Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 27 (2005) 561–578

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Privacy provision in e-learning standardized systems: status and improvements

Borka Jerman-Blažič*, Tomaž Klobučar

Laboratory for Open Systems and Networks, Jožef Stefan Institute, Jamova 39, 1001 Ljubljana, Slovenia

Received 16 February 2004; received in revised form 2 September 2004; accepted 8 September 2004
Available online 12 October 2004

Abstract

Privacy is understood as a freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. Appropriate use of technologies may provide privacy and data protection; however, these technologies require relevant attributes in the databases containing information that need protection. These are not obvious in the existing e-learning standard schemes. This paper discusses first the current e-learning standards regarding the schemes used for defining, storing and managing user profiles in e-learning standardized systems. Later, it gives an overview of the requirements for privacy provision and discusses the elements required in such systems. Comments and assessments of the existing solutions are given. An enhanced solution being developed within the ELENA project from the European IST 5th Framework Programme is described. The new solution is built up on the existing standards, but it introduces new features enabling better protection of sensitive data and more efficient management, enabling the users to decide about the relevant protection.

Keywords: E-learning systems; Standardization; Learner profile; Privacy

1. Introduction

Advances in information and communication technologies, and specifically in multimedia, networking and software engineering have promoted the appearance of a huge amount of learning resources. During the last years, thousands of electronic texts, images, movies, Java applets or complete electronic courses have been developed for learning purposes in Internet environments. New services were developed, and the search, classification, organization and exchange of learning resources by learners, instructors, course developers and human resource developers have become common marketplace. The appearance of the technological capabilities for a common e-learning marketplace and the huge amount of learning resources allowed a high number of

* Corresponding author. Tel.: +386 1 4773 408; fax: +386 1 423 2118.
E-mail address: {borka,tomaz}@e5.ijs.si (B. Jerman-Blažič).

0920-5489/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2004.09.006

technology-based learning platforms to show up. As they were usually developed ad hoc to meet the requirements of a particular institution, heterogeneous systems appeared with no interoperability mechanism provision. Careful analysis of these systems has shown that they provide very similar functionalities, such as content delivery, learner tracking, learner management and administration, questionnaires evaluation, communication and collaboration facilities, search tools, etc. [1]. In other words, they have common functionality.

In parallel with the development of the high number of technology-based learning platforms, a standardization process started in the e-learning area. Standards are usually defined as "documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, and services are fit for their purpose" (FDIS 15944-1). In the context of e-learning, technology standards are generally developed to be used in the system design and implementation for the purposes of ensuring interoperability, portability and reusability, especially for learning resources as they require for their preparation qualified professionals and are very timely demanding. The standardization of these reusable learning resources is focused to metadata, enabling standardized description and indexing. Metadata helps to carry out the tasks of selecting, assembling and managing the offered e-learning services. Several specifications for learning object description were produced in the last years [2]. Related to them, specialized search engines and indexing tools for learning were also made available [3].

E-learning standards are often multipart, typically consisting of: (1) a "data model", which specifies the standard's normative content in abstraction; (2) one or more "bindings", which specify how the data model is expressed in a formal way, which is most often XML based; and (3) an Application Programming Interface (API) or "service definition" that defines points of contact between cooperating systems. Important part of the e-learning system providing services on the common marketplace is the *Learners Administration.* This part of an e-learning system provides support for management of the administrative information concerning *Learners*, representing students or trainees. Implementation of the administration is expected to contain introspection mechanisms for identification of the supported profile data models of the e-learning system customers and to manage the learner's evolution through the consumed learning services. This part of the e-learning system also provides the business logic for *Learner* registration and enrolment. The design of these profiles requires careful inspection and approach as the attributes used in the profiles and the granularity of the profile data regarding the performance of the system influence in many aspects the e-learning system. In this context, special attention in the design deserve the attributes related to privacy and data protection. These attributes enable implementation of technologies that guarantee the privacy and data protection of the learner. Privacy is here understood as freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual [4]. Privacy relates to the controlling of the unauthorized copying or gathering of information, controlling transfer of information or other techniques that may lead to any kind of misuse. Internet operators, service providers and other users can use the learner information collected for various purposes, e.g., to support personalised view of the systems and provide personalised content, but also for unsolicited marketing, price discrimination, government surveillance or identity theft.

Appropriate use of the technologies that provide privacy and data protection demands relevant attributes in the learner profiles and databases. These are not obvious in the existing e-learning standard schemes. In this paper, we are analysing the existing standards in the learners administration part of the e-learning system regarding privacy provision policy and relevant user data. After careful analysis and based on our findings, a scheme together with the relevant attributes is proposed that overcomes the deficiencies in the existing solutions. The solution is being developed in the European project from the 5th Framework Program with a name "Creating a Smart Space for Learning" and acronym ELENA [5].

The paper is organized as follows. In the next section, we present the elements required for privacy and data protection provision. Section 3 gives a short overview of the current standardization in e-learning, Section 4 analyses the privacy attributes in e-learning

profile standards, while Section 5 provides comments and assessments, including presentation of the solution being developed in the ELENA project that introduces new features in the context of privacy provision in e-learning systems. The paper finishes with comments in the Conclusion.

2. Privacy and security provision in e-learning systems

2.1. Privacy threats

In order to identify relevant data and attributes required for privacy provision and data protection, we will have a short look at the threats that the learner and her personal data might be exposed to. The general privacy threats in the communication network are known as identity disclosure, linkability of data, observability of data, location disclosure in mobile networks or data disclosure [6]. Privacy and security mechanisms that could help against those threats are described in more detail in the next section.

The identity disclosure often happens through identification mechanism enabled over the web, either by identification through the IP address of the learner's browser or through technology known as "cookies". These two identification mechanisms can be used to provide means to outside parties for tracking, linking, profiling and monitoring the activities of a learner. The HTTP cookie is a file mechanism that creates the opportunity for more automated interaction between a web server and a client—it provides the remote server with a 'memory' of a user's identity. Cookie files may typically store information about an e-customer's personal ID, recent activities at a web site, credit card details or site password information. However, cookies are also a technology that has a number of inherent flaws that pose additional threat to personal privacy, e.g.:

Security failures: Sensitive information is often stored in cookies, which can be passed openly over the Internet. The contents of a cookie are, in theory, accessible to anybody capable of intercepting the cookie on the Internet or maliciously gaining remote access to a networked computer.

Monitoring: Many people believe that user identification via cookies is an invasion of their personal privacy. People are at liberty to enter a retail store in the physical world with anonymity and without their purchases or activities being recorded or monitored. Privacy advocates feel that the same choice for anonymity should be available during browsing an e-learning market place. Cookies may also permit a third party to investigate the activities of an individual in case this third party has access to their computer and their cookie files.

Data Disclosure: An e-learning market place that has personal information about a learner, stored via cookies, may exchange this data with other sites (for example, related educational partners or sites that buy advertising space from them). This sharing of data may extend as far as cookies being synchronised for a group of educational activities. This implies that personal information supplied voluntarily at one site may be used to track or identify an individual at other sites where they have never intentionally disclosed such information.

Limited control: In the latest web browsers, learners have some control over the content and use of cookies, although to most users, they are still totally invisible technology. Web browsers provide the user with an option to disable cookies (i.e., to not accept them) or delete them. However,

this can often make some sites totally inaccessible.

Collecting data: One way of using cookies for collecting personal data invisibly or for assigning users a unique identifier is via links to a mechanism typically described as a Web Bug. A Web Bug is a graphic, usually defined as a blank image that is 1 by 1 pixels in size, on a web page or in an e-mail message that is designed to monitor the user of the web page or reader of the e-mail message. The Web Bug is typically placed on a web site by a remote third party, in order that the activities of a web site user can be monitored indirectly. Web Bugs are also used to gather statistics about web browser usage at different places on the Internet. Web sites that are invisibly hyperlinked can place cookies and collect typed keywords, unless the learner disables this option in his/her web browser. Tools also exist that can check whether a web page contains Web Bugs (e.g., http://www.bugnosis.org).

Privacy threats can be prevented by adoption of appropriate privacy protection policy by the learning service provider and at the learner side, by use of appropriate security mechanisms, such as encryption and digital signature, and by privacy protection mechanisms, such as anonymisation, private credentials or identity management. Provider's privacy policy must be known and visible to the learner. However, this is not sufficient. There are other threats that, if not prevented, may cause additional breaches of privacy and may endanger the security and confidence of the learners in the e-learning process. For example, it is quite common for the profiling databases to hold references to millions of web clients—potential customers of the web-based learning space. Many e-learning web sites have associations with commercial information brokerage companies or publishing companies. These sites make use of cookies to monitor client's activities at the host site and record the data that were provided to the web server. Learner's interests, browsing patterns and selecting courses, affiliation and advancement in the learning process are stored as a profile in a database without their knowledge or consent. This profile information is used to decide which advertisements or services will be offered later at the affiliated web sites. The information is typically collected and stored without the learner's knowledge or, more importantly, consent. The information collected is purported to be nonpersonally identifiable; however, where a learner provides personal data to the web server (e.g., name and address) the data are correlated with e-mail addresses, IP addresses and demography, to create a far more personalised profile.

Technological tools that assist in safeguarding online privacy show a range of characteristics. Some filter cookies and other tracking technologies, some allow for "anonymous" Web browsing and e-mail, some provide protection by encryption data or digital signature methods and some allow for the advanced, automated management of users individual data on their behalf. In essence, these technologies reinforce transparency and choice, which can lead to greater individual control of data protection. Different products, technologies and various functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology.

2.2. Requirements for privacy and data protection and relevant technologies

Taking into account the threats presented above to the environment of the online e-learning systems and drawing some conclusions regarding the list of the main privacy threats, this may lead to the list of requirements regarding provision of privacy and data protection in e-learning service environment. These requirements are:

- Learner personal data must be protected, i.e., integrity and confidentiality guaranteed, in communication between the learner and the educational

node, and in the learner profile where the data is stored.
- The learner's personal environment, for example, personal learning assistant (PLA), and the educational node must be provided with appropriate control in the internal processing of the data in order to control and regulate the disclosure of the learner's data. The learner must be able to decide what privacy-sensitive information is given at which stage and to whom.
- The learner must be able to formulate her privacy demands and wishes, for example, by attaching the privacy preferences to personal data attributes.
- The service provider should prevent unauthorized access to the e-learning environment—the environment should be protected against attacks from other entities in the system that may manage to get an access to the learner profile data.
- The learner's personal environment, where learner's personal data is stored, must be able to distinguish between the public and private data—in order to make appropriate decisions regarding permissions for interactions of the learner with e-learning site.
- The e-learning service provider must have its privacy policy declared and published.

In order for these requirements to be met, the appropriate privacy policy of the educational node should be adopted, and additional data in the learner's profile added in order for the privacy-enhancing technologies to be applied and to work. Privacy-enhancing technologies (PETs) are nowadays considered to be helpful technological tools to assist in protecting online privacy as part of a wider package of online privacy framework [7]. PETs can be deployed on the learner side, for example, in her personal learning assistant, at the provider's side for protecting customers' data, but also need to be supported by the underlying infrastructure. They can empower individual users seeking to control the disclosure, use and distribution of personal information online. PETs enable organizations in enforcing their privacy policy and practice. They are crucial tools in managing the flow of personal information on global networks.

In the last few years, several privacy-enhancing technologies and practices appeared with a goal to provide means for privacy provision. One of the most well known is the Platform for Privacy Preferences or P3P, developed by the WWW Consortium [8]. Using P3P learning service provision sites can encode their data collection and data use practices in a machine-readable XML format known as P3P policy. Browsers can compare site policies against user privacy preferences (specified in APPEL [9] or by other mechanisms in the latest web browsers) and take actions based on the comparison, for example, for cookies blocking decisions. Another system has been developed by IBM, known as Enterprise Privacy Authorization Language (EPAL) for encoding an enterprise internal privacy-related data handling policies and practices [10]. EPAL and P3P have different goals. While P3P enables automated matching between privacy policies and learner preferences, EPAL allows privacy enforcement system.

Another approach is the Hippocratic databases that include responsibility for the privacy of data [11]. They incorporate 10 fundamental privacy principles that are then applied in different context, e.g., in decisions dealing with answers to queries sent to the database. The system first checks whether the user issuing query is aiming the users authorized by the privacy policy for that purpose. Next, the database analyses the query to check whether it accesses any fields not explicitly listed for the query's purpose in the privacy policy. Finally, the database ensures that only records having a purpose attribute that includes the query's purpose will be visible to the query, thereby enforcing any "in" or "out" preferences.

Other approaches fall in categories known as identity protectors and identity management systems, anonymous web proxies and remailers, mix networks, private credentials, etc. [7,12,13]. Useful concepts for personal data protection are pseudonymity and anonymity. An identity protector can be seen as a system element that controls the exchange of the identity between the system elements. Identity protectors generate pseudoidentities and convert learner's identity into pseudoidentity. Anonymizers range from centralized privacy proxies, such as anonymizer.com, to decentralized mix networks and Web browsing networks, such as Crowds from AT&T [4]. In fact, some companies, like iPrivacy.com, allow users to anonymously use their services by arranging special arrangement with credit card companies. Here, crypto-

graphic protocols are used as well especially in authentication mechanisms and access control. Recently, the most actual approaches based on P2P communication are used for decentralized authentication and access policy-enforcement mechanisms to support uniform searching of restricted content.

An important aspect is privacy-friendly access control. Educational service access control decisions are still too often identity based. Access to learning services is granted or denied according to user's personal information, such as name or date of birth, that have to be disclosed to the service providers, rather than on credentials and other characteristics (e.g., being over 18, being a member of an association, or just having enough amount of electronic coins), which are sufficient to prove the authorization to access the services without revealing one's identity. Authorization schemes should be compliant with the "minimal disclosure of personal data" principle. Credentials, such as attribute certificates, or private credentials can be used for privacy-friendly access to learning services [7]. Shibboleth, a project of Internet2/MACE, for example, uses attribute certificates to support interinstitutional sharing of learning resources that are subject to access control.

However, we must bear in mind that the total solution for privacy provision must combine laws, markets and technology. Here, we are interested to see how the current e-learning standards answer regarding the needs for technology application that provide protection of privacy and security of the stored and collected data. For that purpose, we analyse the existence and appropriateness of the privacy and security attributes available in the e-learner profiles specified in the e-learning standardization documents and known approaches. The evaluation outcome will provide us with basic information that may suggest further improvement and possible acceptable solutions.

In order to find the appropriate answers in the next chapter, we are expecting the existing standards the data and the attributes defined in the learner's profile. The overview of these data can give us a view if the known techniques for security and privacy provision can be applied in the developing e-learning space according to the internationally adopted standards.

3. E-learning standardization

The e-learning standardization process is an active, continuously evolving process that will last for years to come, until a clear, precise, and generally accepted set of standards for educational-related systems is developed. Among the main contributors to this effort are the IEEE's Learning Technology Standardization Committee (LTSC) [14], the IMS Global Learning Consortium [15], the Aviation Industry CBT Committee (AICC) [16], and the U.S. Department of Defense's Advanced Distributed Learning (ADL) [17] initiative and the reference model known as Sharable Content Object Reference Model or SCORM. Projects such as Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE) [18], Getting Educational Systems Talking Across Leading Edge Technologies (GESTALT) [19], PROmoting Multimedia access to Education and Training in EUropean Society (PROMETEUS) [20], Gateway to Educational Materials (GEM) [21], and Education Network Australia (EdNA) [22] and the European Committee for Standardization, Information Society Standardization System, Learning Technologies Workshop (CEN/ISSS/LT) [23] are also contributing to the e-learning standardization.

The outcomes of these standardization efforts can be identified into two levels:

(1) *Specification of the information models involved*. Several proposals have been produced to specify the format, syntax and semantics of data to be transferred among heterogeneous platforms (e.g., courses, e-learner profiles, evaluation objects, etc.).
(2) *Specifications of the architectures, software components and provided interfaces*. So far, in this area, results are not so advanced as in the previous layer. New attempts are oriented towards more service- and P2P-oriented architecture embracing the ontology developed for semantic Web approaches.

The more mature results regarding e-learning standardization correspond to the first level. In most cases, XML is used to define supporting information models enabling interoperability in Web environment. Standards at this level can be seen as common

specifications that are intended to be used by different vendors in order to produce learning objects and other relevant components of the e-learning system.

Relevant specifications at this level are being developed by the following organizations: IEEE LTSC, IMS and Internet2/EDUCAUSE [24]. The IEEE LTSC is developing models for:

- Metadata (this is one of the most active standardization areas, and several proposals are available): information here is used to define, as precisely as possible, educational contents. The most outstanding contribution so far is the Learning Object Metadata (LOM) specification, which is becoming a de facto standard.
- Learner profiles and records in information that characterize e-learners, their knowledge and preferences. The Public and Private Information (PAPI) of IEEE LTSC specification [25], which is now being developed by ISO JTC1/SC36, describes implementation independent learner records.

IMS Learner Information Packaging Specification and the IMS Enterprise Data Model are being developed by IMS Global Learning Consortium (http://www.imsproject.org). IMS is a worldwide non-profit organization that includes more than 50 contributing members and affiliates.

The Internet2/EDUCAUSE specification was produced by the Internet2 Middleware Architecture Committee for Education, the Directory Working Group eduPerson task force. The task force had a mission of defining an LDAP object class that includes widely used person attributes in higher education.

At the second level, e-learning standards define the expected behaviour of software components responsible for managing learning objects in online environments. The software interfaces for educational components enabling building up of new e-learning systems without being developed from scratch, and are also aimed to provide interoperability among heterogeneous systems at runtime. The IEEE LTSA specification corresponds to a conceptual model applicable to a broad range of learning scenarios. It is pedagogically, content, culturally and platform neutral. In the United States, the IMS project started in 1997 defining a system model and architecture for learning environments. They abandoned this work very soon, as they considered of prior interest the development of data and information models to be managed by such architectures.

4. Privacy and security attributes in e-learner profiles in the current standardization scheme

The use of the information about a user in order to adapt the interaction of the e-learning system with the information resource is well established. The stored information about the learner is referred as a user profile or user model, in our case, the learner profile or the learner model. Many adaptive systems among which we classify modern e-learning systems contain an embedded learner model or learner profile that is used for personalisation and adaptation. In this paper, we consider the content of the user profile to be modelled by data types that belong to three types of information: user data, usage data and environment data, according to the specification given in the paper of M. Teltzrow and A. Kobsa [26]. User data denotes information about personal characteristics of the user, while usage data is related to a user's interactive behaviour. Usage regularities are related to the user behaviour and based on frequently reoccurring interactions of users and environment data focuses on the user's software and the hardware and the characteristics of the user's current locale or origin. Within the user (learner) data, the following characteristics are considered: demographic data, affiliation, relationship, user knowledge, skills and capabilities, past achievements and certificates, user interests and preferences, and user goals and plans. The usage data includes selective user actions, temporal viewing behaviour, ratings, purchases, and other conformity and discomformity actions. Usage regularities are covered by usage frequency, situation–action correlations, action sequences and data about the hardware and software used and the locale of the user (localization characteristics of the computing system used by the user). It is clear that most of these data are very sensitive in the context of privacy and as such they need to be protected.

The e-learning standards have different categorisation of the user data and the relevant categories. Here,

we are reviewing four of them: the IEEE LTSC Personal and Private Information draft standard, the IMS Learner Information Package (LIP), the Internet2/EDUCAUSE EduPerson collection of attributes and the Universal Learning Format (ULF). As some concepts of the standards and approaches for describing general users can also be relevant for learner profile standardization, we also briefly assess Extensible Customer Information Language (xCIL) specification, developed by OASIS [27], CPExchange [28] and UserML [29].

4.1. IMS

4.1.1. General information

Learner Information in the IMS Learner Information Package (LIP) is a collection of information about a learner (individual or group learners) or a producer of learning content (creators, providers or vendors). The IMS LIP specification addresses the interoperability of internet-based learner information systems with other systems that support the Internet-based learning environment [30]. The intent of the specification is to define a set of packages that can be used to import data into and extract data from an IMS compliant e-learner information server. A learner information server may exchange data with learner delivery systems or with other learner information servers. It is the responsibility of the learner information server to allow the owner of the learner information to define what part of the learner information can be shared with other systems.

The IMS LIP is more focused on other learner information, i.e., information such as administrative activities in a manner in which they interact with learning activities. The typical sorts of learner information to be supported in LIP are: education record—the record of educational achievement from school through to college/university; training log—the record of training activities undertaken, e.g., courses carrying formal certification; professional development record—the record of professional development activities undertaken including membership in the appropriate professional bodies; resume/CV—a record of personal achievement that includes relevant work experience, qualifications and education history, different types of resumes need to be supported, e.g., business, academic, medical, etc.; lifelong learning record—a cradle-to-grave record of the learning activities and achievements of an individual. The time-related nature of the record is reflected by the sequential nature of the information and the tagging of the specific record by its date of entry and the community service record—a record of the community-oriented activities of an individual as well as the corresponding work and training experience.

Learner Information Package is based on a data model that describes the characteristics of a learner required for recording and managing learning-related history, goals and accomplishments, engaging a learner in a learning experience and for discovering learning opportunities for learners. The specification supports the exchange of learner information among learning management systems, human resource systems, student information systems, enterprise e-learning systems, knowledge management systems, resume repositories and other systems used in the learning process. In IMS specification, such systems are called learner information systems regardless of any other functionality they possess or roles they fulfil. The IMS Learner Information Package specification does not address requests for learner information or the possibility of the existence of exchange transaction mechanism. IMS Learner Information Package is a structured information model. An XML binding is included but is not meant to exclude other bindings. The information model contains both data and metadata about that data. The model defines fields into which the data can be placed and the type of data that may be put into these fields. Typical data might be the name of a learner, a course or training completed, a learning objective, a preference for a particular type of technology, and so on. Metadata about each field can include: time-related information, identification and indexing information; and privacy and data protection information. This metadata is available for each and every field in the information model, either directly or via inheritance.

General categories of Learner Information data in IMS LIP contain characteristics about the consumer or producer that affect learning in some way. Learners are usually individual learners, but they can also be learning groups. Producers may be organizations or

individuals, and include three general categories: creators of the learning resources, providers that deliver the learning resource and vendors providing technology tools required in e-learning process. The primary learner information as specified in IMS LIP is presented in Fig. 1. The figure also gives a structure of the *securitykey* attribute.

4.1.2. Privacy and security attributes

According to the IMS LIP specification in the learner information tree structure, each node and leaf can have an associated set of privacy information (the usage of these fields is optional). This information that can be used to describe the level of privacy, access rights and integrity of the data is part of the privacy and data protection meta-structure. The granularity of information that can be exchanged is defined by the smallest set of data at which there is no further independent privacy data. However, in the IMS LIP specification, it is claimed that the nature of the privacy data is beyond the scope of that specification as all that is defined within the LIP is the place at which such information is associated with the learner information data structure. The support for learner information that will be used to enable the secure and/or authenticated transfer of the data is enabled with the attributes described as the learner security keys. These attributes include the learner's public keys for public key encryption, passwords for access to the information (electronic and verbal) and digital signatures to be used to ensure data authenticity. The detailed structure for the keys in the IMS LIP is not defined.

4.2. The IEEE LTSC Public and Private Information (PAPI)

4.2.1. General information

The PAPI Learner Standard is a multipart standard that specifies the semantics and syntax of information about learners. Learner information may be created, stored, retrieved, used, etc., by learning technology systems, individuals (e.g., teachers, learners, etc.) and other entities, and due to this property, they are considered as portable. The PAPI Learner Standard [31–34] defines and/or references elements for recording descriptive information about knowledge acquisition, skills, abilities, personal contact information, learner relationships, security parameters, learner preferences and styles, learner performance, learner-created portfolios, and similar types of information. The standard permits different views of the learner information (known perspectives could be: learner, teacher, parent, school, employer, etc.) and substantially addresses issues of privacy and security. The PAPI Learner Standard is a data interchange specification, i.e., it is used for communication among cooperating systems ("cooperation" may be achieved by conformance to the PAPI Learner Standard and, possibly, other specifications). The data could be exchanged: (1) via external specification, i.e., only PAPI Learner coding bindings are used while some other data communication methods if they are mutually agreed upon by data exchange participants; (2) via control transfer mechanism to facilitate data interchange, e.g., PAPI Learner API bindings; or (3) via data and control transfer mechanisms, e.g., PAPI

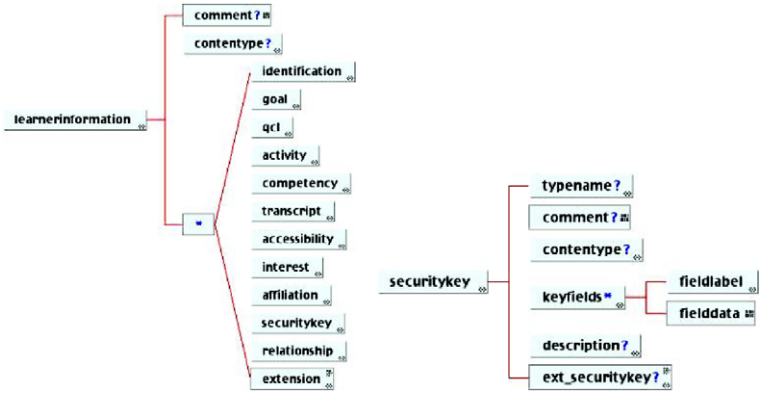

Fig. 1. Primary learner information as specified in IMS LIP and securitykey attribute.

Learner protocol bindings. An important feature of the PAPI Learner Standard is the logical division that separates security and the administration of several types of learner information. These types of information are denoted in the standard as "profile information" and "learner profiles". The PAPI Learner Standard may be integrated with other systems, protocols, formats, and technologies. It is organized in six parts covering different aspects, e.g., the *Core Features* describes the main data model and references to other standards, the *Rationale* gives an explanation of important decisions during the development of this Standard, the *Learner Information Security Issues* provides information and recommendations on important security issues for implementations, the *Examples and Illustrations* specifies information for implementers, the *Registration Authority Process* provides how data elements, value space, coding schemes, code sets, etc. are registered, and the *Data Element Registry* specifies the registry of data elements, value space, coding schemes, code sets, etc. The second part dealing with learner information security issues is organized in six subparts specifying important information in the learner's profile, such as:

- *Learner Contact Information*, e.g., name, postal address, telephone number, etc.
- *Learner Relations Information*, e.g., classmates, teammates, mentors, etc.
- *Learner Security Information*, e.g., public keys, private keys, credentials, etc.
- *Learner Preference Information*, e.g., as useful and unusable I/O devices, learning styles, physical limitations, etc.
- *Learner Performance Information*, e.g., grades, interim reports, log books, etc.
- *Learner Portfolio Information*, e.g., accomplishments and works, etc.

The high-level architecture of the PAPI profile is given in Fig. 2.

4.2.2. Privacy and security attributes

Two parts of the PAPI Learner standard are directly related to security and privacy issues. IEEE 1484.2.3 gives information and recommendations on important security issues for implementations, while 1484.2.23 describes learner security information, e.g., keys and credentials.

The PAPI standard introduces by definition notions that are relevant for provision of security and data protection by specifying the meaning of terms related to access control, administrative security, authentication, authentication exchange, integrity (data) authentication information, computer security, confidentiality, learner credentials, inbound security threat and digital signature. The security, privacy and data protection are defined in so-called conceptual models. In the Session-View Security Model, the security features are provided on a per-session, per-view basis. Each security session is initiated by an accessor (a user/learner or agent that requests access). The accessor provides security credentials that authenticate the accessor, authorize the accessor, or both. A view in the PAPI vocabulary represents a portion of PAPI Learner information; a "view" is similar to the notion of a database "view". Each view that is established represents a session, i.e., the "session" represents the duration of access and the "view" represents the scope of access. Security Parameter Negotiation Model enables the participants in the e-learning session to negotiate security parameters prior to, during and after each session.

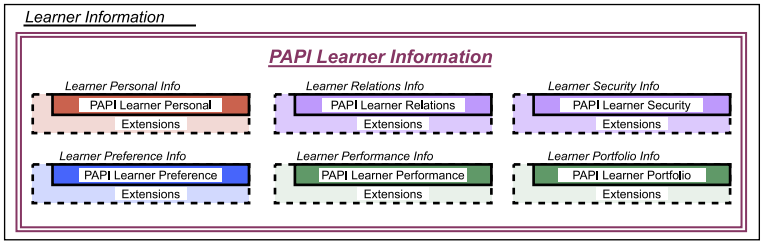

Fig. 2. High-level architecture of PAPI profile.

The security parameters are defined in the bindings of the PAPI Learner Standard, e.g., Parts 1, 6, 21–26. The Security Extension Model enables additional security features to be used besides the ones specified in the current model. The method of incorporating extensions is defined in the bindings of the PAPI Learner Standard. Access Control Model enables accessors to read data elements, to write data elements, to create new data elements (separately or within aggregates), to destroy data elements (separately or within aggregates) and to change attributes of data elements under condition that these actions are permitted in their profile. Other access methods, if any, are implementation-defined. Identification Model specifies the methods for identifying learners. These methods are implementation-defined. Authentication Model and the methods of authenticating users are outside the scope of the PAPI Learner Standard and they are not specified. The other security mechanisms, such as authorization and nonrepudiation, are implementation dependent and are not defined. The PAPI Learner Standard does not specify a digital signature model and does not specify digital signature requirements, but supports several signing frameworks and techniques permitting in such a way the integration of various digital signature models, policies and technologies. This Digital Signature Model is harmonized with ISO/IEC 15945, Specification of Trusted Third Party Services to Support the Application of Digital Signatures.

As far as privacy is concerned, the PAPI model has no specification that covers explicitly this part of the requirements for privacy. The same holds for the confidentiality model, which is missing as well. The technology for access control is also not specified. However, the partitioning of learner information into PAPI Learner information types directly addresses security issues as the learner identifier links (connects) the learner's information types to form consolidated pieces, as necessary (e.g., joining learner preference information with learner portfolio information). Information repositories as well are expected to use learner identifier surrogates: temporary identifiers that are generated on-demand for each session. This is illustrated by an example: for each "remote" (distance) learning management system, the "local" (home) repository assigns a temporary, per-session learner identifier helping the protection of user privacy. The local repository translates these temporary identifiers to private, internal identifiers. With this approach, it is much more difficult to identify and track a learner, except as authorized within specific learning experiences. This process of creating temporary, surrogate identifiers is completely transparent to the learner, the learning content and the learning management system. From the perspective of privacy, because learner contact information is separated and PAPI Learner information is de-identified, partitioned and compartmentalized, most of the privacy concerns actually are addressed as the learner cannot be identified, i.e., connected to his/her learner contact information. The use of these dynamic, temporary, surrogate identifiers generated on the fly further protects the learner.

4.3. The EDUCAUSE–Internet2 EduPerson

4.3.1. General information

The eduPerson specification is a document produced by the Directory Working Group of the Internet2 initiative. EduPerson is an auxiliary object class for campus LDAP directories that includes widely used person attributes in higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes. The eduPerson specification recommends that learner directory entries have also person, organizationalPerson and inetOrgPerson object classes defined. The former two are defined in X.521 (2001) and inetOrgPerson is defined in RFC 2798 and based in part on RFC2256. The list of learner attributes in eduPerson specification is not as extensive as in the IMS LIP or PAPI specifications. The attributes range from the learner's name, nickname and affiliation (organization, organizational unit) to contact information, such as postal address, e-mail address, phone and fax numbers, person photo and preferred language. Person's primary relationship to his/her institution can also be specified in broad categories, for example, faculty, student, staff, alum, member, affiliate, employee, etc.

4.3.2. Privacy and security attributes

Several attributes are important for privacy and security provision in this specification. For storage of

their credentials, learners can use userCertificate and userSMIMECertificate attributes. They define learner's X.509 public-key certificate and an X.509 certificate specifically for use in Secure/Multipurpose Internet Mail Extensions (S/MIME) applications, respectively. Entry's password and encryption method are specified in userPassword, while for access control provision, eduPerson relies on the Lightweight Directory Access Protocol (LDAP) mechanisms.

An important attribute for the purpose of inter-institutional authentication is the attribute "eduPerson-Principal Name". The attribute contains person's "NetID" in the form of user@univ.edu, where univ.edu is the name of the local security domain. If populated, the user should be able to authenticate with this identifier, using locally operated services. Local authentication systems should be able to adequately affirm (to both local and remote applications) that the authenticated principal is the person to whom this identifier was issued. The initial intent in defining this attribute was to use it within the Shibboleth project, http://www.shibboleth.internet2.edu/. However, it has quickly become clear that a number of other applications could also make good use of this attribute (e.g., H.323 video, chat software, etc.).

Another attribute that deals with security domains is eduPersonScopedAffiliation that specifies the person's affiliation within a particular security domain in broad categories, such as student, faculty, staff, alum, etc. An eduPersonScopedAffiliation value of "x@y" is to be interpreted as an assertion that the person in whose entry this value occurs holds an affiliation of type "x" within the security domain "y", for example, faculty@ijs.si.

The eduPerson specification is addressing the privacy issues as well. The attribute eduPersonTargetedID is persistent, privacy-preserving identifier for a principal shared between a pair of coordinating entities, such as the identity provider (in the X.500 directories, where eduPerson is an object) and the service provider—e.g., e-learning service. An identity provider uses the appropriate value of this attribute when communicating with a particular service provider, and does not reveal that value to any other service provider except in limited circumstances. A given value is intended only for consumption by a specific requester, and may be derived from some function over the requester's identity and other principal-specific input(s). It might not itself be stored by the identity provider, but usually is used to support changes or revocation of the value. It should be considerably difficult for an observer to guess the value that would be returned to any given requester, even given knowledge of the principal-specific input(s) to that value. This attribute is typically used to represent a long-term account linking relationship between an identity provider and a service provider. Note that such a service provider might itself also be an identity provider.

4.4. Other approaches

The Universal Learning Format (ULF) developed by Saba [35] is a modular set of XML-based formats for capturing and exchanging various types of e-learning data, including online learning content, catalogues of learning resources, certification libraries, competency libraries and learner profile information. ULF borrows from a wide spectrum of industry standards for exchanging learning data in a web environment (including ADL, IMS, LRN, IEEE LTSC, Dublin Core and vCard) and brings together the key elements of these standards into an integrated solution. ULF is compatible with its constituent standards and provides a two-way path for conversion and reconversion. Profile Format in ULF is an XML-based representation for describing learner profile information. Learner profiles comprise a variety of data about learners, including personal and job information, learning history, goals and plans, and held competencies and certifications. Profile Format captures this information in an XML-based format using RDF to define metadata for describing learners. Profile Format incorporates several existing metadata standards, including the Dublin Core and vCard, which ensures compatibility with existing person/profile descriptions. Privacy and security information is not part of the learner profile.

Learner profiles can be seen as special examples of the user profiles. Therefore, from the privacy and security point of view, some other standardization approaches for user modelling can also be worth mentioning. The OASIS specification Extensible Customer Information Language (xCIL) defines information that can be associated with a person or

an organization. The framework supports different customer data elements, such as name, birth details, occupation, qualification details, hobbies or habits. Specification xCIL does not define a vocabulary for privacy or security of the data represented in xCIL format.

The Customer Profile Exchange Specification (CPExchange) defines a data format for disclosing customer data from one party (customer/enterprise) to another. It defines basic and complex data types for many different kinds of personal data (e.g., fields for address, name, hobbies, etc.). It enables the specification of privacy meta-information as an option. The privacy meta-information includes the exchange partners, the applicable jurisdiction and a privacy declaration (based on P3P). Privacy declaration contains policy characteristics that describe how data can be used, how long data can be retained and whether access may be granted to the customer's data. The main focus of the specification lies in standardizing the data exchange format. UserML is an approach for describing users in ubiquitous computing. The user is enabled to annotate situational and user-specific data in the profile with the following privacy settings only: access (public, friends, private), purpose (commercial, research, minimal) and retention [long (year), middle (month), short (day)].

5. Assessment and proposed improvements

5.1. General findings

A significant concern over the use of personal information and intention to protect this can be seen throughout most of the studied models. A general problem is the lack of comparability between the approaches. In general, it may be said that these standards do not address privacy issues sufficiently. They contain some attributes and means that may provide solutions to the learner privacy, but the detailed specification is still missing. PAPI is somehow superior and addresses the security issues in the best way. However, the learner involvement and decision making about his/her readiness relevant information to be shared by the system is not enabled.

5.2. Enhancement through introduction of privacy preferences—the ELENA solution

One of the possible solutions to the privacy protection problem in e-learning systems is being introduced within the ELENA project from the European IST programme. The goal of the ELENA project is to demonstrate the feasibility of smart spaces for learning that are defined as distributed systems, which provide management support for the retrieval and consumption of heterogeneous learning services via personal learning assistants (PLAs). The term "space" is used as a synonym for "network", while "smart" refers to the smart mediation of learning services based on user profiling and artificial intelligence techniques [5]. The ELENA smart space for learning directly interfaces with learning-related information systems, such as learning management systems, educational repositories, assessment tools or live delivery systems, e.g., video conferencing systems. Smart spaces for learning rely on an infrastructure of heterogeneous learning services with open interfaces. The underlying communication framework of ELENA is decentralized and based on a three-level architecture (see Fig. 3). Layer 1, a Peer-to-Peer (P2P) layer called Artefacts and Service Network, provides basic services and allows users and institutions to connect to a learning network without any central administration, and with a possibly large variability in client and server capabilities. The P2P middleware layer enhances and connects corresponding system capabilities and services, and is based on providing service and metadata announcements as well as

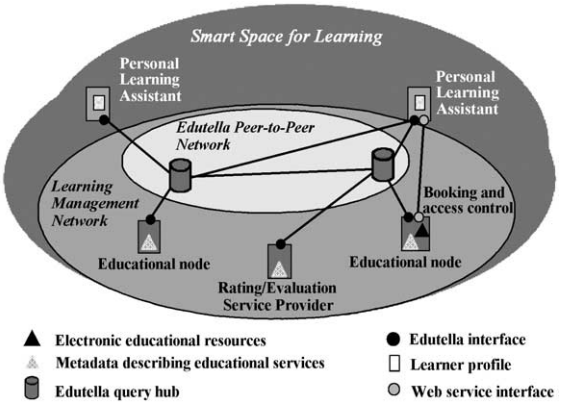

Fig. 3. Smart space for learning.

exchange and mapping functionalities. Learners enter a network of interconnected educational nodes (Learning Management Network) through personal learning assistants that provide personalised access points to learning resources on the network. PLAs support learners in searching for, selecting, contracting and evaluating learning resources.

Central design element of the ELENA smart space for learning is a dynamic learner profile, which contains learner identification information, affiliation, learning history, performance, achievements, goals, interests and preferences, as well as security- and privacy-related attributes. Most of the learner personal data in the profile is privacy and security sensitive and must therefore be adequately protected. ELENA learner profile does not contain special categories of data as defined by EU Directive 95/46/EC, e.g., data concerning health or sex life. According to our analysis, two types of security- and privacy-related information should be part of a learner profile for privacy and data protection provision. First, a learner must be able to store his/her security information, such as cryptographic keys, public key certificates, Kerberos tickets, username tokens, private credentials for pseudonymous service access or any other security credentials. These credentials can be used, for example, to prove learner's identity and nonidentifiable attributes, or for access of different learning object repositories.

The second requirement is a support of the learner to define when, how, to whom and to what extent his/her personal data is disclosed. Learners are willing to disclose certain personal information if this disclosure is potentially beneficial. If a learner, for example, does not care much about privacy issues, his/her PLA can send a query to the network with all necessary information included, e.g., identification, location, time, preference and goals. In this case, the peers within the network will know learner's personal data, and will be able to start collecting the data and building their own profiles about him/her. The query may also leak ideas behind the query to other peers and subjects within smart space for learning; for example, it may tell learner's competition what he/she is interested in. On the other side, the PLA could just ask other nodes for any learning services that they offer, and then filter out those services that do not meet learner's preferences. In this case, none of the personal information is revealed to the outside. Control of data disclosure is not relevant only for searching. The same applies for information exchange during other events, such as booking or consumption of learning services. Disclosure of personal data should therefore depend on learner's preferences. Privacy support is achieved by integrating privacy policies in the profile.

ELENA builds on existing standards and introduces new solution where there are missing artefacts or unspecified details. The ELENA approach, which is presented in Fig. 4 in the form of an RDF class diagram, combines both the IMS LIP specification (*Securitykey* element and *Privacy* metadata) and PAPI specification (*Learner security information* element) concepts. The ELENA *SecurityAndPrivacy* category is similar to the LIP Securitykey category and contains learner's credentials, such as public-key certificates, attribute certificates, keys, and username tokens. The credentials can be of several types, i.e., KeyInfo, EncryptedKey, BinarySecurityToken and UsernameToken. They are defined in detail in XML Signature [36], XML Encryption [37] and Web Services Security [38] recommendations and standards.

A novelty of the ELENA approach is that the privacy preferences in ELENA learner profile are specified in the *PrivacyInfo* attribute that is attached to each element. The attribute contains a privacy label, optional privacy policy and signature. A signature of the element can be XML signature, Public Key Cryptography Standard (PKCS) #7 signature or HMAC signature. Profile elements can be given a privacy label as follows:

- Low sensitive (0): these personal data may be exchanged to anybody without any security or privacy protection. The disclosure of the data represents no risk to the learner;
- Medium sensitive (1): these personal data may only be exchanged to particular parties. Privacy policy defines when, how and to what extent the information can be disclosed;
- High sensitive (2): these personal data may never be exchanged to other parties.

A default personal privacy policy in ELENA, initially set up by a PLA, classifies personal data as high sensitive. A learner can later change sensitivity and define to whom medium-sensitive data can be

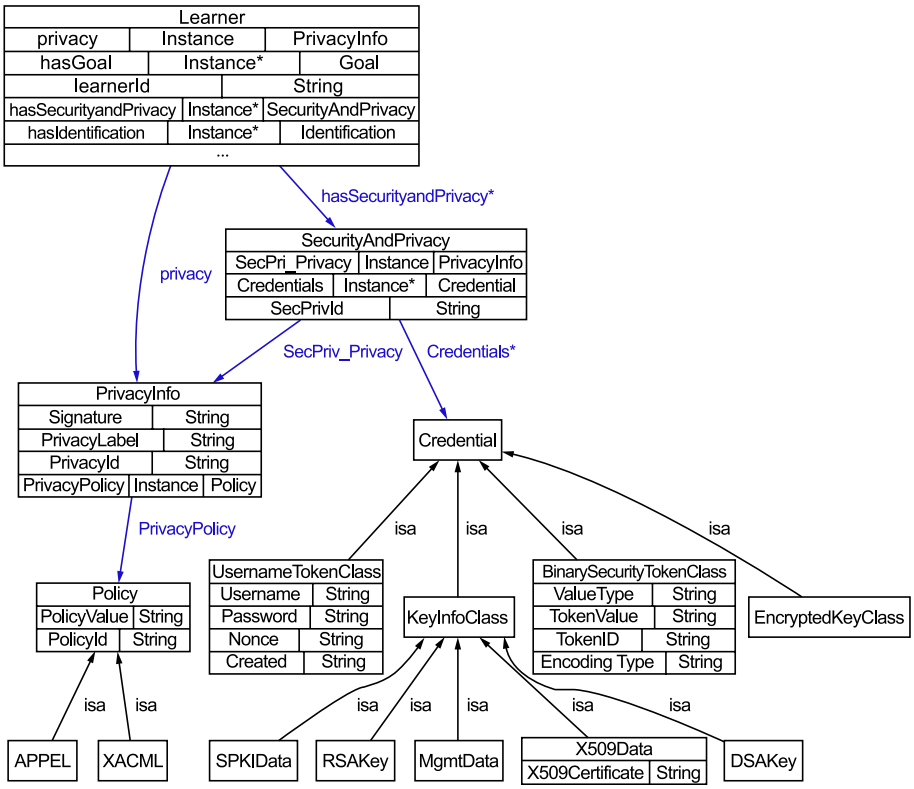

Fig. 4. Learner privacy and security information.

revealed. As policies are generally complicated, studies show that real-time release of personal data should be supported, i.e., learners might initially be asked what to do when the data is about to be released [39]. Policy development is also easier when initiated by real-time releases. Examples of predefined policies in a PLA are needed to help learners formulate their requirements in an easy and consistent way.

Personal privacy-related data is checked before query rewriting in order to ensure that none of the sensitive information is included in the query, as well as exchange of personal data with other educational nodes, for example, in booking procedure and consumption of a learning service. Envisaged formats for description of learner's personal privacy policy are either APPEL P3P language [9] or Extensible Access Control Mark-up Language (XACML) [40] format. Using APPEL, a learner can express his/her preferences in a set of rules, which can then be used by PLA to make automated or semiautomated decisions regarding the acceptability of machine-readable privacy policies from P3P-enabled service providers. XACML is a general-purpose access control policy language, developed by OASIS consortium.

Educational service providers are supposed to publish public privacy policies that specify how learners' personal data is handled at their site. Their privacy practices are expressed in a standard P3P form that can be retrieved and interpreted automatically. These policies will give more information to learners and to their personal learning assistants in order they to be able to decide (based on APPEL rule sets) whether some personal attributes should be disclosed to a particular provider or not. A learner or his/her PLA may decide to disclose certain information (medium sensitive) if provider's policy is in compliance with learner's personal policy requirements. However, it should be noted here that P3P is not suitable for monitoring whether educational nodes adhere to their own stated procedures, so some caution is still necessary before deciding to whom the information will be disclosed. Enterprise Privacy

Authorization Language (EPAL) seems to be better for the providers as EPAL policies can also be enforced by privacy-enforcement systems. E-learning service providers may also announce their security-related requirements and preferences, such as envisaged security mechanisms, protocols or credentials. A provider may, for example, require that all learners authenticate themselves by X.509 public-key certificates or that TLS protocol is used whenever data is exchanged between the provider and learner.

The learner scenario regarding privacy protection in ELENA is explained by an example presented in Appendix A.

6. Conclusion

Privacy is understood as a freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. Privacy provision techniques may include controlling the unauthorized copying or gathering of information or controlling transfer of information. Appropriate use of technologies that provide privacy and data protection demands relevant attributes in the databases provided within the e-learning systems. These are not obvious in the current e-learning standard schemes. In this paper, we have shown that the existing standards regarding the contents in learners administration part of the e-learning system do not meet properly the user requirements in the context of privacy provision policy and data. The careful analysis resulted in a proposal of an improved scheme together with the relevant attributes that overcomes the deficiencies in the existing solutions. The new scheme was specified within the systems being developed in the European project from the 5th Framework Program with a name Creating Smart Space for Learning and acronym ELENA [5]. The novelty in ELENA approach is in the personal data concept schema that allows disclosure of personal data being dependent on learner's preferences. Which data will be revealed or protected is left to the learner's decision. Even in the case when the learner is not capable to decide by him-/herself due to lack of knowledge or competence, the system is instructed to do so according to the selected preferences.

However, total solution for privacy provision cannot be based on technology only. It must combine laws, markets and technology. Here, we have presented how the current e-learning standards answer regarding the needs for technology application that provide protection of privacy and security of the stored and collected data. The new improved scheme specified in ELENA contributes to further improvement in the field and offers new acceptable solutions.

Acknowledgments

This work was supported in part by the EU IST ELENA project (IST-2001-37264, http://www.elena-project.org). The work has benefited from the collaborative work carried out in the ELENA project. We specially thank Peter Dolog for providing Fig. 4 and for the discussion that led to several improvements, and Bernd Simon.

A. ELENA learner scenario

For better understanding which learner information is involved and which requirements are imposed to the ELENA learner profile model, we give a short exemplary scenario. Bob has a meeting next month in Munich. His PLA proactively tries to find out if there are any seminars that are organized in Munich shortly after the meeting. Before a query is sent to the network, it is adapted according to Bob's privacy preferences regarding disclosure of sensitive personal data. The query for learning services related to computer security (Bob's preference) gives the following results: an introductory 2-day course in basic computer security, a refreshment course in computer security and two seminars on advanced security technologies in networking.

Bob's PLA knows that Bob already attended an online course on basic security from his local university, as part of a larger seminar on computer networks, so it suggests only the last three seminars: one to refresh the previously obtained knowledge, and the others to gain some new information and knowledge. One of these two advanced seminars is part of a series of seminars that lead to a certified security professional (CSP) title. The PLA knows that Bob's

goal is to become a CSP in the future, so it emphasizes this information.

Since Bob has not forgotten much about basics in computer security yet, he decides for the advanced seminar that may help him to achieve his goal. A prerequisite for attending the seminar is knowledge about basic security. During the booking procedure, Bob's PLA sends the seminar provider a certificate that confirms Bob's attendance to an online course on basic security. The certificate, which contains major topics that were covered in the seminar, also contains grades that are privacy sensitive. Bob's PLA decides to cover this information before sending the registration to the provider.

The seminar provider requires Bob to be authenticated during the registration by valid X.509 public-key certificate issued by well-known certification authority. The provider would also appreciate if Bob sent other personal information, such as his e-mail address, phone number, age and interests. Since Bob had some unpleasant experiences in the past with learning service providers that disclosed his information to advertising organizations, his PLA is instructed that those information should not be exchanged. The PLA also knows that Bob is a member of IEEE, and he is thus eligible for a seminar fee discount. After the Munich seminar, Bob receives a certificate that can later be used in other seminars of the series, enabling him to become a CSP. The certificate is stored in his PLA.

Options that are included in the query as well as data that are disclosed to the seminar organizer depend on Bob's privacy policy. If Bob does not care much about privacy issues, his PLA could send a query to a peer-to-peer network with all necessary information included, i.e., identification, location, time, preference and goals. In this case, all educational nodes within the network will know Bob's personal data and will have the possibility to start collecting the data and building their own profile about Bob. The query may also leak ideas behind the query to other peers and subjects within smart space for learning; for example, it may tell Bob's competition what he is interested in. On the other side, the PLA could just ask other nodes for any learning services that they offer, and then filter out those services that do not meet Bob's preferences. In this case, none of the personal information is revealed to the outside.

References

[1] L. Anido, M. Llamas, M.J. Fernandez, M. Rodriguez, J. Santos, A standards-driven open architecture for learning systems, Proc. of IEEE International Conference on Advanced Learning Technologies, ICALT 01, 2001, pp. 3–4.

[2] IEEE 1484.12/D4.0, Learning Technology Standards Committee LTSC, IEEE, Draft Standard for Learning Objects Metadada (LOM), IEEE Computer Society 2002.

[3] C. Pahl, Managing evolution and change in web-based teaching and learning environment, Computers and Education 40 (1) (2003) 99–114.

[4] Vanja Seničar, Borka Jerman-Blažič, Toma Klobučar, Privacy enhancing technologies—approaches and development, Computer Standards and Interfaces 25 (2) (2003) 147–158.

[5] Bernd Simon, Peter Dolog, Zoltan Miklós, Daniel Olmedilla, Michael Sintek, Conceptualising smart spaces for learning, Journal of Interactive Media in Education 9 (2004) (Special Issue on the Educational Semantic Web. ISSN:1365-893X.).

[6] R.J. Bayardo, R. Srikant, Technological solutions for protecting privacy, IEEE Computers (2003 (September)) 115–118.

[7] Vanja Seničar, Tomaž Klobučar, Borka Jerman-Blažič, Privacy-enhancing technologies, in: Borka Jerman-Blažič, Wolfgang Schneider, Toma Klobučar (Eds.), Security and Privacy in Advanced Networking Technologies. NATO Science Series, Series III, Computer and Systems Sciences, vol. 193, IOS Press, Amsterdam, 2004, pp. 213–227.

[8] Massimo Marchiori (Ed.), The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, 2002 (April).

[9] Marc Langheinrich (Ed.), P3P Preference Exchange Language 1.0 (APPEL1.0), W3C Working Draft, 2002 (April).

[10] Calvin Powers, Mathias Schunter (Eds.), Enterprise Privacy Authorization Language (EPAL 1.2), W3C Submission, 2003.

[11] R. Agrawal, et al., Hippocratic databases, Proc. 28th Int. Conf. Very Large Data Bases, Morgan Kaufman, 2002, pp. 143–154.

[12] R. Agrawal, A. Evfimievski, R. Srikant, Information sharing across private databases, Proc. of ACM SIGMOD Int. Conf. Management of Data, ACM Press, 2003, pp. 86–97.

[13] G. Karjoth, M. Schunter, M. Waidner, Platform for enterprise privacy practices: privacy enabled management of customer data, Proc. of 2nd Workshop on PET, LNCS, Springer Verlag, Berlin, 2002.

[14] Learning Technologies Standardization Committee (LTSC). Web site at http://www.ltsc.ieee.org/.

[15] IMS Global Learning Consortium. Web site at http://www.imsproject.org/.

[16] Aviation Industry Computer Based Training Committee. Web site at http://www.aicc.org/.

[17] US Department of Defense, Advanced Distributed Learning (ADL) Initiative. Web site at http://www.adlnet.org/.

[18] The Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE). Web site at http://www.ariadne-eu.org.

[19] Getting Educational Systems Talking Across Leading Edge Technologies (GESTALT) project. Web site at http://www.fdgroup.co.uk/gestalt.

[20] PROmoting Multimedia access to Education and Training in EUropean Society (PROMETEUS). Web site at http://www.prometeus.org/.
[21] Gateway to Educational Materials (GEM). Web site at http://www.geminfo.org/.
[22] Educational Network Australia (EdNA). Web site at http://www.edna.edu.au/.
[23] European Committee for Standardization (CEN), Information Society Standardization Systems (ISSS), Learning Technologies Workshop (LT). Web site at http://www.cenorm.be/isss/Workshop/lt/.
[24] Internet2 Middleware Architecture Committee for Education (MACE), Internet2-mace-dir-eduPerson-200312, December 2003.
[25] International Standardization Organization (ISO)/Institute Electrotechnical Commission Committee for Learning Technologies (ISO/IEC JTC1 SC36). Web site at http://www.jtc1sc36.org/.
[26] Makimilian Teltzrow, Alfred Kobsa, Impacts of User Privacy Preferences on Personalized Systems– a Comparative Study. Paper presented at the CHI-2003 Workshop "Designing Personalized User Experiences for eCommerce: Theory, Methods, and Research", Fort Lauderdale, 2003.
[27] Extensible Customer Information Language (xCIL) Ver.2.0 (final), http://www.oasis-open.org/committees/ciq/download.html.
[28] Kathy Bohrer, Bobby Holland (Eds.), Customer Profile Exchange (CPExchange) Specification, 2000 (20 October), (http://www.cpexchange.org/).
[29] Dominik Heckmann, Antonio Krueger, A user modelling markup language (userml) for ubiquitous computing, in: Peter Brusilovsky, Albert T. Corbett, Fiorella de Rosis (Eds.), Proc. of User Modeling 2003, 9th International Conference, UM 2003, Johnstown, PA, Springer, 2003 (June), pp. 393–397 (LNAI 2702).
[30] IMS Learner Information Package Information Model v1, IMS Global Learning Consortium, March 2001.
[31] IEEE 1484.2.1, "Standard for Learning Technology—Public and Private Information (PAPI) for Learners (PAPI Learner)—Core Features".
[32] IEEE 1484.2.21, "Standard for Learning Technology—Public and Private Information (PAPI) for Learners (PAPI Learner)—Learner Contact Information".
[33] IEEE 1484.2.23, "Standard for Learning Technology—Public and Private Information (PAPI) for Learners (PAPI Learner)—Learner Security Information".
[34] IEEE 1484.2.3, "Guide for Learning Technology—Public and Private Information (PAPI) for Learners (PAPI Learner)—Learner Information Security Issues".
[35] Saba. Universal Learning Format (ULF) Technical Specification, Version 1.0, October 2000.
[36] Donald Eastlake, Joseph Reagle, David Solo (Eds.), XML-Signature Syntax and Processing, W3C Recommendation, 2002 (February).
[37] Donald Eastlake, Joseph Reagle (Eds.), XML Encryption Syntax and Processing, W3C Recommendation, 2002 (December).
[38] Anthony Nadalin, et al., (Eds.), Web Services Security Username Token Profile 1.0, 2004 (March).
[39] Birgit Pfitzmann, Michael Waidner, Privacy in browser-based attribute exchange, ACM Workshop on Privacy in the Electronic Society (WPES) Washington, Nov. 2002, ACM Press, 2003, pp. 52–62.
[40] Simon Godik, Tim Moses (Eds.), OASIS eXtensible Access Control Markup Language (XACML) V1.1, 2003 (August).

Borka Jerman-Blažič is working as the head of the Laboratory for Open Systems and Networks at Jožef Stefan Institute and as full professor at University of Ljubljana. She has spent her postdoctoral at Iowa State Univesity, Ames, US, as visiting scientist and worked once as project development officer for TERENA – The European Association of Academic and Research Networks. Her main field of applications and research are: computer communications, security in networking, privacy and data protection systems, electronic commerce e-regulation, NGN, e-learning, semantic web, etc. Borka Jerman-Blažič is a member of many professional associations and is appointed expert to Member of UNECE UN (Economic Commission for Europe), appointed member of UNECE/CEFAT Team of specialist on Internet enterprise development, appointed member of eTEN Management Committee, member of New York Academy of Science 1999, Honorary member of Slovene Society for Informatics, member of IEEE on Computers, ACM. She is also Honour member of Slovenian Society for Informatics and Chair of Slovenian Standardisation Committee on ICT as well as Chair of the Slovenian Chapter of Internet Society and is member of the European ICT Standardisation Board. She is chairing the Executive Board of the European Council of ISOC Chapters. She is holding plaque of appreciation for development of Internet services from the Thai branch of IFIP and ACM. She has published more than 50 papers in refereed journals, 154 communications scientific meetings, 15 chapters in scientific books, 6 books and other 142 non-classified contributions.

Tomaž Klobučar is a research assistant at Jožef Stefan Institute. He finished his studies in mathematics and computer science at University of Ljubljana in 2000. His main interests are computer security, privacy and technology enhanced learning. He has been involved in several EU projects on these topics, e.g. in ICE-CAR, ELENA or UNIVERSAL where a platform and the service EducaNext (www.educanext.org) for exchange of learning resources were built. Tomaž Klobučar is also a member of a network of excellence in professional learning (PROLEARN) from FP6 of EU.