

Establishing a Privacy-Aware Collaborative eLearning Environment

Katrin Borcea-Pfitzmann, Katja Liesebach, Andreas Pfitzmann

Dresden University of Technology (Germany),

katrin.borcea@inf.tu-dresden.de, katja.liesebach@inf.tu-dresden.de, pfitza@inf.tu-dresden.de

Abstract

Supporting privacy in eLearning becomes a commonly admitted important issue when designing according infrastructures. This is motivated by a higher awareness of the users with respect to protecting their personal data. In particular, eLearning comprises many scenarios that clearly spell out risks to the users' privacy, such as communicating identifying data during classes.

Nevertheless, current research activities primarily concentrate on non-collaborative eLearning. While those approaches neglect the direct communication of users, they address the protection of indirect misuse of the data.

In contrast, we describe a concept, which is prototypically being realized in the eLearning platform BluES. It aims at as much latitude for the users acting in the collaborative environment as possible – but nevertheless at protecting their personal information. The approach's objectives are to support the users in managing their learning processes and to partition the activities such that a reasonable collaborative working as well as the protection of privacy are possible. The first issue is facilitated by giving the users free access to all functional possibilities of the eLearning environment, i.e. each user is allowed to do anything – within the frame of generally agreed rules and directives. In order to provide reasonable access control, BluES integrates a privacy-enhancing identity management system, which is part of the research project PRIME. This way, users are guaranteed that processing their personal data on services side is reduced to a minimum. Furthermore, they can keep track of all transactions of their data, which allows for maximal transparency.

Keywords: collaborative eLearning, privacy, identity management

Motivation

Learning is one of the most important activities of man – in a Knowledge Society more than ever. Driven both by opportunity and need, eLearning, i.e. computer-network based learning enabling to learn at any time and everywhere using broad knowledge resources and collaboration of various parties, gets ever more important.

If ever major parts of our lives are spent for eLearning, privacy gains high importance there. This is particularly true for collaborative eLearning, where learning is nothing which can be supported (may be after a somewhat huge download of a knowledge base / course) completely locally, meaning that privacy can be provided by securing the machine of the learner. In collaborative eLearning, where many actors interact together in various and changing roles, privacy of individuals requires in addition managing one's own identities, i.e. the eLearning users will not use the same name in many or even all contexts. Otherwise, both eLearning servers as well as collaborating other eLearners or eTutors could profile the learning of individuals. This may be an unacceptable invasion of privacy for these individuals or even illegal in some jurisdictions. In any case, it would mean a biased environment for eLearning, e.g.: Who dares to ask a possibly silly question if “who asks what question” can be recorded and taken notice of in a later examination? Who, as a tutor, dares to give an advice which

might not suit someone higher up in the academic hierarchy, if the eLearning system could provide “proof” of this advice to others?

Therefore, this paper explores, how far we can get with respect to privacy in collaborative eLearning by which means, contributing both to setting the stage and designing a next generation of eLearning systems being privacy aware.

Such an eLearning system should provide a straightforward mapping of traditional learning styles and activities in the “real world” (i.e. natural behavior of the users and learning/working environments) to the “electronic world” thus supporting learners by:

- Support for their independence, individuality, and autonomy – last but not least with respect to their informational self-determination (EU, 1995), which means awareness for what others get to know about them and how they themselves can limit this, e.g. by identity management,
- Support for different learning approaches (behaviorism, cognitivism, constructivism),
- Support of different learning methods (spanning the area of learning “alone”, learning in well defined hierarchical settings, e.g. under supervision of a tutor, until learning in different roles, e.g. both getting tutoring by a particular tutor or by a peer-group of learners – and giving them some kind of tutoring as well),
- Support for collaboration, i.e. communication and interaction, role making and role taking, awareness who others are available by which means and for which topics.

Overall, such an eLearning system should provide an unbiased flexible educational environment, besides others for taking different roles (quasi)simultaneously.

State of the Art

For eLearning, security and privacy mainly are non-issues until now. There are only a few exceptions aiming at limited security and very limited privacy – and this only in non-collaborative environments.

A typical example is the ELENA project (Klobučar, T., Seničar, V., and Jerman-Blažič, B., 2004) and a typical problem statement of security and privacy in eLearning is: “The goal of security in e-learning is to *protect authors’ e-learning content* from copyright infringements, to protect *teachers* from students who may undermine their evaluation system by cheating, and to protect *students* from being too closely monitored by their teachers when using the software. Since these intertwined requirements are not met by existing systems, new approaches are needed” (Weippl, E., 2005).

First descriptions being comprehensive w.r.t privacy and addressing collaborative eLearning are Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005) and Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005a).

While the problem statement is already quite detailed there, the description how to solve these problems is just a start. Borcea, K., Liesebach, K., and Wahrig, H., (2005) and this paper are follow-ups detailing the workspace-concept, which in our view is the main vehicle to solve these problems. In addition, the workspace-concept enables to build eLearning systems that adapt to the user and his/her current situation and context – in contrast to the current approaches that require the user to adapt her/his learning behavior to the eLearning system used.

A new approach towards the design of an eLearning environment supporting natural behavior of its users

As stated in section *State of the Art*, current eLearning systems primarily integrate just isolated – sometimes also combined – aspects that comprise interaction, collaboration, and profound didactics. Occasionally, those approaches are realized such that they are only suited for single use cases. However, a comprehensive approach for supporting education using electronic media is missing.

Outgoing from this pretension, we asked the following questions:

- How can the potentials of didactic aspects in eLearning be combined to open up new ways and possibilities especially for eLearning applications?
- How have those possibilities to be designed to provide all users with an eLearning application supporting cooperation, communication, and interaction as well as fostering learners according to their capabilities and qualifications?
- Based on those concepts, how can learning and working environments be realized that integrate the advantages of the scenarios of the non-electronic world?

Considering those issues, we determined two key principles the design process of the eLearning environment should follow:

1. The behavior of the eLearning users within the electronic environment should closely correspond to their natural behavior in and their knowledge of the real world.
2. Each user – independent from one's roles assigned to the different problem areas – should have free access to all functionalities offered by the environment – in the frame of generally agreed rules and directives.

This means that we want to encourage the users' self-determination by providing all possibilities an eLearning environment has to offer with respect to educational functionalities on one the hand, i.e. reading and annotating learning content, autonomously generating learning materials as well as structuring them according to one's own preferences. On the other hand – and this is supposedly the most important new concept of our approach – the user should be able to perform those actions together with other users of the eLearning environment on his/her own initiative. This implies the availability of support for dynamic group building as well as for non-restricted collaboration and communication. Hence, the central objective of the requirement analysis is to establish a system designed for collaborative eLearning supporting self-determination of its users.

Consequently, it is imperative to refrain from the traditional and rigid approach of role handling in eLearning. The system that we describe poses the individual users and user groups as well as their interests and competencies in the centre of the working and learning environment. Thereby, all functions have to be provided users would need to efficiently achieve their learning and working objectives.

Workspaces

Starting by looking at real-world educational scenarios, we recognized that those are characterized by the provision of several rooms for different working processes, e.g. the creation of learning content typically is done in an office; the use of them normally takes place in seminar rooms; and learning groups typically find themselves in individual spaces. In order to provide the users a comparably objective-oriented partitioning of the eLearning environment, various working areas – we use the *workspace* metaphor for that – are the organizational basis of the environment. Such workspaces are

“equipped” with all necessary functionality and means for an objective-oriented coping with tasks and interactions:

- users and their roles,
- functional modules as well as
- the contents to be worked on.

Current approaches require privileged entities who decide about the creation and the “equipment” of new workspaces. Our idea is geared to the common understanding of democracy: It gives each user of the eLearning environment – independent of his/her individual roles in other workspaces – the possibility to create and configure new shared workspaces of his/her own.

Roles

Even if the enrollment process does not assign users to specific *roles* (such as author, tutor, or learner), nevertheless, for an efficient proceeding of the learning and working processes, the implementation of roles is essential. To make the understanding of the association easier, we would like to give a description of how the real world scenario looks like: Outside of a concrete institution which possesses a special function, people move without a particular role assignment. With the moment they get in touch with someone else, roles become an important factor of social life. The same is valid in case of learning environments as well as special workspaces where users interact with each other. The actual role assignments and their use in a workspace follow the problem areas that have to be worked on as well as the particular approach the users chose for the elaboration of tasks.

Functional Modules

The functionality within a workspace is provided by so-called *functional modules*, the concrete selection of which also depends on the intended actions and interactions. Therefore, they comprise the functional basis for acting in the workspaces and, consequently, also in the whole learning environment. With the functional modules, tools are provided that allow for collaborative elaboration of knowledge (e.g. by the integration of tools for creativity techniques) and documents (e.g. cooperative authoring tools), for structuring contents (e.g. flat, hierarchical or web structures) and communication (e.g. discussion fora or chat) as well as for interaction between users (e.g. whiteboard).

Content artifacts

The third characteristic of workspaces comprises the knowledge itself that is objectified in the form of content artifacts. Those artifacts are elaborated and utilized by the users in the frames of their role and with use of the corresponding functional modules. Thereby, when bringing the elaborated contents into use, we do not distinguish between the contents that were created using a specific functional module, i.e. the description of a glossary term is likewise a content artifact as, for instance, a chat message or a cooperatively elaborated document and can, for instance, be presented as one material in a learning module.

Design of a privacy-enhanced as well as a privacy-aware collaborative eLearning environment

The possibility of storing data in a huge commonly accessible “brain” is, on the one hand, a great potential for the knowledge society. But, on the other hand, it implies a high risk for the user’s privacy. Thus, if we want to map cooperative learning and working from the real world to electronic

learning environments, it appears that there is also a fundamental need for the provision of according privacy-preserving means. These should enable the user to manage as well as to control the disclosure of his/her personal data – as (s)he is used to do in real life – and, hence, protecting her/his privacy.

At this point, our objective is to support users in managing their learning processes and to partition their activities such that a reasonable collaborative working as well as the protection of their privacy is possible. To reach that objective, the design process of the overall system has to follow two privacy-related key-principles:

- Processing a user's personal data at the eLearning server has to be reduced to a minimum.
- The users get the possibility to keep track of all transactions related to their personal data, which allows for maximal transparency.

Based on the partitioning of user activities within the eLearning application, the possibility to configure rules for disclosure of personal data (especially in collaborative scenarios, where interactions between several users of the eLearning environment take place) in order to protect one's own privacy. Moreover, the provision of additional information describing the context of the collaborative eLearning environment the user is currently acting in is necessary in order to arise the user's awareness of privacy aspects. That means, in order to establish a privacy-enhanced and privacy-aware collaborative eLearning environment, the integration of privacy and security aspects has to take place at different (application) levels.

In traditional eLearning applications, the user has to indicate clear attributes, e.g. her/his full name and matriculation number, in order to set up her/his login and to get access to the system. Since this login is unambiguously known on server side, a possibility is established to link the user's name with each of her/his attributes of the user profile. Typically, user profiles contain sensitive data like passed and failed exams, grades, and visited courses. Consequently, by linking this data it is not difficult to generate a comprehensive picture of the user, his/her properties as well as abilities and finally her/his identity.

In contrast, our approach allows for completely anonymous acting in the eLearning environment as long as the user did not enroll into e.g. a workspace to take learning courses, yet. While anonymous, the user may read up on offered workspaces and courses and take up accessible functionalities, e.g. unrestricted chats and fora. Since the users do not communicate their name or login to the server, the eLearning application is not able to unambiguously identify the real persons doing the interactions.

Nevertheless, completely anonymous acting within the eLearning environment is not sufficient, if the user wants to engage support by the tutor (e.g. consultation and exam purposes as well as assessment of learning results and processes) and keep in touch with other learners (e.g. for communication purposes and cooperative working), respectively. But in contrast to traditional eLearning environments offering exactly one login per user, the user of our system should have the possibility to use different "logins", i.e. uncorrelated pseudonyms (Pfitzmann, A. and Hansen, M, 2005), for acting in the system. That means, the user of our eLearning environment should decide self-determined, in which context (s)he will use a particular pseudonym (Chaum, D., 1981). The system should only support her/him by means of indicating situations for possible pseudonym switches based on the current context (Borcea, K. et al, 2005). A context describes a specific situation in which a user works to perform a task. Within our system, contexts are used as means to partition personal data based on separating activities in the eLearning application. The granularity of a context depends on the definition of tasks and subtasks. Each time the user wants to perform a new task, a context switch is caused. This context switch is a potential point to change the pseudonym used.

Furthermore, the granting of access rights takes place based on anonymous, but certified attribute values, which are called credentials (Chaum, 1985). The user has to disclose the requested attribute, e.g. "exam passed: yes/no", to the application, whereas the system is not able to draw conclusions

from the disclosed attribute characterizing a particular property or ability of the user to her/his identity in real life.

Here, the decision about the disclosure of attributes requested by the eLearning application takes place self-determined by the user: (S)he may decide, when (s)he reveals which data to the system, i.e. the user is enabled to partition her/his personal data and to control disclosure of data subsets (Clauß, S. and Köhntopp, M., 2001) (cf. Figure 1). Each of these subsets of information is called a partial identity (Pfitzmann, A. and Hansen, M., 2005), which has to be unlinkable by other users as well as by the eLearning system itself. Therefore, uncorrelated pseudonyms have to be used as identifiers for these partial identities.

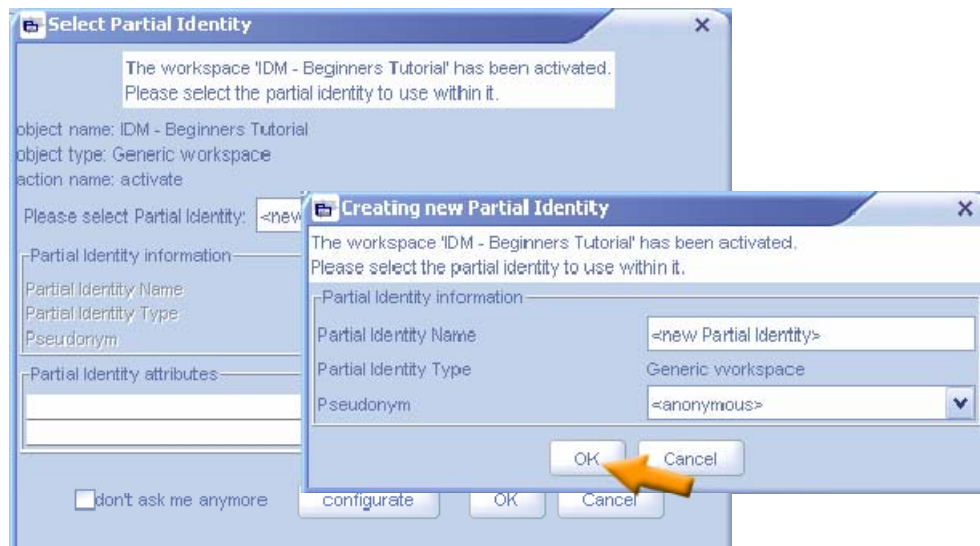


Figure 1: Example for intra-application data partitioning (Privacy Context Management): Configuration of a context by selecting the according partial identity

Since a user could act under various pseudonyms characterizing his different partial identities (quasi)simultaneously, (s)he is not anymore unambiguously identifiable and reachable via her/his identity by other users. Therefore, there are also special requirements on the eLearning environment regarding the collaborative and cooperative working and learning, which are described in the following paragraphs.

One of these issues concerns support to build dynamic groups. Especially in cooperative eLearning scenarios, establishing such groups is of great importance. Depending on objectives and tasks, which have to be elaborated, new learning and working groups as well as subgroups could be formed. Once they achieve their objectives, groups could disperse completely or partly. Therefore, the eLearning application should provide mechanisms to support building of groups based on credentials and properties in order to define conditions, e.g. prerequisites like passed classes a user has to have in order to become a member of the group. Additionally, functions should be provided to contact possible group members by searching for specific properties and attributes as well as to manage defined policies.

Besides the support of building groups, in order to allow a reasonable work within the groups, different mechanisms for intra-group management are necessary. Thus, the group members should be able to negotiate special, potential activities. Two simple examples that underline this requirement relate to a plain chat module: Negotiations are fundamental prerequisites when the users of a chat room have to decide if the communication will be logged. Furthermore, there could be negotiated restrictions on the possibilities a user has who is not willing to be visible in a chat room.

In order to foster the objective-oriented work in the workspaces as well as in the overall eLearning environment, the use of reputations and their management become an important factor. However, in a

privacy-enhanced environment it is not possible to rely on reputations firmly attached to an identity. Therefore, the eLearning application should integrate according mechanisms that allow for assessment of an effort (definition of a reputation) as well as with the use of such assessments when deciding about future activities of a user or a user group, respectively.

To facilitate the establishment of a privacy-aware collaborative eLearning environment, the provision of an appropriate user interface is indispensable. Here, we have to find a balanced compromise between presentable information concerning the avoidance of cognitive overload and needed information in order to support the user's awareness of her/his current privacy state, i.e., of the linkability of her/his actions for other users or the eLearning system, i.e. its servers, itself. Therefore, we have introduced a so called InfoCenter in our eLearning application, which is always present in the user interface. It provides information related to the workspace in which the user is currently working. Particularly, the InfoCenter provides information about her/his own partial identities, partial identities of other users, about the current workspace and functional module (cf. Figure 2).

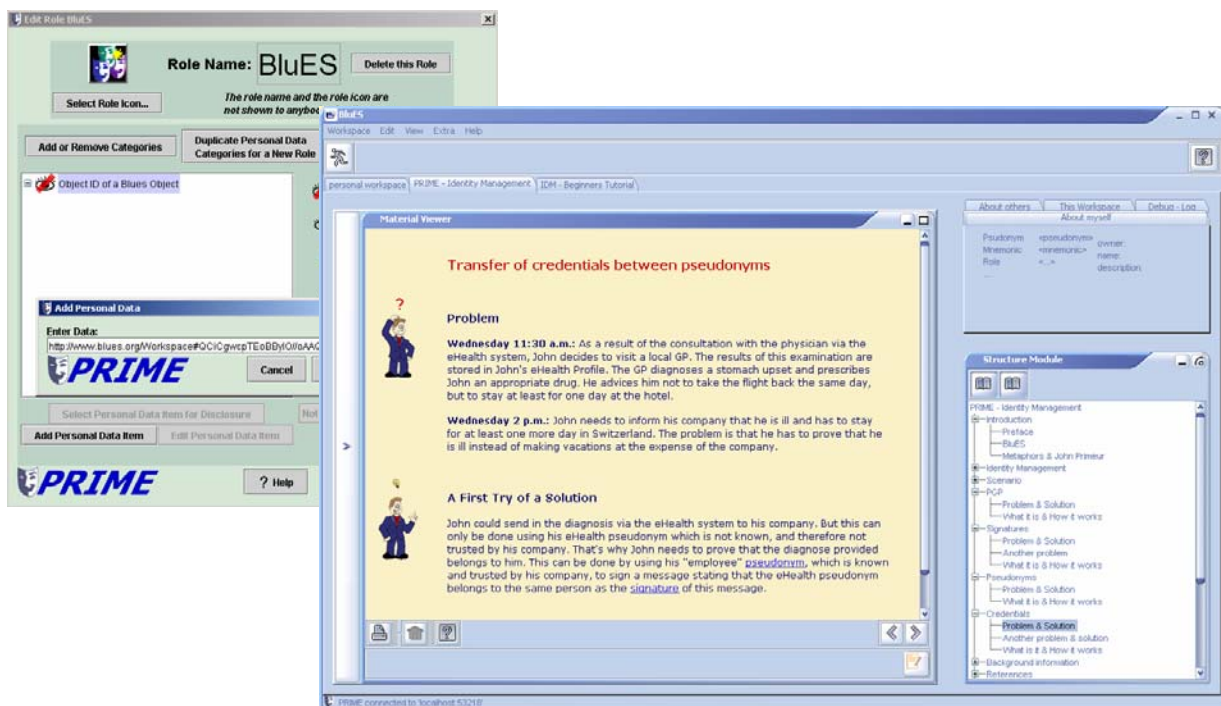


Figure 2: Screenshot of the interplay of the BluES'n environment and the PRIME user-side component: Passing personal data to the privacy-enhancing identity management system PRIME to be managed there.

Conclusions

In future, eLearning will be a collaborative activity, meaning that several users (learner, tutors, authors) work together both to support learning and to improve learning materials. Roles will be taken and abandoned "on demand", i.e. someone being a learner may spontaneously become a tutor to some other learners within an ad-hoc self-help learner's group or it may become an author by annotating learning content or even creating new one from scratch. Besides various kinds of support for communication, collaboration support by the eLearning system has to cover ease-of-use, multilateral security and privacy.

We described why and how the workspace paradigm may support ease-of-use and privacy. In addition, it supports multilateral security.

BluES'n, a first proof-of-concept implementation of such an eLearning system has been finished within the EU-funded Integrated Project PRIME end of October 2005 (cf. PRIME, 2005). During the

next months, BluES'n will be evaluated and further enhanced. Since BluES'n is an Open Source project (BluES, 2005), everybody is not just only invited to participate in its evaluation, but invited to contribute to its evolution as well.

Acknowledgement

We thank Hagen Wahrig and Alexander Böttcher for doing the implementation with us, Elke Franz for her contributions on Management of Privacy-Context Switching, and them and all PRIME partners for various support and encouragement.

References

BluES (2005). URL: <http://blues.inf.tu-dresden.de>.

Borcea, K., Donker, H., Franz, E., Liesebach, K., Pfitzmann, A., and Wahrig, H. (2005). Intra-application partitioning of personal Data, Workshop Proceedings of PEP 2005, Edinburgh, Great Britain.

Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005). Privacy-Aware eLearning: Why and How. Conference Proceedings of ED-MEDIA 2005, Montreal, Canada.

Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005a). Towards Privacy-Aware eLearning, Workshop Proceedings PET 2005, Dubrovnik (Cavtat), Croatia.

Borcea-Pfitzmann, K., Liesebach, K., and Wahrig, H. (2005). Das Workspace-Konzept - neu verpackt im eLearning! Workshop Proceedings of DeLFI 2005 and GMW05, September 2005, Rostock, Germany.

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM (24:2), 1981, pp. 84-88.

Chaum, D. (1985). Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM (28:10), 1985, pp. 1030-1044.

Clauß, S. and Köhntopp, M. (2001). Identity Management and its Support of Multilateral Security. Computer Networks (37), 2001, pp. 205-219.

EU (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

Klobučar, T., Seničar, V., and Jerman-Blažič, B. (2004). Privacy and personalisation in a Smart Space for Learning, Int. J. Cont. Engineering Education and Lifelong Learning (2004), vol. 14, pp. 388-401.

Pfitzmann, A. and Hansen, M. (2005). Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management — A Consolidated Proposal for Terminology. Draft status, August 2005. URL: <http://dud.inf.tu-dresden.de/literatur/Anon-Terminology v0.23.pdf>.

PRIME (2005). URL: <http://www.prime-project.eu.org>.

Weippl, E. (2005). Security in E-Learning. eLearn MAGAZINE. URL: <http://www.elearnmag.org/subpage.cfm?section=tutorials&article=19-1>.