance of education for both the learner, who is helped to select the most appropriate online course or University, and the educational stakeholders, by providing a more trustworthy selection process.

The following section discusses in detail the history of the instruments created to reduce the complexity of the HECS and their shortcomings. Then, we give an overview of computational trust and its applications to further address the complexity issues appearing in the HECS. Finally, we survey the related work and draw conclusions.

TOWARDS LESS COMPLEXITY IN THE HECS

The importance of student mobility has been widely acknowledged by legislations all over the world for both its educational and socio-economical benefits. However, student mobility can still be seen as a composite problem space where several parameters have to be set. Each of these parameters (described below) could be considered by the user (student or University) as an obstacle or an aid to transnational mobility and has to be evaluated in their decision-making process.

Several countries have been offering funds and programs to promote student mobility. Before the European Cultural Convention, in 1946 the Fulbright Program was established by the US Government and designed to "increase mutual understanding between the people of the United States and the people of other countries" [8]. In 1986, the European Community created the Erasmus program, a program for Higher Education which aimed to facilitate and standardize student mobility. Erasmus of Rotterdam (1465-1536) lived and worked in several parts of Europe in quest of the knowledge that only such contacts with other countries could bring. The grant of his fortune to the University of Basel made him a precursor of mobility grants.

[1] Jean-Marc Seigneur, University of Geneva, Switzerland, Jean-Marc.Seigneur@trustcomp.org.
[2] Pierpaolo Dondio, Stephen Barret, Stefan Weber, Trinity College Dublin, Ireland, dondiop@cs.tcd.ie, Stephen.Barrett@cs.tcd.ie, Stefan.Weber@cs.tcd.ie.

In addition to the cost to study in a foreign country, the scale of the number of students is huge. Worldwide, according to the UNESCO in 1994, 1,354,539 students studied in a University abroad. The USA and the EU absorb alone 67% of all the students. In particular, the engineering field scores the second highest percentage of Erasmus participants: 105.000 students representing 10% of the total. Millions of accounts are challenging for the limited centralized IT infrastructure of each local institution. The workload may be more manageable if the IT infrastructure would be distributed and decentralized. We shall return to the issues related to information technologies when we describe how we would deploy the SECURE trust engines within the HECS.

Once students have studied abroad, there is the crucial issue of recognition of their qualifications in countries other than the country where they studied. In 1997 in Lisbon, a convention on the recognition of qualifications concerning Higher Education was signed to initiate a common framework. In 1999, the Bologna Declaration [2] was signed to set objectives and guidelines to create a European HECS. The Bologna Process involves a system of academic grades which are easy to read and compare; the introduction of undergraduate and postgraduate levels in all countries; a system of accumulation and transfer of credits; mobility of students, teachers and researchers; cooperation with regard to quality assurance; and the European dimension of Higher Education. In 2005 in Bergen, 43 countries will discuss the state of the art of the Bologna process. Thus, the European Union recognizes the need for a common framework for Higher Education while it acknowledges the University as an autonomous national institution related to its own legislation and to the government of its country. The EU stressed that the primary responsibility for quality assurance in Higher Education lies within each institution. In this case, it is difficult for students from foreign institutions to unambiguously evaluate the quality of other foreign institutions.

Further Complexity Management Instruments

This is the reason that the EU developed another set of complexity management instruments and set up national institutions to manage its educational common space. This new set comprises the NARIC [6] network, the ECTS [4] system and the Diploma Supplement [3]. The NARIC is a network of national centers created in 1984 to help in regulating title recognition and facilitating the integration of national educational systems. The nature of NARIC is national, according to the autonomy principles described above. Therefore the status and the scope of work of individual NARICs may differ. Most NARICs do not make decisions but instead offer information and advice on request. ECTS is a credit system where each component of an educational program has a credit value attached to it. It is a student-centered system based on the student workload required to achieve the objectives of a program. Recently ECTS is developing into an accumulation system based on the principle that 60 credits measure the workload of a full-time student during one academic year. The Diploma Supplement (DS) is a document attached to a Higher Education diploma; it aims at improving international transparency and setting an easy-to-compare standard for recognition of qualifications. The DS is produced by national institutions according to a template that has been developed by the Council of Europe and UNESCO. In summary, these instruments show that there is a need for increased information exchange, interconnection and interactions between autonomous entities.

Unfortunately, all these instruments fail to correctly address all the issues. For example, recent reports [9, 10] discuss the shortcomings of the ECTS. A student/institution must consider how every country uses the ECTS system and recognizes diplomas. The possible problems that may arise are:

- Many nations have their own national credits system, which are seldom connected or compatible with ECTS.
- Different accumulation systems exist (based on hours of study, number of exams or number of disciplines).
- There are countries where ECTS is legislated (like Hungary or the Netherlands), a few others where it is not, and a few universities that use the system voluntarily. ECTS is not obligatory in countries like Ireland and Portugal. In Denmark, it is obligatory for universities but not for polytechnics. In some other countries it is only suggested by the government.
- The question of how to measure the credits received is still unclear for students. There is no standard way of measuring credits. In Ireland, workload depends on the time spent in classroom whereas in Austria credits are not linked to hours of study but to number of exams. Measuring the workload completed through any non-subjective credit accumulation system can never be completely fair. Swiss students have experienced that sometimes “a credit point is not a credit point” [10], because points are cheaper to gain depending on the reputation of the University where those credits were gained. Depending on the faculties, more work should be required for the same amount of credit. This makes the system difficult to trust.

Students must also consider several economic and social issues: transferability of grant, cost of life, parental support, the right and possibility to work, the tax system in the host country, accommodation and catering facilities, health-care services and coverage, local and international transportation, or psychological counseling. An educational institution may look to earn higher tuition fees income, to achieve greater technological transfer, to strengthen economical and cultural ties, to promote scientific ties, or to win highly qualified

personnel (brain gain). Other issues concern the language barriers and the offer of language courses provided by the host institution, cultural barriers, xenophobia and racism, facilities for the student integration in the community (for example student union activities), host city, or more generally the overall quality of life. Some academic and professional issues like the quality of the education system in the host nation and the reputation of the University must also be taken into consideration.

In our analysis, the principal features of the HECS are:

- Its nature is distributed and decentralized due to the national or local nature of the recognition process and the established autonomy of each institution.
- Its main management instrument – the ECTS – is successfully used but cannot be totally trusted and is not universally accepted.
- The complexity is high due to an increasing number of students, countries and sources of information.

In fact, the sources of information have dramatically increased since the introduction of on-line e-learning, which further increases the overall complexity of the space. The layer of information technology added on top of the traditional HECS has turned it into an on-line intangible space. It is even more difficult to assess the trustworthiness of on-line educational resources because the technical infrastructure acts as a cloud between the stakeholders.

COMPUTATIONAL TRUST OVERVIEW

In the human world, trust exists between two interacting entities and is very useful when there is uncertainty about the outcome of the interaction. The requested entity uses the level of trust in the requesting entity as a means to cope with uncertainty, to engage in an action in spite of the risk of a harmful outcome. Luhmann argues that trust is a means for "reduction of complexity" [15]. The goal of a trust engine is to provide a computational version of the human concept of trust. Therefore, by embedding trust engines into the IT infrastructure of the HECS, we argue that it should be possible to reduce its complexity. One of the main advantage of computational trust is that trust is subjective, which means that each trust engine owner is ultimately responsible for the final decision, which is in line with the established autonomous status of each educational institution.

Marsh introduced in his PhD thesis one of the first computational model of trust [16]. We consider a computed trust value as the digital representation of the trustworthiness or level of trust in the entity under consideration. We define a trust value as a non-enforceable estimate of the entity's future behaviour in a given context based on past evidence. By non-enforceable, we emphasize that the trust value can simply be based on interpersonal trust interactions. For example, the count of positive and negative interaction outcomes is monitored and the trust value is based on the number of positive outcomes and the total number of outcomes. System trust, which may be enforced by insurance or legal actions, is not compulsory to compute such trust values. The basic components of a computational trust engine (depicted in Figure 1) should expose a decision-making component that is invoked when a requested entity has to decide what action should be taken with respect to a request made by another entity, the requesting entity.

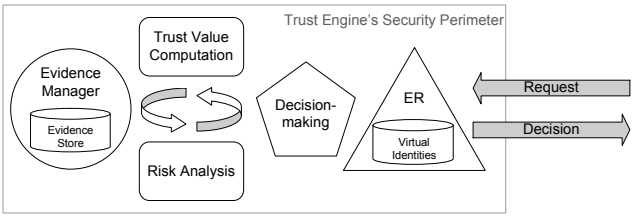

FIGURE. 1
HIGH-LEVEL VIEW OF A TRUST ENGINE

In order to make the decision to grant the request, two sub-components are needed:

- a trust module that can dynamically assess the trustworthiness of the requesting entity based on pieces of evidence (such as, direct outcome observations or recommendations);
- a risk module that can dynamically evaluate the risk involved in the interaction.

The chosen action should maintain the appropriate cost/benefit ratio. Depending on system trust, the weight of the trust value in the final decision may be small. In the background, another component is in charge of gathering evidence (for example, recommendations or comparisons between expected outcomes of the chosen actions and real outcomes). This evidence is used to update risk and trust information. Thus, trust and risk follow a managed life-cycle. The Entity Recognition (ER [21]) module is in charge of recognizing the interacting entities, called virtual identities or pseudonyms. The trust value returned for each entity can be used to select the most trustworthy entity among a set of entities.

Our EU-funded SECURE (Secure Environments for Collaboration among Ubiquitous Roaming Entities) project [20] has investigated dynamic and self-configuring security mechanisms for global computing based on the human notion of trust. The result of the SECURE project is an advanced, formally grounded, trust engine Java API, which can be applied to a large number of application domains. In the next section, we demonstrate how it can be applied to further decrease the complexity of the HECS.

THE USE OF SECURE TRUST ENGINES TO FURTHER DECREASE THE HECS COMPLEXITY

We draw from our analysis of the HECS that there is a need to further network the different Higher Education stakeholders and to increase the information and evidence about each of them. According to Luhmann [15], this evidence can be used to reduce complexity and increase trust

in the HECS. A more trustworthy space would increase its adoption, for example, foster student mobility. There is a need for a new management instrument, which should be more dynamic than static previous instruments and able to take into account the subjectivity of any assessor among the different stakeholders.

Implementation High-Level View

Our architecture assumes that each educational stakeholder taking part in the creation of a common educational network with his or her own computing system runs an instance of the SECURE trust engine. This model (depicted in Figure 2 and 3) includes all stakeholders, such as the education institutions and their main bodies, the alumni office, the student union, the departments, the administrators, the international office, the students, the academic staff, the EU and national institutions such as the NARIC network.

Any trust engine can gather and propagate evidence. Each trust engine is autonomous and responsible for computing the appropriate trust values based on this evidence and for aiding its stakeholder's decision making. In our model, certain recommenders may be privileged. For example, a student from the Technical University of Madrid may privilege the recommendations and evidence provided by his/her alumni rather than the evidence sent directly by the trustee. Depending on which recommenders are privileged, trust values vary from one stakeholder to the other. We assume that cheating is not possible in our trust-augmented on-line HECS. Advanced trust engines, such as the SECURE trust engine, use trust computation algorithms that are hard to attack. Means to achieve this are beyond the scope of this paper and interested readers should consult the *trustcomp* on-line community [11].

Figure 2 illustrates the deployment of the SECURE trust engine within an institution's IT infrastructure. Here, we assume an instantiation of the Java version of the SECURE trust engine per institution member account (either staff or student). This is already possible as long as the IT services agree to spend resources to do so. A large-scale inter-institutions test of our approach may hopefully be one of the outcomes of the publication of this paper. We agree that the first implementations will require a lot of overhead though. At the end of this section, we discuss a lab experiment example, which can this time be easily implemented on top of previous work and uses the marks of the students to allow them to access the experiments. Generally, thanks to cryptographic signature validations, the evidence about the students is not open to cheating. Each main official party also runs a SECURE trust engine. Figure 3 depicts how evidence would be exchanged between different stakeholders.

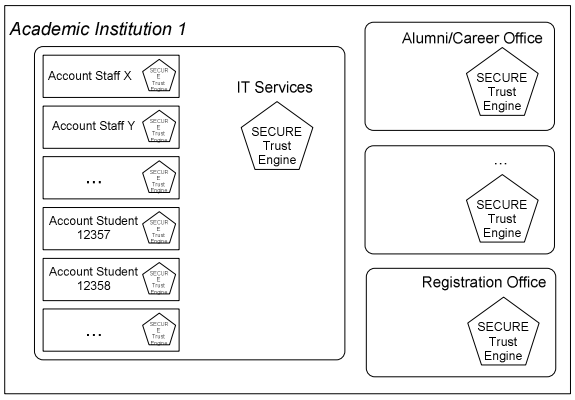

Figure. 2
TRUST ENGINES WITHIN THE INSTITUTION IT INFRASTRUCTURE

For example, the alumni/career office can store evidence about the percentage of previous students who have found a job after a certain amount of time and their average salary. The international office can provide the number of previous exchange students. The registration offices can publish their statistics about admissions. The NARIC centers can give evidence about the percentage of recognized diplomas between two selected universities. Any student account stored in the institution IT infrastructure can give signed information about the courses attended by the students, the student qualifications and their marks.

Each stakeholder can customize its own SECURE trust engine implementation thanks to its personal policies. For example, the trust policy of the SECURE trust engine specifies from whom the recommendations should be accepted or create a greater impact. If a student wonders which foreign institution would probably give him/her the greater chance to find a highly paid job after his/her studies, the student's trust engine would first contact his/her alumni office to get recommendations about candidate institutions based on the evidence given by alumni who have submitted their salary progression and studied abroad during their studies. Evidence from other institutions may also be used but the direct evidence from the candidate institutions may be less trustworthy. Depending on the student's preferences (for example, concerning the main topics), each assessment would be subjective. Over time, the evidence based on the experience of previous students would grow and the trust assessment would become more accurate. If foreign institutions put in place actions to increase their education quality, this would dynamically be reflected thanks to new more positive evidence. Concerning the bootstrapping phase, the trust engines would have to rely on static evidence given by the previous instruments such as the ECTS. However, after a while, evidence would reveal that one ECTS credit point in a foreign institution is actually worth more than another, which solves the Swiss students' concern mentioned in Section 1.

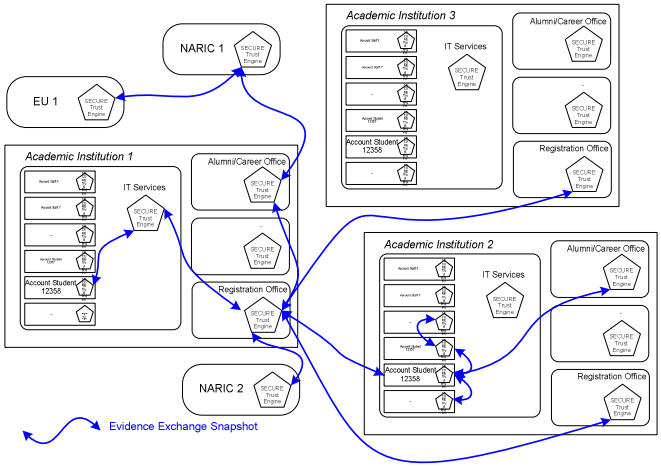

FIGURE. 3
EVIDENCE DISTRIBUTION IN THE HECS

The same recommendation mechanisms can be used to select the most trustworthy on-line courses according to the student's personal policies. Vice-versa, every education institution may take into account evidence about the results of previous exchange students coming form specific foreign institutions, e.g., their number of research publications during their stay, to select the most trustworthy students.

In our solution depicted in Figure 3, there is the issue of the students' accounts termination after they finish their studies. Presently, alumni and career offices seek to collect information about the alumni by means of mail survey's invitational interviews etc. However, many of the alumni may not take the time to reply to mail surveys and other communications. Thus, the amount of evidence may be low, and lead to inaccurate trust computation. Fortunately, the trend to create specialized on-line social networks services for alumni [1] (for example, Stanford University and the University of Michigan have such services) indicates that students may be provided permanent accounts. This type of account already stores information about the places where the alumnus has worked. Marks and salaries may be stored as well. We envision that such accounts may run a SECURE trust engine and share evidence with their career office. This solves evidence shortage. The fact that private evidence must only be shared with the consent of the owner underlines that there is an inherent conflict between privacy and trust. Trust engines can be extended with privacy enhancing technologies (for example to trade privacy for trust as detailed in other work [22]).

Detailed Lab Experiment Access Implementation

Finally, we practically evaluate our approach to allow students to access lab experiments over the Web, even if they are from foreign institutions. The SECURE trust model is applied to our PEARL [19] smart laboratories, where experiments for student engineers are improved by computing and communicating instruments. Labs that can be done remotely are needed to facilitate lifelong education by improving availability beyond standard working hours and to make the best profit of fixed expensive devices, such as electronic microscopes. On-line students may not be physically known and may use degrees from different institutions. Still, they would like their previous studies to be recognised in order to access courses that will improve their competency. A centralized administration of student records will not be possible in this case. In our prototype, the lab administrator specifies in the SECURE trust policy the trust value threshold based on marks gained by students on required topics to safely use the lab devices. When engineering students from institution A want to access the smart experiments of institution B, institution A recommends to institution B whether or not the students are able to conduct the experiment based on submitted signed evidence that the students have the required number of marks in each topic required by the target experiment. The institution A can take into account the reputation of institution B based on the outcomes of granting access to its previous student users such as the cases of failures in spite of a required amount of marks. The cost/benefit of allowing the students to access the smart experiment at time of request is based on schedule optimization and risk of failure.

For example, Alice is in her second year of BSc in electricity in the Technical University of Madrid (TUM) and would like to access the remote electricity lab at Trinity College Dublin (TCD). When she requests access to the lab Web page, her marks in electricity are retrieved. The SECURE trust engine from TUM signs and submits to the TCD lab's trust engine that Alice has earned 250 marks in electricity. The lab's trust policy is to grant access to any student with more than 220 local marks in electricity. There is a higher risk to break the device if the student is less experienced. So, when the lab administrator is not present, a broken device cannot promptly be repaired and many remote sessions may be lost. Both institutions have a BSc in electricity but the contents of the two BScs are not exactly the same. Based on previous evidence, TCD considers that marks recommendations from TUM in electricity are very compatible (for example, at 90%). Therefore, TCD's trust engine considers that Alice's trust value corresponds to $0.9 \times 250 = 225$ marks and Alice is allowed to remotely access the experiment over the Web. Another policy of the SECURE trust engine, called the risk policy, may be used to take into account the cost/benefit of granting Alice given the current circumstances. For example, another student with more marks, directly earned from TCD, may want to use the experiment remotely at the same time and the lab administrator is currently absent. In this case, there is less risk to give access to this more experienced student rather than Alice. Thus, Alice is not granted access to decrease the chance of failure and potentially allow another session after the local student's session.

Our main PEARL prototype consists of a lab experiment to carry out vision recognition algorithms on electronic boards placed under a camera. The camera is

controlled (including its zoom functionality) via Java applets over the Web to locate zones of interests on the electronic board. The SECURE trust engine is also implemented in Java. Thus, it is straightforward to integrate it with such PEARL experiment. The means to specify the trust and risk policies is very open and expressive because all policies in the SECURE trust engine simply correspond to Java classes.

RELATED WORK

Apart from the SECURE trust engine, there are many other approaches for computational trust, which is discussed in the trustcomp on-line community [11].

Although, as far as we know, no computational trust engine has been applied to the HECS application domain, there are applications related to this domain. Golbeck et al. describe in [14] how they use the existing Friend-of-a-Friend (FOAF) vocabulary [13] along with a vocabulary of their own to create trust networks and to allow the user to specify different trust levels in a person about particular knowledge domains. Croucher [12] proposes a model of trust based on the assertions that certified users with certain profile make on learning materials. He extends the previous FOAF/Golbeck trust vocabulary to be applicable to any resource and not only to individuals. Inferences can be made from rating results to check the quality of resources, their authors, or the trustworthiness of a particular user's assertions compared to all other assertions. Parker [17] describes the problem of quality in online education and the differences between standards present in US, UK, Canada and Australia. Sims et al. state that the learning community is best conceptualized as "an environment that integrates collaboration, communication among linked learners" [23]. The distributed and dynamic aspect of nowadays learning world is described by Pond [18] as a new paradigm for accreditation and quality assurance that must be learner-centered, local, open, collaborative, and flexible and can be seen as a distributed delivery model. It is in line with our approach where students/learners own their SECURE trust engine and their trust computation is personalized, subjective and local based on collaborative evidence distribution. In the EU project ELENA [5], learners are interconnected in a network community to demonstrate the feasibility of smart spaces for learning, defined as an educational framework that allows the consumption of heterogeneous learning services via assessment tools, learning management systems, educational repositories and live delivery systems such as video conferencing. ELENA keeps a dynamic learner profile, which includes learning history, learner specific information and learning goals to select the most appropriate learning material. ELENA does not use computational trust for decisions but our work indicates that such extension would be of interest.

Finally, Weippl [24] presents how the standard security mechanisms (authentication, access control, encryption…) can be reused to provide secure e-learning platforms but he does not cover computational trust.

CONCLUSION

There is a need for new instruments to manage the complexity of the Higher Education Common Space. In this paper, we argue for the use of trust engines within the IT infrastructure of this space. Trust contributes to reduce complexity and gives an incentive for students to engage into studies abroad. To engineer computational trust free from attacks is difficult, so we reuse our formally grounded SECURE trust engine. We hope to initiate larger scale trials.

REFERENCES

[1] "Alumni Social Software", http://www.affinityengines.com/.

[2] "The Bologna Declaration", 19.XI.1999, Bologna.

[3] "Diploma Supplement", http://europa.eu.int/comm/education/policies/rec_qual/recognition/diploma_en.html.

[4] "The ECTS - European Credit Transfer System", http://europa.eu.int/comm/education/programmes/socrates/ects_en.html.

[5] "The Elena project, Smart Spaces for Learning", http://www.elena-project.org.

[6] "The Enic-Naric program", http://www.enic-naric.net.

[7] "The European Cultural Convention", 19.XII.1954, Paris.

[8] "The Fulbright Program", http://exchanges.state.gov/education/fulbright.

[9] "Green Paper: the obstacles to transactional mobility", European Commission , COM96(426).

[10] "Survey on ECTS", ESIB, 2002.

[11] "Trustcomp", Online Community, http://www.trustcomp.org/.

[12] T. Croucher, "A model of trust and anonymity in a content rating system for e-learning systems", W3C, 2004.

[13] FOAF, "The Friend-of-a-Friend Project", http://www.foaf-project.org/.

[14] J. Golbeck, J. Hendler, and B. Parsia, "Trust Networks on the Semantic Web", University of Maryland, 2002.

[15] N. Luhmann, "Familiarity, Confidence, Trust: Problems and Alternatives", in *Trust: Making and Breaking Cooperative Relations*, University of Oxford*, chapter 6*, pp. 94-107, 1994.

[16] S. Marsh, "Formalising Trust as a Computational Concept", PhD Thesis, University of Stirling, 1994

[17] N. K. Parker, "The Quality Dilemma in Online Education", in *Theory and Practice of Online Learning*, pp. 385-421, 2003.

[18] W. K. Pond, "Distributed education in the 21st century: Implications for quality assurance", in *Journal of Distance Learning Administration*, 2002.

[19] T. Schäfer, J.-M. Seigneur, and A. Donnelly, "PEARL: a Generic Architecture for Live Experiments in a Remote Laboratory", in *Proceedings of the conf. on Simulation and Multimedia in Engineering Education,* 2003.

[20] SECURE, "Secure Environments for Collaboration among Ubiquitous Roaming Entities", http://secure.dsg.cs.tcd.ie.

[21] J.-M. Seigneur and C. D. Jensen, "The Claim Tool Kit for Ad-hoc Recognition of Peer Entities", in *Journal of Science of Computer Programming*, Elsevier, 2004.

[22] J.-M. Seigneur and C. D. Jensen, "Trading Privacy for Trust", in *Proceedings of iTrust'04 the Second International Conference on Trust Management*, LNCS 2995, Springer-Verlag, 2004.

[23] R. Sims, G. Dobbs, and T. Hand, "Enhancing quality in online learning: Scaffolding planning and design through proactive evaluation", vol. 23(2), pp. 135-148, Distance Education, 2002.

[24] E. R. Weippl, "Security in e-Learning", in *Series: Advances in Information Security, Vol. 16*, Springer, 2005.