

Collaborative E-Learning

Katja Liesebach, Elke Franz, Anne-Katrin Stange, Andreas Juschka,
Katrín Borcea-Pfitzmann, Alexander Böttcher, and Hagen Wähg

Technische Universität Dresden

In the following chapter a short overview about the collaborative eLearning application prototype BluES'n is given. Starting by emphasising its need and potentials for PRIME, the integrated and realised privacy-enhancing components and functionalities are described. A summarising section points out lessons learnt when integrating PRIME into the application.

24.1 The Collaborative eLearning System BluES'n

24.1.1 Democratisation of an eLearning Environment

“Everyone is allowed to do everything – in the frames of generally-agreed rules and directives” – this statement depicts the idea for designing an eLearning environment where every user gets access to all functionalities provided by the environment (cf. [BPL07], [BPLW05]). Each user should have the possibility to read and annotate learning contents, to generate own contents as well as to structure them according to his preferences. Furthermore, the user should also be supported to perform those actions together with other users of the eLearning environment. This implies the availability of possibilities for dynamic group building as well as for the non-restricted use of collaboration and communication modules. Consequently, it is imperative to refrain from the traditional and rigid approach of role handling in eLearning. A system is to be designed that poses the individual user 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 to efficiently achieve learning and working objectives.

Comparable to traditional real-world educational scenarios where various working processes take place in different rooms and areas, users are provided an eLearning environment with according working areas – so-called workspaces. Such workspaces are “equipped” with all necessary functionality and means for an objective-oriented coping with tasks and interactions.

The metaphor of a “workspace” for an objective-oriented partitioning of the eLearning environment is used to facilitate different fields of activity. Two types of workspaces can be identified: In the centre of *Shared Workspaces* are the corporate work and communication of the participants. In contrast, *Personal Workspaces* represent users’ individual working environments, i.e., every user has her own individual workspace – the Personal Workspace – which represents, therefore, a special form of a shared workspace.

Following the democracy approach, each user has the possibility to create and configure new shared workspaces. A newly created workspace is equipped in accordance with the requirements of the task that should be elaborated as well as with the individual characteristics of the working community. These settings are performed by the corresponding workspace owner. The main characteristics of an individual workspace are *functional modules*, the *contents* to be worked on and *users and their roles*.

The functionality necessary for learning and working in a workspace is provided by so-called *functional modules*. That way, the users get access to very different educational functions, such as tools that allow for collaborative elaboration of knowledge and documents, for structuring contents and for communication as well as for interactions between users.

Another element characterising a specific workspace is the *content*. It is the working basis since it objectifies the knowledge that is created and enhanced during the accomplishment of work in the workspaces.

Finally, the efficient proceeding of learning and working processes requires roles describing intentions and responsibilities. According to real-world scenarios, roles become an important factor of social life when people are interacting, i.e., no global pre-assignment of roles is intended. Instead, two different kinds of roles are considered: Administrative and functional roles. By means of *administrative roles*, general possibilities of users and their rights to access resources in the corresponding workspace are described. Beside the *workspace owner*, which has extensive rights in the workspace, we consider *participants* and *guests* as further administrative role instances. While *participants* are allowed to act and take active part in a specific workspace, highly restricted access to offered contents and functionalities are provided to *guests*. In contrast to administrative roles, the instances of functional roles, e.g., tutor, author, moderator, describe privileges and obligations of users. They are used to communicate other users of this workspace their own status, role-related

assignments, and responsibilities while working with a corresponding functional module.

Summarising, the support of collaborative and cooperative learning scenarios is in the focus of the described concept. Depending on the current task and situation, learners become enabled to jointly elaborate knowledge. One of the major aims of such collaborative eLearning environments is to foster users' self-determination with respect to learning methods and styles by allowing for the creation of new working areas and groups as well as for the possibility to re-organize learning groups by the users.

24.1.2 Need for Privacy and How PRIME Helps

In traditional eLearning environments where users work under one login only, all their actions within that application can be linked. This, however, offers the possibility to create detailed user profiles: First, it is recognisable which classes and groups a learner attends. Second, all actions within a class or group can be assigned to the particular user. For example, frequency of learning sessions, average duration of processing learning modules, or results of tests can be observed. Third, this collected information allows drawing conclusions about the learner, e.g., about interests, learning speed, habits, or equipment. Users may lose reputation due to failures. This may result in a biased environment: A user may be prejudiced against other users due to bad results in other classes or due to former discussions or questions. If users are aware of these threats, they might feel to be observed and be afraid of failing. Hence, they may feel restricted and become afraid to disgrace themselves. They possibly become discouraged to ask and practice.

Despite these possible privacy risks, however, users cannot act completely anonymously within a collaborative eLearning system, i.e., performing all actions anonymously and unlinkably. Collecting and evaluating personal data such as information about users' preferences and goals is necessary, e.g., to provide assistance for users, to realise assessment, or to support collaboration between users. However, privacy issues are not sufficiently considered in current eLearning environments and especially within collaborative eLearning. As users just begin to become sensitised for privacy problems in other application areas such as eShopping, awareness of privacy threats is not yet widely established within the field of eLearning.

Results of surveys regarding privacy protection in the Internet ([INR97, WHA98, CRA99, TK04],) as well as of eLearning services [KBG04] have shown that the majority of users are concerned about the usage of their personal information while being online. Survey results of a study conducted within the project PRIME had shown that users of eLearning systems set a high value on informational self-determination [BPS07]. Furthermore, an analysis was conducted regarding data protection in Learning Management Systems (LMS) in general [Sta07]. Six state-of-the-art LMS, e.g., WebCT and Moodle, were investigated. The results show that currently used LMS support aspects of

data protection only insufficiently. The processing of personal and identifiable information is not or only in part designed transparent for users of these systems. In addition, users are not able to determine what exactly happens with their personal data. Summarising, the wish and need for informational self-determination expressed by eLearning users of the study conducted in 2006 is not yet supported in the desired degree.

Considering the acceptance of an application in the long run, handling privacy risks is a vital task [BFD⁺05, BDF⁺05b]. A known approach to preserve privacy despite the need for collecting and processing personal data is to partition this data by means of Privacy-enhancing Identity Management (PIM) [CPHH02]. Users are enabled to decide on their own which data is delivered to whom after considering the current situation. The established sub-sets of personal data are called *partial identities* (*pIDs*). Since different pIDs should not be linkable except by their owner, *pseudonyms* are used as identifiers replacing the real name of the user [PH06].

The use of pIDs would enable users to be recognisable only if necessary, e.g., in order to enable reasonable discussions with others or to enable the tutor to assist them. If learners start learning in a new class, they get the possibility to work in an unbiased environment independently of results of former classes. Additionally, learners can act under different pIDs and possibly even anonymously within one and the same class. Separating activities encourages learners to feel unrestricted and, thus, to learn without pressure. Besides this separation, the explicit linking of information is needed. Users must be able to build up their own reputation by disclosing certain information. Finally, a fine-grained partitioning of information in order to enable reasonable assistance of users or evaluation while enforcing their privacy requirements is needed.

A corresponding proof-of-concept implementation is the privacy-enhanced collaborative eLearning application BluES'n¹ which was developed in the project PRIME. BluES'n follows on the one hand the approach for collaborative working and learning as described in Sec. 24.1.1 and is otherwise enhanced by mechanisms to support user's privacy while acting in the environment.

The BluES'n system gives users the opportunity to get detailed information on the processing of their personal data and determine the data processing concerning their wishes and needs. Thereby, BluES'n utilises PIM functionalities provided by the PRIME integrated prototype. It allows for working under different pIDs for controlling the dissemination of personal information. The PIM functionalities support users to manage their pIDs, comprising tasks like creating and managing pseudonyms and managing preferences about disclosure of personal data. Policies at user side can control the disclosure of personal data. Furthermore, possibilities are needed to explicitly restrict users. For example, they should be able to take examinations only once. This problem can be solved by means of *anonymous credentials* [CL01]. Anonymous credentials

¹ BluES'n stands for BluES like universal eEducation System privacy-enhanced.

ensure that users can demonstrate possession of certain assertions without the necessity to link this show to their user identity.

Despite these privacy-enhancing extensions, the eLearning application must still be easy and intuitive to use. If users are just overwhelmed with many new tasks, they will most probably not utilize the functionality that enables privacy-aware learning.

24.2 Intra-Application Partitioning of Personal Data

24.2.1 Necessity and General Goals

Usually, PIM is used to keep data in different applications separate from each other (inter-application partitioning). However, this approach is not sufficient for applications providing a lot of complex and/or collaborative scenarios such as BluES'n: If all actions of one user were linkable, creating detailed user profiles would become possible. Consequently, a fine-grained partitioning of personal data within the application itself, i.e., *intra-application partitioning (IAP)* is necessary [BDF⁺05a, FE06, FBP06]. IAP enables users to work under different pIDs within one application (Fig. 24.1).

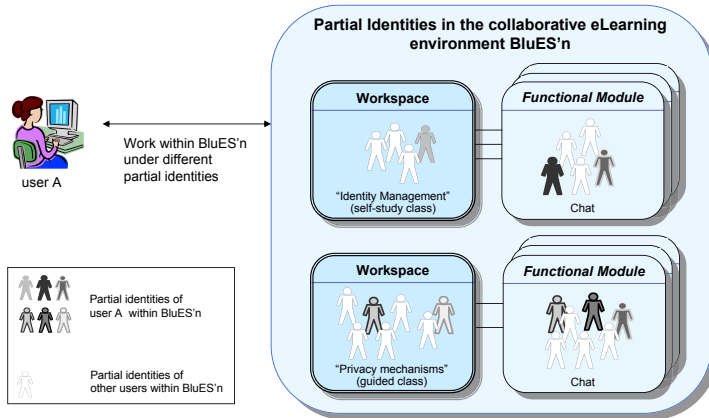


Fig. 24.1 The concept of intra-application partitioning applied to BluES'n

For usability and user acceptance reasons, we aim at supporting users in partitioning their data within the application. Thereby, we focus on two aspects:

1. Continuous *privacy awareness* (Sec. 24.4) should enable users to assess their current privacy state and, therefore, motivate them to apply IAP.

Furthermore, users will be supported in a reasonable use of IAP due to the feedback provided.

2. The system should support users in partitioning their personal data according to their preferences while they are working on other tasks. If possible, decisions should be automated. Simplifying the ongoing partitioning as much as possible should motivate users to apply IAP.

24.2.2 Concept for the Support of IAP

A context-aware component of the system (the *Decision Suggesting Module, DSM*) has the task to realise the necessary user support. Particularly, the DSM evaluates the current context and generates a suggestion regarding the decision under which pID an initiated action should be performed. All information related to an action, i.e., data requested by the server due to access control policies, data explicitly sent by the user, and information about the action itself, can be assigned to this pID. Within BluES'n, the following attributes of a user are considered:

- A pseudonym as unique identifier of a pID within the whole environment,
- A local alias as usable representation of the pseudonym [BPFP05],
- Roles describing rights and privileges of users within BluES'n, and
- Additional information helpful for supporting collaboration between users, e.g., name, address, age, and interests.

Observing actions allows to determine, e.g., when and how often a user works (under a specific pID) in a special workspace. The partitioning shall prevent others from getting a global view on all attributes assigned to a user as well as on all actions performed by the user.

The DSM evaluates a number of context features to assess the (un)linkability of an action from the point of view of other users (Tab. 24.1). The user defines rules targeted for various scenarios, e.g., for working in an authoring workspace or for participating in a chat in that workspace in order to decide whether privacy or recognition shall be supported. It depends on the aspects that should be considered by the suggestion which context features are actually evaluated. Generally, several aspects can be considered for generating the suggestion, e.g.:

- Granularity of partitioning,
- Support recognition by other users,
- Functional roles, and
- Linkability from point of view of other users.

Generally, the DSM assigns a rating to all pIDs already used within BluES'n as well as to the possibility to generate a new pID for the initiated action. If exactly one pID gets the highest rating, the user can also decide on applying this suggestion automatically. A common example is that the user performs a sequence of actions within one and the same workspace. Obviously,

Table 24.1 Context features considered by the DSM

Class of context features	Examples	Higher-level context features
<i>Application-internal context features</i> provided by a context monitoring component executed within BluES'n	current workspace and functional module	user's current objective, reasonable privacy preferences
	initiated action	
	pIDs currently visible for other users	potential visibility of an action for other users
<i>Contact-related context features</i> derived from server requests and from awareness information	pIDs of other users who can potentially observe this action	
	data required due to access control policies	increased degree of knowledge of other users about own pIDs due to necessary delivery of data
	details about data request, e.g., purpose and storage	
<i>History-related context features</i> derived from a history of former actions performed by the user	pIDs already used within the current workspace	increased degree of knowledge of other users about own pIDs, possibility to be recognised
	pID used for the last action performed in the current workspace	
	pIDs used for communicating with pIDs of other users currently present in the workspace	

it is reasonable in this case to use one pID for all actions instead of disturbing the user every time.

Finally, the user must select one of the pIDs for the initiated action. He should use the pID with the highest rating, but he always has the possibility to select another pID or to generate a new pID, respectively.

24.2.3 Realisation within the CeL Prototype

The DSM is called within PRIME when a decision regarding the delivery of personal data is required. It gets as input all pIDs used so far within BluES'n. The *Context Monitoring* delivers the application-internal context features; the DSM derives history-related context features from the PRIME history data base. Afterwards, it selects the appropriate configuration considering the state of the corresponding scope, e.g., a user works for the first time in this workspace/functional module.

The current prototype version only supports a granularity of partitioning considering the levels "BluES'n", "Workspace", and "Functional Module". The level influences the scope of pIDs, e.g., the level "Workspace" implies

that pIDs are mainly used within *one* workspace and, hence, personal data and actions are partitioned between different workspaces.

According to the context and based on the configuration, the DSM generates a rating for all pIDs which is a numeric value ranging from 10 (highest rating, should be preferred) to 0 (should not be used). Automatically applying the suggestion is possible as described above. Otherwise, the adapted “Send Personal Data”-Dialogue displays the suggestion (Sec. 24.4.4).

Since foreseeing all possible situations is not feasible, users must be able to intervene the application of predefined rules, especially if the suggestion should be applied automatically. Thus, users can switch off the DSM for the next action or until it is re-activated. The scope of deactivation is the respective workspace. If the DSM is switched off, any server request implies a user interaction by calling the adapted “Send Personal Data”-Dialogue.

Furthermore, in certain situations the pre-selection of a pID is of interest, e.g., during synchronous communication such as a chat session. Therefore, accordant functionalities are provided to the BluES’n user.

24.2.4 Discussion

The integration of a context-aware component allows for an easier partitioning of personal data. There are mainly three advantages: First, users can define rules regarding the selection of pIDs before they start their actual work, i.e., without pressure. Second, the evaluation of these rules during everyday work in the application ensures that suggestions are made according to the actual privacy preferences. Finally, the suggestions speed up the decision; the pIDs are grouped according to their suitability for the current situation, and the most plausible one is already highlighted and can be selected quickly. Additionally, the possibility to automate decisions increases the performance and reduces user interactions.

Future versions will consider further aspects, e.g., supporting recognition. It is a challenging task to define reasonable rules for conflicting goals like recognition and linkability. Defining rules dependent on the current role seems to be advantageous since it will be more intuitive for users.

Currently, the DSM supports IAP especially for BluES’n. However, a reasonable support for users will be needed also for other complex or collaborative applications which require IAP. Furthermore, the evaluation of contextual information can also be applied in order to support inter-application partitioning. Thus, it is a topic of future work to generalise the concepts applied to be used for other scenarios.

24.3 Policy- and Credential-Based Access Control

24.3.1 Necessity for Privacy-Enhancing Access Control

Access control mechanisms are required to protect resources from unauthorised access. This comprises services for *identification* and *authentication*, i.e., who is allowed to access resources, i.e., data and services, and *authorisation*, i.e., to decide who is allowed to operate on these resources.

Within collaborative eLearning, access control is needed to constrain the usage of services and functionalities, to regulate access to provided contents, and to protect user data stored on the server side. Storing some user data on the server side is needed to make them available even if the corresponding user is not online in order to provide important services such as delivering awareness information to other users to support cooperative working or to enable tutors to assist learners.

Usually, in collaborative eLearning environments, access rights are assigned to certain users of a system based on so-called access control lists. However, since users in BluES'n have the possibility to work under different, primarily unlinkable pIDs addressed by unique pseudonyms, relying on traditional login/password mechanisms is not possible. In order to allow for using assigned rights under different pIDs, realising a capability-based access control is reasonable. In such a model, access to resources is granted by holding a corresponding capability, i.e., an unforgeable reference, to that object. Finally, privacy-enhancing access control requires the consideration of following issues:

- Possibility for access control even if users act under several pIDs;
- Possibility to access resources independently of the user's current pID;
- Unlinkability of pIDs must not be threatened by access control.

In order to achieve flexibility, a user should be able to use capabilities independently of pIDs. However, showing such capabilities must not threaten the unlinkability of different pIDs. That means, providing evidence to own capabilities must not be linkable to user's real identity and, furthermore, showing one capability repeatedly or in different contexts must not allow for linking different pIDs of one user. A possible way to ensure that, is to use anonymous credentials as provided by PRIME in order to express the capabilities assigned to pIDs (see [FWBBP06]).

24.3.2 Realisation within the CeL Prototype

Due to the possibility for IAP in BluES'n, the need for a fine-granular access control based on credentials as well as pseudonyms can be derived. Thus, pseudonyms, credentials, and policy mechanisms provided by PRIME are used to realise a privacy-enhancing access control within the application. In BluES'n access control takes place on the level of resources, i.e., for each

resource, such as workspaces, structure elements, and learning materials, access rights are defined. Corresponding access types are *create*, *read*, *write*, and *delete* operations, whereby an access type is the smallest entity on which access control decisions can be performed. The assignment of access rights to users, i.e., to their pIDs, is made based on the BluES'n concept of administrative roles as already described in Sec. 24.1.1. A user who creates a BluES'n resource, automatically becomes its *owner* and obtains all possible access types on that resource. An owner is able to admit other users to reuse owned resources by granting according rights to them by assigning users the according role *participant* or *guest*.

Defining access rights for workspaces is closely related to the question how administrative roles are assigned to users. Therefore, we realised the concept of *workspace access modes* in BluES'n. These modes are in general pseudonym based or credential based, i.e., access to a workspace depends either on the usage of a specified pseudonym or on showing a requested credential. The latter case implies also credentials evidencing properties and pre-requisites, such as the successful conclusion of another workspace or holding a specific certificate to access a workspace. If a workspace is created, the BluES'n server issues a credential to its owner permitting *create*, *read*, and *write* operations within this workspace. Corresponding PRIME access control policies are created on the server side specifying which evidence, i.e., which workspace credential, must be delivered by the BluES'n clients in order to get access to and execute an operation on the required resource. The owner is allowed to grant other users access to his workspace by issuing according credentials to them. Whenever a BluES'n resource is to be created within a workspace, the BluES'n server first checks whether the user owns a credential containing the workspace identifier and the necessary administrative role. If the user is allowed to create a new resource within this workspace, the resource is added and corresponding PRIME policies are created for that new resource. Instead of issuing new credentials for each new resource, the BluES'n server derives the new policy for the new resource from the policy of the workspace to which the new resource is to be added.

24.3.3 Discussion

The described access control approach based on pseudonym, policy, and credential mechanisms provided by PRIME focuses on being privacy enhancing. Users are allowed to partition their personal data, i.e., work with the application using different pIDs while their actions are unlinkable.

During the realisation of access control for BluES'n, two different models for newly-created resources of workspaces are considered:

Model I: Issuing (new) credentials and creating (new) policies.

- *Content of credential:* Reference to that resource.
- *Content of policy:* Request for credential with reference to the resource, where the resource was created.

Model II: Reusing workspace credentials and creating (new) policies.

- *Credential*: Reuse of corresponding workspace credential.
- *Content of policy*: Request for the *owner*, *guest* or *participant* credential of the workspace where the resource was created.

While Model I was already integrated and tested in the first prototype version, tests and evaluations have shown that users are overstrained by this model. The process of selecting and showing an appropriate credential in order to use the created resources has to be applied too often by the user. Consequently, users felt overstrained and were distracted from their particular work. In order to avoid disturbing the user, finally, Model II was applied. Here, users create resources in the context of an opened workspace, which will become part of the policy of the created resource. That means, the creation of new resources only leads to the definition of new policies without the need for issuing a new credential. The policy is generated on basis of the active workspace and the current administrative role the user owned during the creation process. However, the chosen approach raises still open question with respect to, e.g., the deprivation and delegation of access rights. Challenges such as guaranteeing and ensuring copyrights, usage and exploitations rights within a privacy-enhancing collaborative application are further research questions the developer team is currently working on.

24.4 Privacy-Aware and Usable Application Design

Since collaboration and communication between users are of special interest within BluES'n, providing users with awareness information is of great importance in many ways. Awareness information covers all information which is necessary to allow a user assess his current situation within the application, e.g., information about the own learning progress in comparison to other users, information about other users, information about the workspace he currently acts in. Obviously, an evaluation of user's personal data is needed to provide the necessary information. Therefore, knowing what the application is doing with his personal data gives the user transparency about the information visible to and processed by the system, which might raise his trust in and thus, acceptance of the system as well. Receiving information regarding availability and current activities of other users improves the perception of inherent collaborative opportunities. However, this kind of awareness information is also an intrusion to privacy, since building up detailed profiles of other communication partners might be possible. Due to this and PRIME's maxim "design must start from maximum privacy" special attention has to be paid to the design of a privacy-aware application. Besides the need for providing group and privacy awareness information, usability is another important requirement which has to be considered when designing for end users. Achieving given objectives in an effective, efficient and satisfying way is just as essential as a user-friendly design and handling of according user interfaces.

BluES'n addresses the mentioned requirements by appropriate interfaces and functionalities in order to provide privacy-aware but also intuitive user-interfaces. In the following sections, these approaches are presented.

24.4.1 Management of Aliases

Motivation and Description of the Idea

The usage of randomly generated and uncorrelated pseudonyms as identifiers of pIDs ensures that pseudonyms do not leak information related to the user which might allow others to link different pIDs or even to draw conclusions about the real identity of the pID's holder [BPFP05]. However, the handling and management of such pseudonyms presented by randomly-looking character strings are neither user-friendly nor usable. It is not possible for users to remember these pseudonyms easily or to recognise already known pseudonyms of other users in highly dynamic situations like a chat. Hence, a user may wish to assign additional shorthand semantics – mnemonics – to pseudonyms. A mnemonic is the presentation of a pseudonym to a user and can be of arbitrary type, e.g., an alias as textual representation, images, or sound. For BluES'n, an alias/pseudonym mapping was chosen. In order to retain the privacy and security properties, these aliases should be assigned and used locally. However, a reasonable support of local aliases is necessary in order to achieve user acceptance as well. Managing local aliases basically requires the three components

- Alias Assignment,
- Alias Improvement, and
- Alias Replacement.

First, the *Alias Assignment* component assists the user in assigning aliases to pseudonyms. Generally, aliases are assigned to own pseudonyms as well as to pseudonyms of other users. Possible aliases are contained in a local alias dictionary (LAD); assigned aliases are stored as attributes of the partial identities. Especially for aliases assigned to pseudonyms of other users, *Alias Improvement* may be required for increasing their usability. The improved alias might encode additional knowledge about the communication partner, drawn from additional observations or experiences made in interactions or from knowledge collected over time, respectively. To allow for an easy handling of current aliases and for representing information about former aliases, only pseudonyms are stored as part of application data. Finally, *Alias Replacement* is an especially important component: It has to ensure that only secure pseudonyms leave the client system, i.e., are transferred, and that aliases are represented to users. In order to support local alias management, the *Alias Replacement* is also responsible that the locally-assigned aliases are represented to each user (cf. Fig. 24.2). Finally, replacement has to deal with possible errors resulting from ambiguities and typos during alias/pseudonym mapping and vice versa.

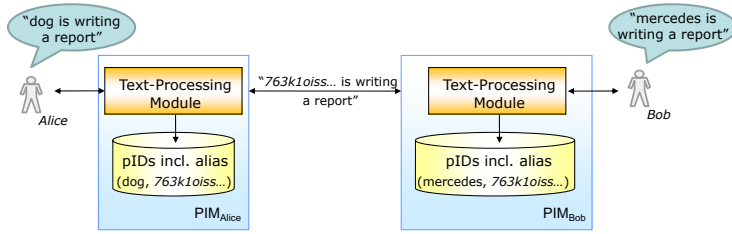


Fig. 24.2 Replacement of aliases and pseudonyms in BluES'n

Realisation in BluES'n

In BluES'n a general pseudonym/alias mapping was integrated which locally assigns an alias to each pseudonym automatically. By means of this approach the user is supported in handling and managing his own pseudonyms as well as pseudonyms of other users in a comprehensible and user-friendly way. Additionally, a first automatic analysis and replacement of pseudonyms appearing in commonly-used content by aliases takes place in communication and cooperation processes. Thus, for example, a replacement within a chat session takes place in case of addressing, i.e., naming, the communication partner directly by means of his locally-assigned alias. The *Alias Replacement* component of BluES'n checks during a user is writing a message whether the typed-in text corresponds to an existing alias/pseudonym mapping. If such a mapping exists, the user is asked on the fly whether the word should be marked as alias. By computing the Levenshtein distance², the user is also presented a list of possibly matching aliases. In case of an ambiguity error, he could select the one, he wanted to address.

Supplementing text-based aliases by means of graphical representations for pIDs might raise the recognizability of pIDs of other users. A first approach is described in Sec. 24.4.2. The consideration of additional contextual information for dynamically assigning aliases to pseudonyms are challenging approaches for future work in this field. Additionally, investigations beyond text-based representations should take place in order to support further target audiences, such as acoustic representations for blind people, and user's end devices.

24.4.2 Chernoff Faces

During their work in a complex and collaborative environment such as BluES'n, users will create various pIDs for different scenarios. In order to assess their linkability from the point of view of other users, they should get informed which information others might know, especially, which pID was

² <http://levenshtein.net>

used in which scenarios, for which actions, and which information was delivered while working under this pID. Likewise, users should be able to recognise pIDs of other users within a collaborative environment. Consequently, an intuitive and clear representation of pIDs is of fundamental importance. Thereby, a number of different information items must be encoded and represented.

Generally, the representation should enable users (1) to recognise pIDs and (2) to assess their relevant features regarding the current context. It is not possible to consider these two requirements within one single representation: While a static identifier is needed for recognition, the attributes of a pID are context dependent and might also change over time. Therefore, they require a dynamic representation.



Within BluES'n, pictograms in style of Chernoff Faces [Che73] are used to dynamically visualise multivariate data in the shape of a human face [FLBP06]. The alias as static pID identifier is displayed together with the icon. The representation of relevant features of pIDs adheres to fixed rules in order to increase its usability, especially to support users in intuitively recognising these features (Tab. 24.2). Furthermore, the system can automatically generate the corresponding representation and dynamically adapt it.

Table 24.2 Features used for visualisation

Selected feature	Encodes information about
Eyes	Degree of Knowledge
Mouth	Kind of communication
Eyebrows	Links to other pIDs
Shadow behind face	Scope of pID
Color of face	Online state
Margin of face	Active workspace
Additional symbols	Delivery of additional information
Font style of alias	Administrative role

The meaning of the features might differ for own pIDs and pIDs of other users. For example, the degree of knowledge reflects the knowledge others might have about own pIDs. For own pIDs, this value is estimated from the number of actions performed under this pID and the delivered data. In contrast, eyes of pIDs of other users represent the average degree of knowledge the other one might have about the user's own pIDs. Tab. 24.3 shows an example for a pID as well as the representation of a new pID together with an interpretation of the encoded information. Within the current version of BluES'n, only the online state and the alias including the representation of the administrative role are realised. Even this information gives some feedback about pIDs currently working within BluES'n. Future versions will enhance the representation by further features, which is needed for providing privacy-relevant information.

Table 24.3 Visualising relevant features of pIDs within BluES’n

<div>Example pID of other user</div> <div></div>	<ul style="list-style-type: none">• medium degree of knowledge• indirect communication in a functional module occurred• explicit links to other pIDs• pID was only met in one workspace• awareness objects of this pID received; pID is on-line• subscribed to inactive but opened workspace• notes assigned; pID is tutor in current functional module• pID is participant in active shared workspace
<div>New pID</div> <div></div>	<ul style="list-style-type: none">• least degree of knowledge• no communication• no links to other pIDs

24.4.3 GUI Components: InfoCenter and Echobar

Users do need usable and user-friendly graphical interfaces for getting an overview about their privacy- and group-related awareness information as described above. For that purpose, BluES’n was enhanced by a so-called InfoCenter which is a special module being always presented to and accessible to the user. Besides displaying awareness information, it serves also as starting point for configuring several aspects such as the contribution of awareness information or level of partitioning of users’ personal data, respectively. By means of three different panels, in the current version of BluES’n awareness information are provided as described in Tab. 24.4.

Table 24.4 Information provided by the BluES’n InfoCenter panels

InfoCenter panel	Information provided by panel
Workspace	The tab provides information about the state of the current workspace and the ongoing activities in this workspace.
About Me	This panel shows information about the user himself and the representation of the user to other members of the current workspace.
Community	All members of the current workspace are listed in this tab. Moreover, detailed information about the participants is available.

In addition, a so-called Echobar was integrated consisting of small traffic lights and an additional status bar which are used to visualise important, privacy-relevant aspects during the work within BluES'n. As soon as an event occurs, the corresponding lamp lights up and an appropriate message is displayed via the status bar.

24.4.4 Adapted “Send Personal Data”-Dialogue

Based on the current context and the user-defined rules, the DSM (cf. Sec. 24.2.2) generates a rating for pIDs already used within BluES'n or suggests generating a new pID, respectively. If an automated decision is not possible, a user dialogue is displayed which has the task to present the rating to the user for supporting him in the decision which pID should be chosen for the next action. PRIME already provides an appropriate dialogue, the so called “Send Personal Data”-Dialogue (cf. Sec. 20.5.1.1). However, this dialogue is tailored for communication with different application providers who request various personal data items from the user. It is not perfectly suited for the use within BluES'n due to the following reasons:

- Section *Select a Template*: The concept of templates shall be used within Blues'n to summarise data that can be requested in specific situations; however, there is no need to select one out of different possible templates as in the scenario considered by the PRIME dialogue.
- Section *Your data*: The PRIME dialogue focuses on representing which data are requested from the user. In BluES'n, information about users arise primarily due to their actions: All actions performed under one pID can be assigned to it and allow one to collect information which might simplify linking different pIDs or linking a pID to a user. A dialogue for BluES'n should instead present the rating of the pIDs already used within BluES'n.
- Section *Will be sent to*: This section informs the user about the communication partner who receives the data. Within BluES'n, this “technical communication partner” is always the BluES'n server. However, other users might recognise the action of a user due to the awareness information. Thus, the user should be informed who might recognise what.
- Section *Purpose*: Only business purpose should be possible; thus, this information could be integrated into the section *Will be sent to*.

To conclude, we integrated an adapted dialogue into BluES'n tailored for the application scenario (Fig. 24.3):

- 1 A dynamic DSM Configuration Button signals the current settings regarding the context management.
- 2 Introductory text informing why the dialogue is started.
- 3 Information about the requested data.
- 4 Introduction about the information given and handling of this section.

- 5 Via the “Create”-Button the user can generate a new pID (see “Create new partial Identity”-Dialogue). If the DSM suggests creating a new pID instead of using an already existing one, the button is highlighted orange.
- 6 The rated list of pIDs – the rating is visualised via the scales on the left hand sides of the Chernoff faces representing the pIDs. If a pID gets the highest rating, it is highlighted. Additionally, the user can have a look at attributes already assigned to a specific pID.
- 7 Information about the suggestion generated by the DSM.
- 8 Information about the initiated action and about the degree the provided data might be known to other users.

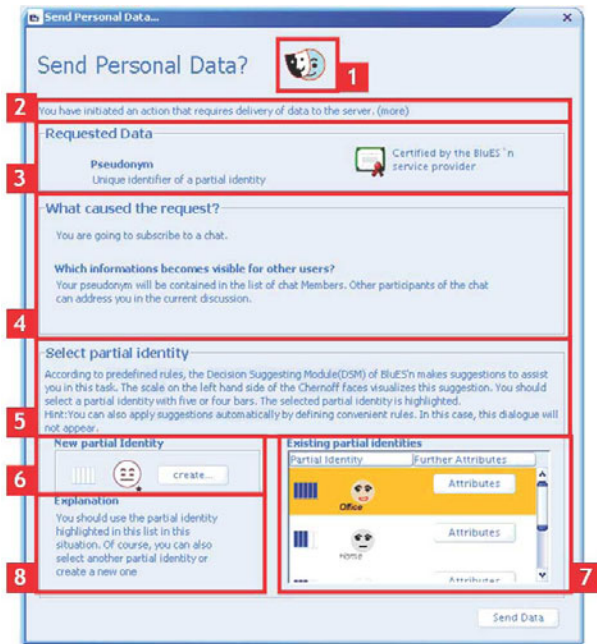


Fig. 24.3 Adapted “Send Personal Data”-Dialogue (the labelled parts are explained in the text)

24.5 Summary – The Final CeL Prototype

Reducing the collection as well as processing of users’ personal data on the services side to a minimum and providing users a possibility to keep track of all transactions of their data are the main objectives of BluES’n. During the

PRIME project, two development cycles were performed resulting in two versions of the application prototype BluES'n: Within the first version, special attention was paid to the integration of basic features of PIM into a comprehensive workspace-based collaborative eLearning prototype. During the realisation of the enhanced second prototype version, requirements on the PRIME integrated prototype were refined, particularly with regard to the support for privacy-enhancements based on PRIME technologies and considering the evaluation results of the previous application prototype version. In particular, revisions and conceptual refinements with respect to access control mechanisms, the realisation of intra-application partitioning and the privacy-aware user interface have been performed. Evaluations of the first prototype have shown that the approaches go in the right direction in terms of concepts, but that concrete implementations lack a systematic usability-engineering process with respect to the application's primary objectives as well as the integration of components of the PRIME toolbox. Thus, beside the development of the 2nd prototype version, the privacy-enhanced eLearning application BluES'n underwent a detailed and comprehensive usability-design process. Comparing both versions, modifications and improvements listed in Tab. 24.5 are part of the final BluES'n version.

According GUI improvements and enhancements of the final prototype version were additionally checked by an internal evaluation focussing especially on usability improvements. Eight students from the field of computer and media science participated as test persons. They had no experiences in using BluES'n; only two of them used other eLearning systems like WebCT before. The evaluation was organised as a collaborative session with two test persons at the same time. Altogether, the evaluation confirmed that the final BluES'n version provides a more usable and user-friendly environment:

- After a short training, based on the additionally-created *BluES'n Getting Started Tutorial*, the system can now be used more intuitively. Furthermore, six of eight test persons indicated that they would potentially use BluES'n in the future. The majority of the test persons stated that they understand and can cope with the PRIME concepts and their integration into BluES'n.
- The *credential handling* in the 1st version was a hard-to-understand and time-consuming process. In contrast, the evaluation of the final prototype version has shown that the revised credential handling, i.e., requesting and granting access to workspaces, is more user-friendly, unobtrusive and comprehensible. The user is no longer confronted with credentials as long strings representations. Now, he can handle them intuitively by understandable dialogues and menus, which was explicitly emphasised by one of the test persons.
- The adapted "Send personal data"-Dialogue provides a more transparent and understandable integration into the application. One test person using

Table 24.5 Summary of enhancements of the BluES’n prototype

Main concepts	Features provided by the enhanced prototype
pIDs, pseudonyms, and aliases	Possibility of defining attributes of users by means of pIDs with BluES’n (currently only pseudonyms as attributes)
	Realisation of pseudonym/alias mapping
Enhancements of access control based on policies and anonymous credentials	Administrative roles and workspace access modes
	Requesting and granting access to shared workspaces
	Simplification/grouping of policies for BluES’n resources
Enhanced context management to realise IAP	Integration of Decision Suggesting Module (DSM)
	Enhanced configuration and monitoring functionalities
Privacy-aware user interface	Revision of GUI and workflows based on evaluation results of version 1 particularly focussing on improving usability
	Provision and representation of group- and privacy-related awareness information
	Realisation of Chernoff faces for visualising pIDs
	Tailoring of integrated PRIME “Send Personal Data”-Dialogue for representing suggestions generated by the DSM and adapting it to the BluES’n specific design
Further concepts and features	Integration of basic reputation management
	Enhancing, respectively adding, communication supporting functional modules <i>MailForum</i> , <i>Chat</i> and <i>Group Calendar</i> as demonstrators of PRIME component’s interplay
	Provision of BluES’n Getting Started Tutorial

the highest anonymity level was able to cope with mostly all concepts of pseudonyms and IAP.

- In contrast to the 1st version, information relevant for privacy and group awareness are integrated into and now displayed via specific components in the graphical user interface of BluES’n. Particularly, assigning aliases as user-friendly representation of secure pseudonyms and visualising pIDs by means of Chernoff faces was helpful for working with different pIDs during the evaluation.

Summarising, the architecture of the PRIME toolbox and the provided PRIME Integrated Prototype meet the requirements for establishing a privacy-preserving collaborative working and learning environment for the most part from the perspective of BluES’n. However, the Integrated Prototype is mainly built for bilateral scenarios; consequently, it is not applicable for complex environments such as BluES’n comprising a variety of comprehensive collaboration, cooperation, and communication scenarios. Between interacting users and user groups manifold dynamic and flexible relations exist – so-called *multilateral interactions* (MLI) – resulting in complex requirements concerning

privacy and performance issues which have to be reflected in an appropriate system architecture (Section 22).

24.6 Beyond PRIME – An Outlook

At the end of the project PRIME, with BluES'n a collaborative learning and working environment which is enhanced by privacy functionalities by design was established for the first time. From the functional perspective, the integration of privacy-enhancing components was in the focus – their usable and user-friendly realisation was only a secondary goal. However, for practically-deployable complex and collaborative environments such as BluES'n, the focus has to be changed: Primarily, the user's attention should be on intended learning and working processes, while the management of his privacy preferences and settings comes second – only in the background. Introducing to users the available possibilities for privacy and identity management and offering default settings of possible privacy configurations before using the application for the first time would be an important refinement step. That way, users could concentrate on their actual work at first to become more familiar with the application and thus, would be able to adapt the configurations according to their preferences. In this context, designing concepts for supporting users in making decisions with respect to their desired level of privacy is reasonable.

With respect to collaborative working and learning, the consideration of two aspects is needed: First, the application should be enhanced by functionalities allowing for building up trust despite the possibility for intra-application partitioning of personal data and, thus, an increased level of anonymity. Beside an advanced role concept, a privacy-enhanced reputation system as it is already realised in parts for BluES'n belongs to functionalities addressed in that context. On the other hand, PRIME is primarily focussing on traditional client-server applications especially for service providers and users. Until now, collaborative approaches, where multiple clients respectively their users are interacting with each other, are not considered. However, using privacy-enhancing identity management for use cases on top of such multi-lateral interactions is thoroughly necessary for performing collaborative as well as privacy-supported team work.

Beyond the mentioned issues, an improvement of performance is necessary for practical deployments. PRIME does not integrate multi-threading technology and, therefore, it runs in just one single thread which means that all requests are sequentially processed, which is not sufficient for a collaborative application using the features of PRIME. Enhancing the collaborative functionalities provided by BluES'n might be also in the focus of further developments. Currently, concepts such as a privacy-enhanced eVoting,

cooperative content creation, and a BluES'n wiki exist only as design ideas or first prototypes. Their integration into BluES'n might contribute to a broader acceptance as well as the applicability of privacy-enhancing collaborative environments in general – and BluES'n in particular.