Project Number **027023**

APOSDLE: Advanced Process Oriented Self-Directed Learning Environment

Integrated Project

IST – Technology enhanced Learning

Legal and Ethical Issues Version 1

Deliverable D1.5

Due date	**2008-02-29**
Actual submission date	**2008-02-29**
Start date of project	2006-03-01
Duration	48
Revision	**Final**

Organisation name of lead contractor for this deliverable

SAP

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Dissemination Level

☒	PU	Public
☐	PP	Restricted to other programme participants (including the Commission Services)
☐	RE	Restricted to a group specified by the consortium (including the Commission Services)
☐	CO	Confidential, only for members of the consortium (including the Commission Services)

Disclaimer

Imprint

Full project title:	Advanced Process-Oriented Self-Directed Learning Environment
Title of work package:	WP 01: Work Processes
Document title:	Legal and Ethical Issues Version 1
Document Identifier:	APOSDLE-D01.5-SAP-Legal-and-Ethical-Issues1
Work package leader:	SAP
List of authors:	Andreas Zinnen (SAP) Manuel Görtz (SAP) Victor M. Garcia-Barrios, Günter Beham (TUG) Sybille Hambach (FhG) Stefanie Lindstaedt (KC)
Administrative Co-ordinator:	Harald Mayer
Scientific Co-ordinator:	Stefanie Lindstaedt

Copyright notice

Document History

Version	Date	Reason of change
1	2007-11-14	Document created
2	2008-02-26	Added input from TUG, FhG
3	2008-02-28	Added Executive Summary
4	2008-02-29	Final Version for Submission

Executive Summary

This document gives an overview of the activities the APOSDLE project consortium has undertaken in the first and second project year in the privacy area while rolling out the socio-technical solution APOSDLE into small or medium enterprises (SMEs) or departments of a global (European) company. In consultation with SAP's departments of Works Council, Corporate Legal and Data Protection & Privacy Office and IHK security consultants a privacy policy was specified to fulfil the seven principles Notice, Purpose, Consent, Security, Disclosure, Access and Accountability as stated in OECD's recommendations for protection of personal data and in directive 95/46/EC on the protection of personal data. The experiences and resulting privacy policy have been summarised in the paper "Privacy Issues when rolling out an E-Learning Solution" accepted for ED-Media 2008 in Vienna.

In the first chapter, the purpose and scope of this document are specified. Chapter "Directive 95/46/EC on the protection of personal data" motivates how Directive 95/46/EC protects individuals with regard to the processing of personal data and on the free movement of such data. Here, it must be noted that EU directives are addressed to the member states, and aren't legally binding for citizens in principle. The member states must transpose the directive into internal law. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998. All member states have enacted their own data protection legislation.

Chapter 3 steps into data protection principles at SAP. Instead of claiming to be complete, this chapter addresses the privacy basics which might be slightly different in another use case depending on boundary conditions of the company or country. In consultation with SAP departments of Works Council, Corporate Legal and Data Protection & Privacy Office a privacy policy was specified to fulfil the seven principles Notice, Purpose, Consent, Security, Disclosure, Access and Accountability as stated in OECD's recommendations for protection of personal data and in directive 95/46/EC on the protection of personal data. This policy will have to be signed by APOSDLE users before logging on for the first time.

Chapter 4 describes security management within APOSDLE. Here, security and privacy issues have to be implemented by the task observer, the security manager of the central server and the privacy enhancement services. The last paragraph shortly describes a potential approach to integrate Web Service Security as a standardized way to ensure SOAP message integrity and confidentiality.

The undertaken actions in terms of legal and technical issues shown in this report allow to roll-out APOSDLE into organisations. Finally, the success of the prototype or later an APOSDLE-like product depends heavily on the trust of the user into the system. This user behaviour will be studied during the evaluation of the second APOSDLE prototype in more detail.

Table of Contents

1 Introduction

1.1 Purpose of this document

This document describes privacy issues while rolling out the socio-technical solution APOSDLE into small or medium enterprises (SMEs) or departments of a global (European) company. In order to select relevant knowledge artefacts, the system accesses and stores privacy critical information like users' competencies, performed tasks or social contacts. In consultation with SAP's departments of Works Council, Corporate Legal and Data Protection & Privacy Office a privacy policy was specified to fulfil the seven principles Notice, Purpose, Consent, Security, Disclosure, Access and Accountability as stated in OECD's recommendations for protection of personal data and in directive 95/46/EC on the protection of personal data.

1.2 Scope of this document

Instead of claiming to be complete, this document addresses the privacy basics which might be slightly different in another use case depending on boundary conditions of the company or country. The integration of mechanisms to comply with the privacy rules is often neglected in research projects. However, these should be considered while designing research prototypes used for evaluation within real working environments.

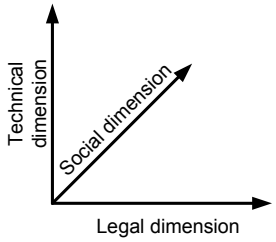

Figure 1 Three axis model for Legal and Ethical issues

We have identified three dimensions – as shown in Figure 1 – that have to be considered in order to address privacy issues in a socio-technical system like APOSDLE in a proper way. All these dimension will be covered in this document. However, the technical and legal dimension will be the main part. The legal aspects are covered in Section 2 and Section 3. The technical approaches to ensure privacy are described in Section 4. The ethical and social dimension will be covered in a separate forthcoming deliverable. In this deliverable the results from the evaluation of the APOSDLE system at the workplace will be presented. Showing if and how the trust of the user in respect to the system was.

1.3 Related Documents

EU data protection page: http://ec.europa.eu/justice_home/fsj/privacy/

2 Directive 95/46/EC on the protection of personal data

2.1 Privacy Context/History

Data privacy refers to the relationship between technology and the public expectation of privacy in the collection and sharing of data. Privacy concerns exist wherever uniquely identifiable data relating to a subject or several subjects are collected and stored. The storage might be in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The challenge of data privacy is to both share data and protect personally identifiable information. Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared. The legal protection of the right to privacy in general and of data privacy in particular varies greatly around the world.

The Universal Declaration of Human Rights states in its *§12* that:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence," subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence. In 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did.

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its “Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data”. The seven principles governing the OECD’s recommendations for protection of personal data were:

- *Notice:* Data subjects should be given notice when their data is being collected;
- *Purpose*: Data should only be used for the purpose stated and not for any other purposes;
- *Consent*: Data should not be disclosed without the data subject’s consent;
- *Security*: Collected data should be kept secure from any potential abuses;
- *Disclosure*: Data subjects should be informed as to who is collecting their data;
- *Access*: Data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- *Accountability*: Data subjects should have a method available to them to hold data collectors accountable for following the above principles

But the OECD Guidelines were nonbinding, and data privacy laws still varied widely across Europe. Therefore the European Commission decided to unify data protection regulation and submitted the Directive 95/46/EC on the protection of personal data.

2.2 Scope of 95/46/EC

Personal data is defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (§ 2a). This definition is meant to be very broad. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data" are address, credit card number, bank statements, criminal record, birth date etc.

The notion processing means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (§ 2b). The responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (§ 2d).

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (§ 4) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any on line shop trading with EU citizens will process some personal data and is using equipment in the EU to process the data (the customers' computer). As a consequence, the website operator would have to comply with the European data protection rules. The directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject.

2.3 Principles

Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose and proportionality.

2.3.1 Privacy Transparency

The data subject has the right to be informed when his personal data are being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. (§ 10 and 11)

Data may be processed only under the following circumstances (§ 7):

- When the data subject has given his consent
- When the processing is necessary for the performance of or the entering into a contract
- When processing is necessary for compliance with a legal obligation
- When processing is necessary in order to protect the vital interests of the data subject
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (§ 12)

2.3.2 Legitimate Process

Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. (§ 6b)

2.3.3 Proportionality

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (§ 6)

When sensitive personal data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply. (§ 8)

The data subject may object at any time to the processing of personal data for the purpose of direct marketing. (§ 14)

A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data. (§ 15) A form of appeal should be provided when automatic decision making processes are used.

2.3.4 Supervisory authority and the public register of processing operations

Each member state must set up a supervisory authority, an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated. (§ 28) Individuals may lodge complaints about violations to the supervisory authority or in a court of law.

- The controller must notify the supervisory authority before he starts to process data. The notification contains at least the following information (§ 19):
- The name and address of the controller and of his representative, if any;
- The purpose or purposes of the processing;
- A description of the category or categories of data subject and of the data or categories of data relating to them;
- The recipients or categories of recipient to whom the data might be disclosed;
- Proposed transfers of data to third countries;
- A general description of the measures taken to ensure security of processing.

This information is kept in a public register.

2.3.5 Transfer of personal data to third countries

“Third countries” is the term used in EU legislation to designate countries outside the European Union. Personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.

The European Commission has set up the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries.

The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbor Principles were the result. According to critics the Safe Harbor Principles do not provide for an adequate level of protection, because it contains less obligations for the controller and allows the contractual waiver of certain rights.

2.3.6 Implementation by the member states

EU directives are addressed to the member states, and aren't legally binding for citizens in principle. The member states must transpose the directive into internal law. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998. All member states have enacted their own data protection legislation.

2.4 Privacy in the Workplace

2.4.1 Data protection laws around the world

The following figure gives a short impression about countries with comprehensive data protection law, pending effort to enact laws or without any laws.

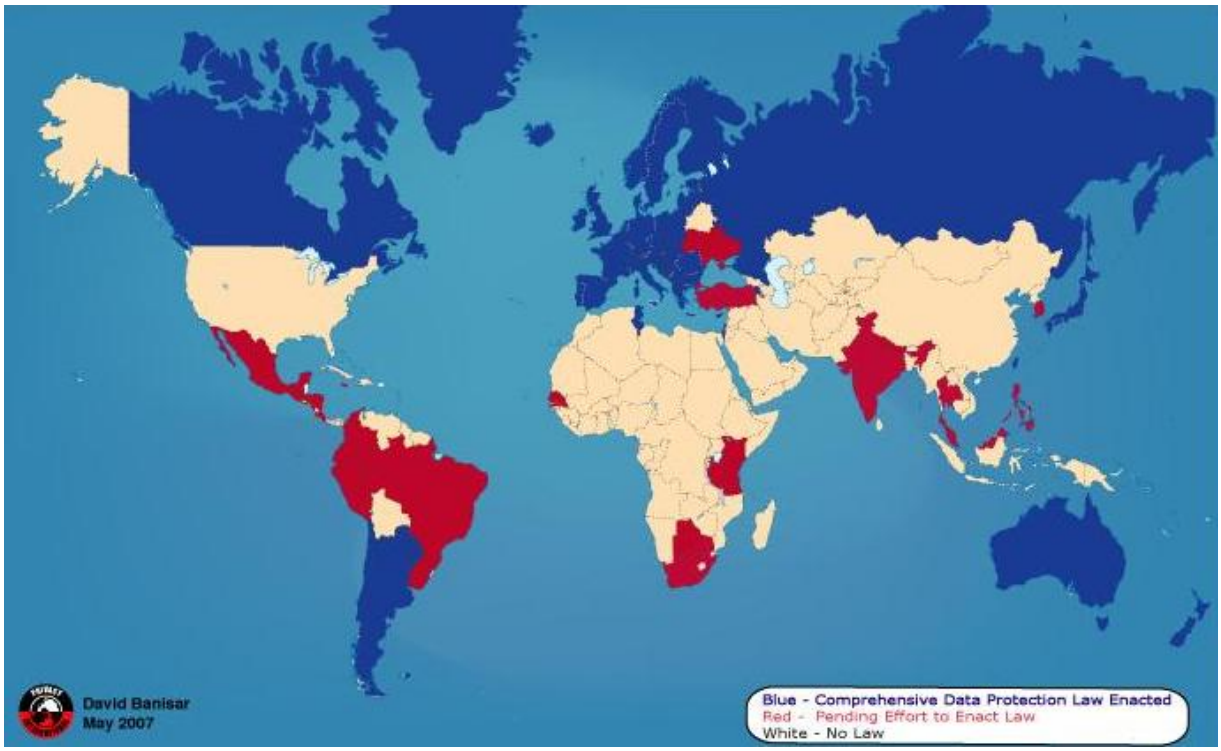

Figure 2 Data Protections Worldwide

2.4.2 European workplace privacy

The EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data limits and regulates the collection of personal information on individuals, including workers. Firms that monitor employees' use of e-mail, the internet or phones as part of their business practice, and do not tell employees or have not obtained employee consent to do so, can in most cases be sued under Article 8 the European Convention on Human Rights which provides for the right to respect for his private and family life. On the other hand, although EU law is clear that e-mail interception is illegal, the law is not totally clear as to whether companies may prohibit employees from sending private e-mails

2.4.3 U.S. workplace privacy

In the United States, the situation is quite different. Data privacy is not highly legislated or regulated in the U.S. In the United States, access to private data is culturally acceptable in many cases, such as credit reports for employment or housing purposes. In 2005 for example, a survey of more than 500 U.S. companies found that over half had disciplined and about one in four employers had terminated (fired) an employee for "inappropriate" use of the internet, such as sending an inappropriate e-mail message to a client or supervisor, neglecting work while chatting with friends, or viewing pornography during work hours

2.4.4 Other countries

Countries such as France protect privacy explicitly in their constitution (France's Declaration of the Rights of Man and of the Citizen), while the Supreme Court of the United States has found that the U.S. constitution contains "penumbras" that implicitly grant a right to privacy against government intrusion, for example in Griswold v. Connecticut (1965). Other countries without constitutional privacy protections have laws protecting privacy, such as the United Kingdom's Data Protection Act 1998 or Australia's Privacy Act 1988. The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as Directive 95/46.

3 Data Protection Principles @ SAP

In consultation with SAP departments of Works Council, Corporate Legal and Data Protection & Privacy Office a privacy policy was specified to fulfill the seven principles Notice, Purpose, Consent, Security, Disclosure, Access and Accountability as stated in OECD's recommendations for protection of personal data and in directive 95/46/EC on the protection of personal data. Instead of claiming to be complete, this section addresses the privacy basics which might be slightly different in another use case depending on boundary conditions of the company or country.

3.1 Overview

The figure below illustrates involved roles in the data protection process at SAP.

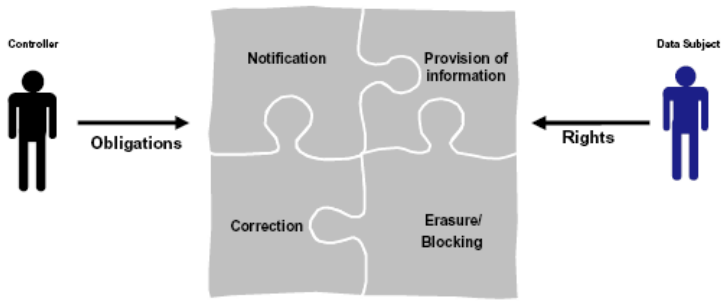

Figure 3 Data Protection Process at SAP

1. The controller is the legal party in charge of the processing of the data, e.g. the company in general, but also derived down to the single employee processing data on behalf of the company.
2. As an employee of SAP AG or one of the subsidiaries you will get in touch with data protection in many ways:
   - You are working in areas where personal data is collected and processed
   - You have access to personal data, e.g. to the internal address book with e-mail addresses, phone numbers, positions of all employees in SAPNet
   - You are developing software for processing of personal data, which has to be compliant to data protection needs
   - You collaborate with customers, suppliers and other subsidiaries of SAP AG and transfer or receive personal data
   - Your own personal data is processed by SAP AG and/or the subsidiaries, you are also „Data Subject" to this processing
3. Data subjects have a set of inalienable rights against the "controller" and third parties:
   - Notification
   - Provision of information
   - Correction, erasure, blocking

3.2 Scope – What is personal data @ SAP

At SAP the BDSG Section 3 of the Federal Data Protection Act is in place. The detailed information about what personal data is is shown in Figure 4.

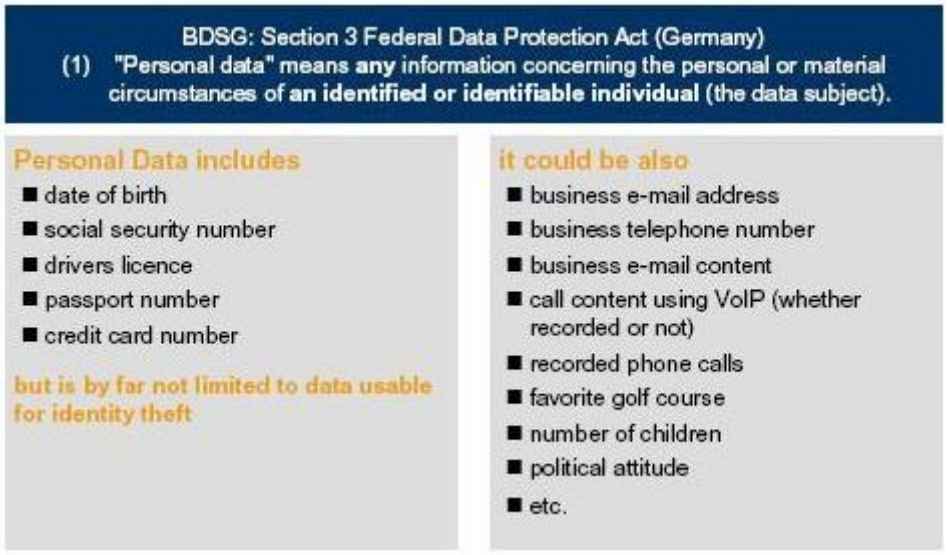

Figure 4 Federal Data Protection Action

3.3 Involved Organisation Units

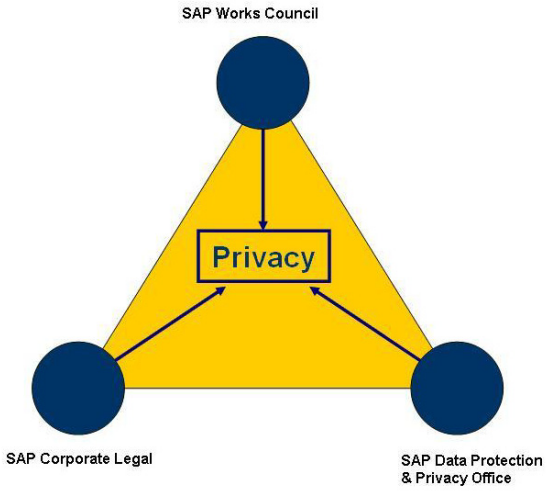

Figure 5 Involved Organisation Units

Three SAP organizational units supervise the rollout of privacy critical products within the company.

1. SAP Corporate Legal:
   - Representing SAP in proceedings before the labour court
   - Providing advice to the Executive Board regarding the implementation of legal changes
   - Distributing information about legal changes to all affected parties within SAP

- Contributing to projects of the Executive Board and the HR department
- Focusing and guiding the collaboration between SAP's specialists for European law and legal regulations

2. SAP Works Council:
   - A works council is a "shop-floor" organization representing workers, which functions as local/firm-level complement to national labour negotiations. Works councils exist with different names in a variety of related forms in a number of European countries, including Germany (Betriebsrat), the Netherlands and Belgium (Ondernemingsraad), France (Comité d'Entreprise), Belgium (Conseil d'Entreprise) and Spain (Comité de empresa).
3. SAP Data Protection & Privacy Office (DPPO):
   - DPPO is a supervisory authority ensuring the protection and privacy of all data collected, processed or used within SAP's field of responsibility including employees' and clients' data. DPPO supports SAP and SAP employees in following and meeting the security laws.

In accord with those three instances, we developed a privacy policy for APOSDLE within SAP. See the next section for the policy. Users of APOSDLE have to accept the policy before using the system. The policy will be show while starting the system the first time. Users can withdraw

3.4 Privacy Policy for APOSDLE (Data Protection & Privacy)

Purpose of the APOSDLE System

APOSDLE will conceptually integrate the three roles a knowledge worker fills at the workplace (Worker, Learner and Expert), and provides integrated technological support for these roles.

- Work: APOSDLE automatically identifies the knowledge worker's needs and provides context-sensitive support tailored to their specific learning goals and work situations.
- Learn: APOSDLE helps knowledge workers explore, apply and reflect on knowledge in a self-directed manner: By considering their work context, APOSDLE ensures that learning and working are tightly integrated and learning is transferred to actual workplace tasks.
- Collaborate: APOSDLE helps knowledge workers to informally convey and jointly create knowledge via their computational environment and embedded in their work context. The context of knowledge transfer and creation is captured in order to turn knowledge artifacts into valuable learning resources. The system proposes collaboration partners with low social distance for specific problems. Both participants of collaboration have to agree on the collaboration.

Legally responsible unit and basis for collection and usage of data

The data (outlined below in DETAILS) will be collected and applied in APOSDLE instances deployed in several independent legal entities (list of APOSDLE partners: http://www.aposdle.tugraz.at/partners). Your personal data is collected and used only with your explicit consent, given by actively clicking the "I accept" button". In case you decline to accept this privacy agreement, you will not be able to use APOSDLE. The collected data within APOSDLE is used for the operation of the APOSDLE system itself and can be used by APOSDLE partners for statistical analysis of research questions.

Data Maintenance

A proper maintenance of the learning resources and personal learning goals in the APOSDLE system is a key for achieving our objective to provide an advanced process oriented self-directed learning environment. Every participating person is asked to create and maintain their personal performed task

profile as well as knowledge artifacts. Participation is voluntary. It is suggested that you check and update the information in your personal performed task profile at least several times a year.

Access to your data

All personal data will only be used for the purposes outlined in this document. Your data will be treated according to the German Federal Data Protection Act (Bundesdatenschutzgesetz). Through saving the transaction you agree to the processing and transfer of your data (outlined below in DETAILS). The consent can be revoked at each time. Consequently, the collected data will be made anonymous or deleted.

Administrators of the APOSDLE system will have access to all collected data. Users of the APOSDLE system will see your contact information and performed tasks as described in following details section. Access to collaboration contents will be granted to other persons after explicit agreement.

Details

- What information do we collect and why?
  - Activity Recognition:
    - Training of the models: (Desktop Context)
      - User Interaction: Keyboard and Mouse interaction (mouse position, entered words, letters) of several test users will be collected. The data is stored as hash values, not in clear text. The hash values will be used for statistical analysis. Results of the statistical analysis are activity models for each trained activity. All data is stored anonymous; therefore, drawing conclusions from the hash values or models to the test users' identities cannot be drawn.
      - System Status: The system status includes activities on the file system (access/delete/modify/rename/delete directories/files/documents), started/stopped applications, sending/receiving emails, visited or bookmarked web sites, content of documents, visited web sites or emails, printed documents, and finally the username. The data is stored as hash values, not in clear text. The hash values will be used for statistical analysis. A result of this statistical analysis is models for each trained activity. All data is stored anonymous; therefore, drawing conclusions from the hash values or models to the test users' identities cannot be drawn.
    - Applying the models to APOSDLE users for activity recognition:
      - For applying the trained models to the current Desktop Context, the same data as described in the training phase will be collected. The data will be collected as hash values, not in clear text; furthermore, the data is not stored permanently on a disk, instead it is kept in the working memory to recognize the current user's activity. After closing the application, the data will be lost.
  - Collaboration:

    To find adequate experts, the system stores following APOSDLE user data. This data can be seen by all APOSDLE partners (see following URL http://www.aposdle.tugraz.at/partners).
    - Starting a collaboration:
      - In-house Address/Email/Phone Number/Messenger IDs: Other participants of APOSDLE can contact you via e-mail, mail, phone or messenger. You can choose not to be contacted at any time.
      - Organizational Unit/Job Role: The organizational unit and job role are considered in the social distance between APOSDLE participants while proposing collaboration partners.

- Name/First Name/Picture: Name, first name and a picture are part of the general contact information. The picture mainly helps to visualize the collaboration partner. The user can choose to not publish his/her picture.
- Performed Tasks, number of executions: For a selection of according experts, the APOSDLE system stores information about users' performed tasks and processed learning resources. The system also stores how often a task was performed. Assured by a low granularity of the collected information, conclusions about users' performance and overall learning goals in a whole work context cannot be drawn.

▪ Extracting new learning artefacts from a collaboration: Contents of the collaboration (e.g. chat contents) might be extracted and reused as future learning resources. Learning artefacts from collaboration will not be stored and published automatically. APOSDLE will provide an editing tool for the collaboration contents. Both parties must approve the publication before the contents will be accessible to third persons. A proper objectification is primitive before the publication. After making the artefacts public, they can be provided as learning material to all users of the APOSDLE system (see http://www.aposdle.tugraz.at/partners).

o Retrieval of adequate learning material: For a selection of the according learning resources, the APOSDLE system stores information about users' performed tasks and processed learning resources. Assured by a low granularity of the collected information, conclusions about users' performance and overall competencies in a whole work context cannot be drawn.

- Period of Time: The data will be deleted in reasonable time if the user revokes the privacy agreement. Please send an email to following address if you want your data to be deleted: delete@aposdle.com
- Links to Other Site: This system contains links to other sites. APOSDLE is not responsible for the privacy practices or the content of other Web sites and documents.
- Inquiries: If you have any questions about this privacy statement – if, for example, you wish to inspect, update or delete the information we hold about you – feel free to contact:

Project APOSDLE

SAP Research CEC Darmstadt

Bleichstr. 8

64283 Darmstadt, Germany

3.5 Foundations

§3 BDSG

"Personal data" means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject). Within business context even many attributes are seen as "personal" in one way or the other. Several rules apply if you want to use personal data. First of all, every use and processing is forbidden by default.

§ 2 Directive 95/46/EC:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular

by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

§ 6 Directive 95/46/EC:

Member States shall provide that personal data must be:

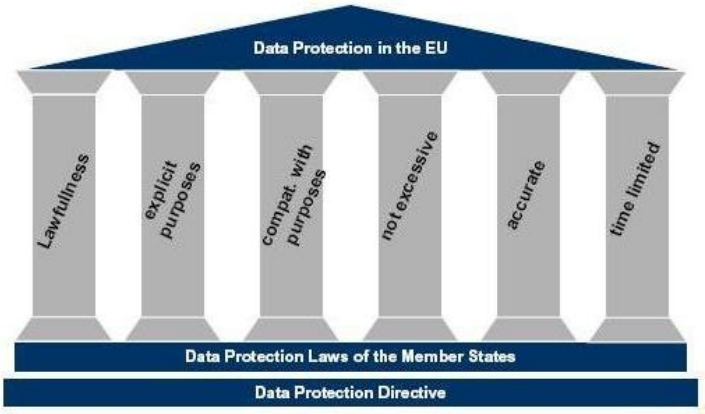

Figure 6 Data Protection in the EU

- Processed fairly and lawfully;
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

§ 7 Directive 95/46/EC:

Member States shall provide that personal data may be processed only if:

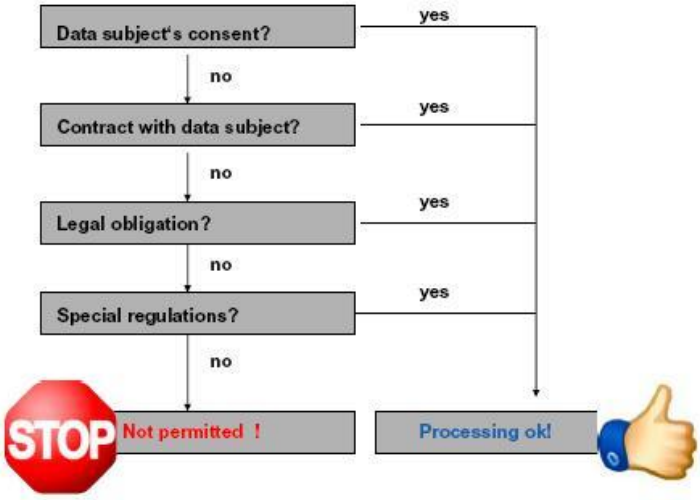

Figure 7 Directive 95/46/EC

- The data subject has unambiguously given his consent (can be withdrawn); or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary in order to protect the vital interests of the data subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under § 1 (1).

Section 33 BDSG:

Notification of the data subject: If personal data are stored for the first time for one's own purposes without the data subject's knowledge, the data subject shall be notified of such storage, the type of data, the purposes of collection, processing or use and the identity of the controller. If personal data are stored in the course of business without the data subject's knowledge for the purpose of transfer, the data subject shall be notified of their initial transfer and of the type of data transferred.

Section 34 BDSG:

Provision of information to the data subject The data subject may request information on
1. Stored data concerning him, including any reference in them to their origin and recipient,
2. Recipients or categories of recipients to whom data are transmitted and
3. The purpose of storage.

Principle 41 - Directive 95/46/EC:

Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

Section 35 BDSG:

Correction, erasure and blocking of data:

1. Incorrect personal data shall be corrected.
2. Apart from the cases mentioned in paragraph 3, Nos. 1 and 2, below personal data may be erased at any time. They shall be erased if
    a. Their storage is inadmissible,
    b. They relate to health matters, criminal offences, administrative offences as well as religious or political views and the controller of the data file cannot prove that they are correct,
    c. They are processed for one's own purposes, as soon as knowledge of them is no longer needed for fulfilling the purpose for which they are stored, or
    d. They are processed in the normal course of business for the purpose of communication and an examination five calendar years after their first being stored shows that further storage is not necessary.
3. Instead of erasure, personal data shall be blocked in so far as
    a. In the case of paragraph 2, No. 3 or 4 above, preservation periods prescribed by law, statutes or contracts rule out any erasure,
    b. There is reason to assume that erasure would impair legitimate interests of the data subject or
    c. Erasure is not possible or is only possible with disproportionate effort due to the specific type of storage.
4. Personal data shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect.
5. Where they are stored in the normal course of business for the purpose of communication, personal data which are incorrect or whose correctness is disputed need not be corrected, blocked or erased except in the cases mentioned in paragraph 2, No. 2 above, if they are taken from generally accessible sources and are stored for documentation purposes. At the request of the data subject, his counterstatement shall be added to the data for the duration of their storage. The data may not be communicated without this counter-statement.
6. If necessary to protect legitimate interests of the data subject, the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage shall be notified to the bodies to which these data are transmitted for storage within the framework of regular data communication.
7. Blocked data may be communicated or used without the consent of the data subject only if
    a. This is indispensable for scientific purposes, for use as evidence or for other reasons in the overriding interests of the controller of the data file or a third party and

b. Communication or use of the data for this purpose would be admissible if they were not locked.

§ 10 Directive 95/46/EC:

Information in cases of collection of data from the data subject: Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

1. The identity of the controller and of his representative, if any;
2. The purposes of the processing for which the data are intended;
3. Any further information such as
   - The recipients or categories of recipients of the data,
   - Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
   - The existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

3.6 Summary

This section described privacy issues while rolling out APOSDLE into organizations like SAP. In consultation with the SAP Works Council, Corporate Legal and Data Protection & Privacy Office, a privacy policy was specified to fulfil the seven principles Notice, Purpose, Consent, Security, Disclosure, Access and Accountability as stated in OECD's recommendations for protection of personal data and in directive 95/46/EC on the protection of personal data. Even for research projects, privacy is an important issue that cannot be ignored. It is not allowed to collect private data even for research purposes in a global European company. The users always must be informed and explicitly agree that the specified data can be collected. Our findings should raise awareness and provide some basic insights into the topic of privacy in socio-technical systems.

4 APOSDLE Security Management

This section introduces the technical solutions which have been implemented in APOSDLE to address the technical issues as shown as one axis in Figure 1 These technical solutions are necessary to comply with the regulations introduces in Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

To provide a learner with helpful and suitable learning material in form of documents, Learning Events, or previously generated multimedia courses, the e-learning environment strongly has to take the learner's work task, his competencies, his preferences and his history into account. These information are referred in APOSDLE as the user's context. A collection of learners' essential context information introduces wide privacy and security issues in context-aware informal e-learning environments. The APOSDLE application automatically records the user activity both on client side (the user's personal computer) and server side. The logging works implicitly, i.e. it is not triggered by a particular user action, but just as "the sum of all user actions". Subsection 4.1 describes how this privacy critical information can be collected and stored in a secure way.

Furthermore, the Platform Interface (PI) acts as a central connection point for different components in the system. It will be shown how the security management is operating. APOSDLE's PI is separated into a number of *Service Interfaces* that are exposed as Web Services. Two additional APOSDLE components exist and tightly interact with the PI before passing messages to/from the Platform, namely the Security Manager (see Section 4.2) and the Privacy Enhancement Service (see Section 4.3).

Finally, a short introduction of WSS Security (see Section 4.4) will be given although message encryption and integrity are not yet implemented within the APOSDLE intranet application.

4.1 Security within the Task Observer

Different kinds of user interaction with the desktop and switches in the system state are recorded. An exhaustive list of possible sensors is represented in Figure 8:

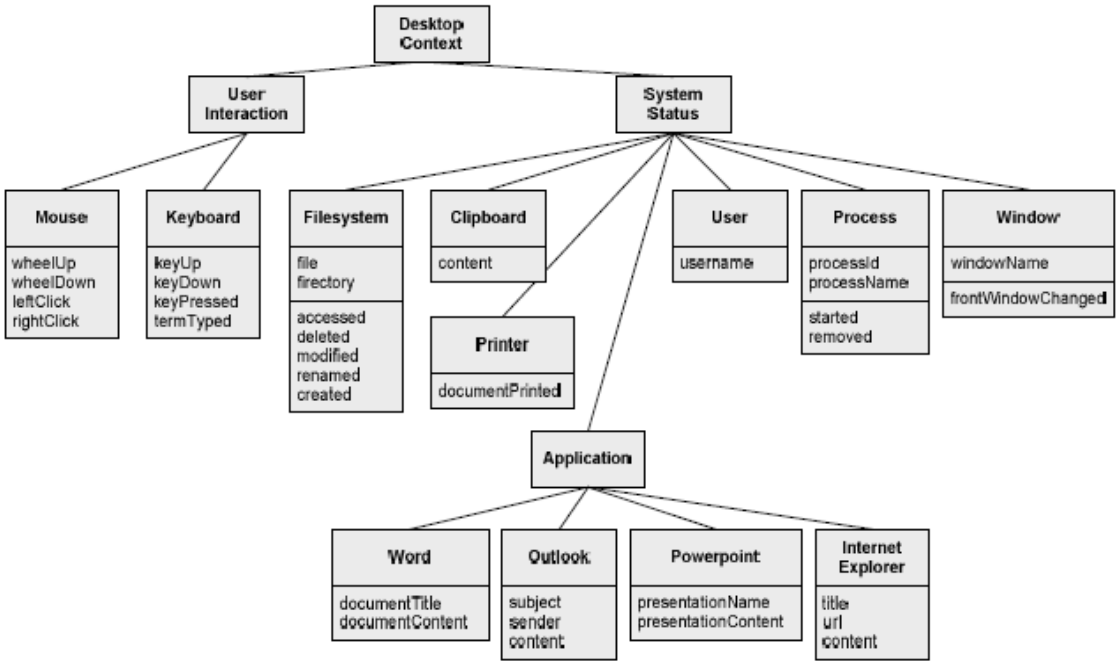

Figure 8 Overview of Context Sensors

Different classes of desktop sensors potentially reveal highly sensitive data like passwords, credit card data, or private chats and visited URLs. Not only the user is loosing control over his work history and aggregated user profile data but also context-aware system with rich context models are able to disclose security-relevant access control data. The APOSDLE application implies the strong need for protecting sensitive context information from misuse.

In many cases, logging and polling context information is an inherent loss of users' privacy since context data is potentially very sensitive. Even though the privacy statement as described in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** provides the legal background to operate a system such as APOSDLE additional mechanisms must be in place to increase the user's trust in the system. The introduction of protection measures will ensure privacy and security of the users' collected context information and therefore raise trust and acceptance in context-aware systems and promote their dissemination. Following section motivates how data obfuscation algorithms assure privacy and security of sensitive context information without eliminating a context-adaptive of the context data.

Two scenarios have to be taken into account:

Scenario 1:

Only local context attributes are collected. Local context attributes are defined as information that can be monitored on the user's electronic workplace (computer desktop environment). Furthermore, all processing of context data is computed on the device itself on which the context is monitored. No external parties are involved in any context analysis step and the user's context is not disseminated. The problem hereby is the storage of the context history on the local machine. Such storage is essential because many personalized systems need to acquire a certain amount of context data to adapt themselves accordingly. It becomes obvious that the unsecured long-term storage of context information is a possible threat for sensitive data of the user that needs to be solved.

Scenario 2:

After obtaining the context information on the client side, context-enriched queries are constructed and sent to some distant information retrieval service (e.g. search engine). The provided results are often offered to the user in forms of links to documents or other informal learning material, whose relevance to the actual user's task or intension is often higher than the results of manual queries without context-enrichment. Especially the distributed scenario of context adaptation creates some serious problems in ensuring the security and privacy of sensitive context information. As soon as the context items are transmitted, the user fully looses control over them. Not only that the transport channel can be intercepted and unencrypted data can be logged, but also apparently trustworthy 3rd-party servers (e.g. intranet enterprise search solutions) can be compromised or intentionally publish sensitive information later on.

In the APOSDLE project we apply a modification in the context processing procedure (see Figure 9) to overcome the privacy and security threats of disseminating sensitive context information (Scenario 2) and logging context information (Scenario 1). We insert a special data obfuscation step after the context elicitation at the end of the context pre-processing that masks all context information, so that no sensitive data is visible anymore thereafter.

Data 'obfuscation' (anonymisation) is applied to the stored log data on the client side. This is a one-way encryption which prohibits clear-text readability of the data for humans and cannot be reverted (irreversibility of anonymisation). But it preserves statistical patterns for further analysis purposes or for the analysis of the interaction patterns with the APOSDLE UI.

An example of a string of an unobfuscated client-side log file of the APOSDLE context monitor is:

```
<event eventName="FRONTWINDOW_CHANGED" atTime="07.03.2007 14:22:53"
eventCategory="Process">
<eventattribute name="processname" type="String" value="iexplore.exe" />
<eventattribute name="windowtitle" type="String" value="Microsoft Internet
Explorer" />
</event>
```

This string means that on 2007-03-07 at 14:22:53 the user changed the active foreground window to Microsoft Internet Explorer with a process name of iexplore.exe. At the user's client side this data is stored obfuscated: it is neither possible to extract a particular user from a log file nor does the log file contain details of the work process.

Similar 'obfuscation' applies to the logging data in the APOSDLE User Profile Service. It shall be emphasised that in APOSDLE the User ID is NOT related to the User Information (name, email, etc). Always when a User selects a task in the APOSDLE sidebar, the APOSDLE User Profile Service logs the Task-Identifier (YAWLid) and the "Starting Time" (timestamp). APOSDLE will not log how long the User has performed the same task. APOSDLE does not log the user's name, or other personal data of the user, but only the User ID. No personal information of a User can be accessed via his/her User ID.

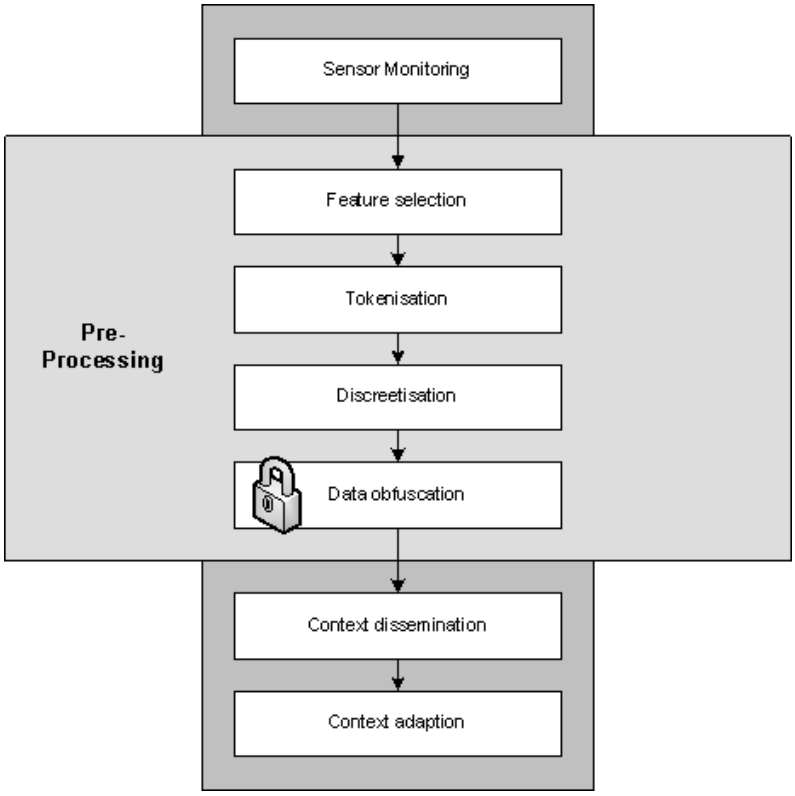

Figure 9 Obfuscation Processing Steps

As obfuscation function we apply a cryptographic hashing function $H(x)$, where we instantiate $H(x)$ with the SHA256 [Nat01] hash sum. MD5 and SHA-1 are no more recommended for general usage by the NIST1, because they have be significantly weakened in the recent past, see [Kli05] and [WYY05] for details. $H(x)$-obfuscation ensures that previously highly sensitive data like captured passwords or visited URLs are no longer stored in clear text and can comfortably be disseminated. Though the concept of cryptographic hashing is not new in general, the way of using it within context-aware e-learning application and the modification as described here is.

The basic idea is that the data of interest can be detected in the hash data. This is achieved by pre-calculating the hash-values of known or expected words (such as the concepts in the domain ontology or key-words in the knowledge artefact repository). These hashes can then be compared with the hashes in the logs. However, word such as passwords are (hopefully) not dictionary or known words such that no known hash exist. This way the sensitive data is protected while the automatic task detection still can use the log-data. The whole hashing process is illustrated in Figure 10 .

Figure 10 Hashing Process

Additionally, it can be configured to protect the hash values against brute force and dictionary attacks by concatenating the input token to $H(x)$ with a secure user id. This unique user-specific id is obtained from the Microsoft Windows identity model and not known to a remote party. This approach leads to different $H(x)$-values for two users, who obfuscate the same token. As a result of those prefix equivalence classes a disseminated context fingerprint can not easily be compared to pre-calculated lists of hash values of all possible context fingerprints. This would result in multiple $H(x)$-obfuscated tokens with the same prefix class and consequently the inability to determine the original token value.

A user dependent hashing would not allow drawing statistical conclusions from other users' performed tasks. Nevertheless, privacy critical information like passwords or visited URLs will not be traceable by third parties. The obvious advantage of $H(x)$-obfuscation is, that even authorised administrators or the user his/herself cannot recover the original data. This lets users disseminate probably sensitive context information in a degraded way in forms of obfuscated data, so that many applications are still able to calculate context-based results or context-triggered actions.

It has to be stated that while the context log data is obfuscated other logging data is stored in clear text. This is the case for all the logging information collected during the use of the APOSDLE Sidebar or within the APOSDLE Platform. However, it is expected that these data is not as sensitive as the logged data of the context monitor.

4.2 Securing Message Exchange using Security Management

If some privacy policies are defined for a service interface, the PES works as information filter during the transfer of messages between PI and the APOSDLE Platform. When a Web service call arrives to the Platform Interface (after a successful user authentication steered by the Security Manager), it is forwarded to the Privacy Enhancement Service, which is responsible of fetching/filtering the required information. In the meantime, the Platform Interface waits for a response from the Privacy Enhancement Service. The response is then sent back remotely to the requesting client.

4.2.1 Security Manager

The Security Manager is a part of the APOSDLE Platform and is strongly tied to the APOSDLE Platform Interface. The three main responsibilities of this module are:

- User authentication
- Session handling
- Storage/retrieval of user master data

As shown in Figure 11, the management of user authentication and the persisting of master data are realised by means of an LDAP directory server. The data about user sessions contains credential user information, such as (a) an authentication token to allow single sign-on when using the different APOSDLE clients (e.g. Sidebar, Annotation tool, etc.) and (b) the system security id for accessing file system resources in the Data Object Repository. Session data is created on each platform login and remains in the memory of the Platform until a user logs out or until the platform is shut down. This session-related data cannot be persisted.

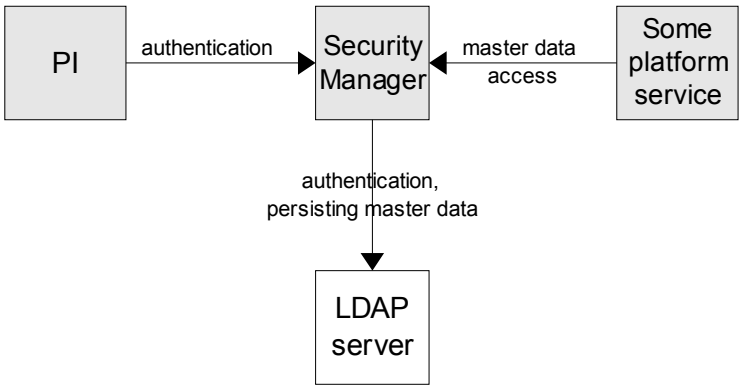

Figure 11 Security Manager Schema

The general functionality regarding the implementation of the Security Manger is shown in Figure 12. A login call to the Platform Interface is bridged directly to the Security Manager, which in turn, checks the users' credentials against an LDAP[1] directory server. If the request succeeded, a session will be created. This session holds all the credential data of the user as well as the master data found on the LDAP system. A secret authentication token is then returned to the client allowing further requests to the platform. Every Web service call received by the Platform Interface contains an authentication token from the client (i.e. it includes a session id). This token is then checked by the Security Manager for its validity. Successful requests will return the user credentials to the Platform Interface, which then can proceed with the call to the specific Platform service. In contrast, invalid tokens will cause an Exception that will be delivered back to the client, thus, avoiding an access to the corresponding service.

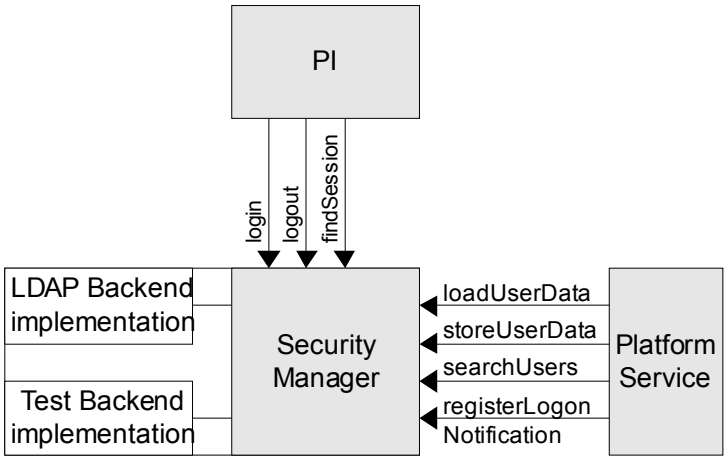

Figure 12 Security Manager Message Flow

Further, every service of the Platform that has access to a user credential data may also request user master data from the Security Manager. So, it is possible to access the own as well another user's master data. The Security Manager itself will return all data that is accessible on the LDAP server. It is subject to the Privacy Enhancement Service to filter out data from users which would not consent in sharing their master data.

1 The platform will be delivered with an OpenLDAP 2 server and a tool to import tables of user data into it.

Finally, a notification mechanism exists to inform about login and logout operations. Platform services can register to these notifications in case they need to set certain actions on a user's login or logout.

4.3 Privacy Enhancement Services

The Privacy Enhancement Service (PES) provides a filtering layer between the Platform Interface and the Platform services (see Figure 11). It is the task of the PES to remove all data from the requests from/to the platform services that a user did not consent in sharing. Therefore, the PES introduces and distinguishes among the following three Privacy Levels:

- *Identified Public* User
- *Identified Private* User
- *Anonymous* User

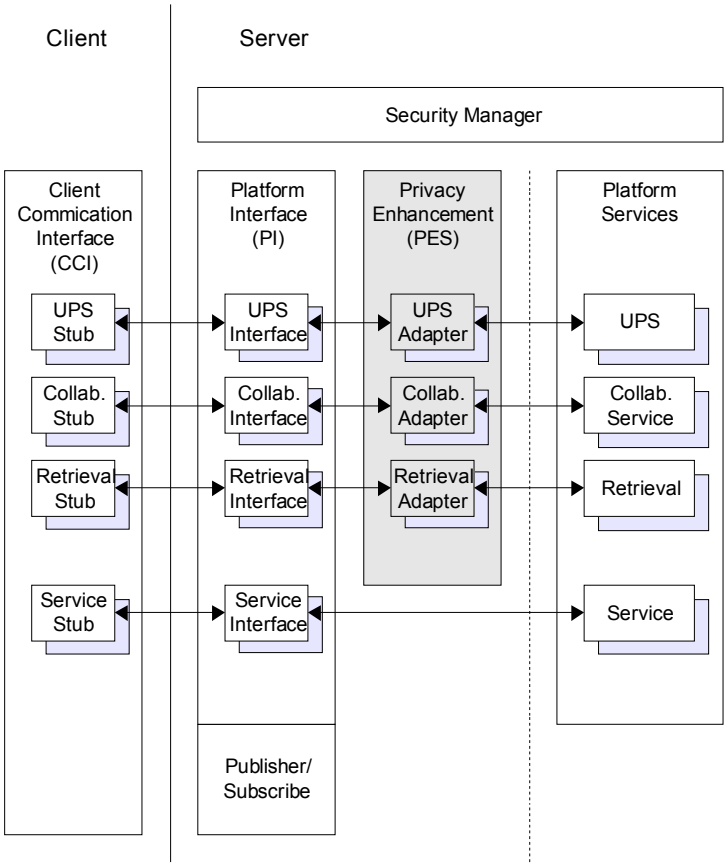

Figure 13 Privacy Enhancement Service Client/Server view

Each of the aforementioned privacy levels consists of a set of attributes that regulate access to the users Business Card, the users Preferences, the Learn and the Work history, as well as whether the user is visible as an expert, or if timestamps should be recorded within the tracked behaviour data stream. The latter privacy issue is allowed for all three privacy levels as for the second APOSLDE prototype, since the services depend on these timestamps.

Further, the PES filters data on learning goal histories, task histories, collaboration histories, on user's master data, and on knowledge artefacts. As for the second prototype, the PES filters the client calls

to the User Profile and the Collaboration modules, and triggers the access-rights check of the Data Object Repository for knowledge artefacts delivered by the Retrieval Service.

The implementation of PES (as depicted in Figure 12) is based on the Sun-XACML engine. XACML is a rule-based standardized[2] policy language. The Sun-XACML engine delivers an interpreter for these policies. It delivers a permit/deny response on the actions applied plus (eventually) an optional set of obligations to fulfil. For the responses to be filtered, the PES defines adapters corresponding to the originally called services. On every client request, the Policy Evaluation Point (PEP) will execute the policy engine. Based on the result of the policy evaluation, (a) none, (b) some or (c) all data will be removed from the response data before it is passed back to the Platform Interface. It is worth mentioning at this point that client requests are never blocked by the PES, only the data from the corresponding responses may be removed from it.

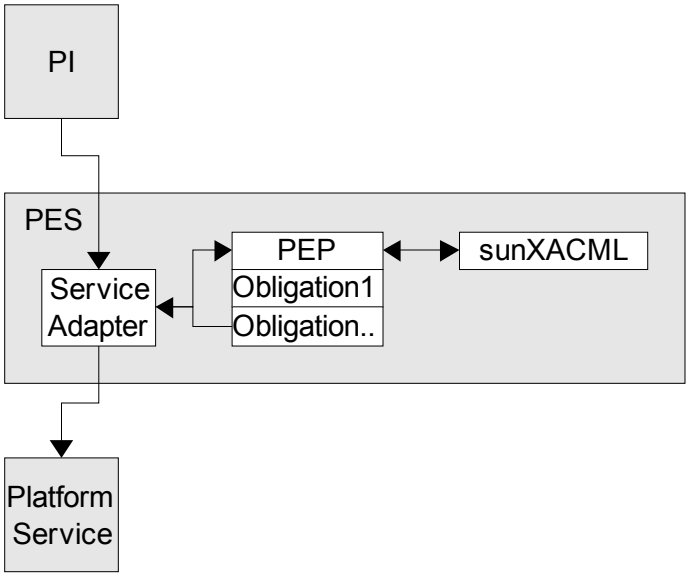

Figure 14 Privacy Enhancement Service

Filtering the data of responses is done by means of requirements stipulated in the obligations. These obligations are built by an internal Factory as specified by the result of the policy evaluation. Thus, privacy-related obligations are represented by a dynamically instantiated Chain of filters. In turn, the PEP hands on the data to the chain of these filters, and its resulting output is returned to the Service Adapter. Only after this procedure, the call is passed on to the target service.

4.4 OASIS WSS Security

The goal of WSS security is to enable applications to conduct secure SOAP message exchanges. The model provides three main mechanisms: the ability to send security tokens as part of a message, message integrity, and message confidentiality. It is designed to work with the general SOAP [SOAP11, SOAP12] message structure and message processing model.

- An authority can vouch for or endorse the claims in a security token by using its key to sign or encrypt (it is recommended to use a keyed encryption) the security token thereby enabling the authentication of the claims in the token. An X.509 [X509] certificate, claiming the binding between one's identity and public key, is an example of a signed security token endorsed by the certificate authority.

2 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

- Message integrity is provided by XML Signature [XMLSIG] in conjunction with security tokens to ensure that modifications to messages are detected. The integrity mechanisms are designed to support multiple signatures, potentially by multiple SOAP actors/roles, and to be extensible to support additional signature formats
- Message confidentiality leverages XML Encryption [XMLENC] in conjunction with security tokens to keep portions of a SOAP message confidential. The encryption mechanisms are designed to support additional encryption processes and operations by multiple SOAP actors/roles.

The model defines a <wsse:Security> element for security relevant content of a SOAP message.

```
<S11:Envelope>
    <S11:Header>
            ...
        <wsse:Security S11:actor="..." S11:mustUnderstand="...">
            ...
        </wsse:Security>
            ...
    </S11:Header>
    ...
</S11:Envelope>
```

The <wsse:UsernameToken> element is introduced as a way of providing a username. More specifically, it describes how a web service consumer can supply a Username Token as a means of identifying the requestor by “username”, and optionally using a password (or shared secret, or password equivalent) to authenticate that identity to the web service producer. Within the <wsse:UsernameToken> element, a <wsse:Password> element may be specified.

Passwords of type wsse:PasswordText and wsse:PasswordDigest are not limited to actual passwords, although this is a common case. Any password equivalent such as a derived password or S/KEY (one time password) can be used. Having a type of wsse:PasswordText, wsse:PasswordDigest merely implies that the information held in the password is “in the clear”, as opposed to holding a “digest” of the information. For example, if a server does not have access to the clear text of a password but does have the hash, then the hash is considered a password equivalent and can be used anywhere where a "password" is indicated in this specification.

The WSS specification is meant to provide extensible framework and flexible syntax, with which one could implement various security mechanisms. The framework and syntax by itself does not provide any guarantee of security.

An example implementation that could be used within APOSDLE considering WSS security is the Web Services Project @ Apache. Apache WSS4J is an implementation of the OASIS Web Services Security (WS-Security) from OASIS Web Services Security TC. WSS4J is a primarily a Java library that can be used to sign and verify SOAP Messages with WS-Security information. WSS4J uses Apache Axis and Apache XML-Security projects and is interoperable with JAX-RPC based server/clients and .NET server/clients.

4.5 Privacy Issues in Cooperation

For the APOSDLE contextualized cooperation concept it is assumed, that basic security as well as basic privacy has been established as regulated by national law and international guidelines[3]. Furthermore it is assumed, that user profile data is accessible for the APOSDLE system and other users (privacy level »identified public«) Taking this into account, there are two questions to be answered for contextualized cooperation within APOSDLE:

[3] See DII.3 »Conceptual Framework and Architecture Version 1«, p. 55f. as well as DI.5 »Legal & Ethical Issues Version 1«

1. What user data is needed for APOSDLE contextualized cooperation and what services may be provided based on this data (systems perspective)?
2. How can the correlation between data provision and quality of services be made transparent to the user and how can he be rewarded for providing the data (user perspective)?

In the following sections we will further explore these questions and provide some ideas on how to answer them.

4.5.1 System perspective

For APOSDLE contextualized cooperation there is a close correlation between the data an APOSDLE user provides about herself and her cooperation activities on one hand side and the services to be provided by the APOSDLE system on the other hand side. This correlation is explained along the APOSDLE contextualized cooperation process as described in section xx of this deliverable. For each data item to be discussed we distinguish

- *Must-have* vs. *nice-to-have* for the necessity a data item is needed.
  If a data item (first column »Data item to be collected« of the respective table) is marked as *must-have* (second column »Necessity«) it is absolutely necessary to have this data in order to provide the corresponding service (last column »Reason for data collection«); if the data item is marked *nice-to-have* the service could be improved.
- *This* vs. *future* for the cooperation event a data item is needed for.
  If a data item is marked as *this* (third column »Cooperation Event«) the data collected is used to provide APOSDLE services for the cooperation at hand; if the data item is marked *future,* future cooperation events of (possibly) other cooperation partners are affected.

The following listings of data items and corresponding reasons for data collection per phase of the APOSDLE contextualized cooperation concept give an impression of the impact of data availability on APOSDLE service provision.

4.5.1.1 Pre-cooperation phase

During the pre-cooperation phase data will be collected of the knowledge seeker as summarized in table 1.

Data item to be collected	Necessity	Occasion	Reason for data collection
Task of KS	Must-have	this	pre-selecting knowledgeable persons
Learning goal of KS	nice-to-have	this, future	pre-selecting knowledgeable persons
Cooperation object	must-have	this	pre-selecting cooperation tool
Description of problem/question	nice-to-have	this	pre-selecting cooperation tool pre-selecting knowledgeable persons
Description of expected outcome	nice-to-have	this	pre-selecting cooperation tool
KP name	nice-to-have	future	refining pre-selection of knowledgeable persons
Urgency for cooperation	nice-to-have	this	pre-selecting cooperation tool
Level of contextualization	nice-to-have	this	pre-selecting cooperation tool

Table 1: Data collection and its impact for APOSDLE services within pre-cooperation phase

4.5.1.2 Cooperation phase

During the cooperation phase data will be collected of all cooperation partners, the knowledge seeker as well as (one or more) knowledgeable persons, and of the cooperation event as summarized in table 2.

Data to be collected	Necessity	Occasion	Reason for data collection
KS name	Must-have	This	Transferring result to KS cooperation management space
KP name	Must-have	This	Transferring result to KP cooperation management space
Start/end date and time	Must-have	This	Transferring result to KS/KP cooperation management space
Cooperation log	Must-have	This	Pre-computing cooperation result
Tool	Must-have	This	Transferring result to KS/KP cooperation management space
Tool	Nice-to-have	Future	Refining pre-selection of cooperation tool
Notes	Must-have	This	Transferring result to KS/KP cooperation management space
Responsibility for post-cooperation reflection	Must-have	This	Having a cooperation partner assigned responsible for reflection

Table 2: Data collection and its impact for APOSDLE services within cooperation phase

4.5.1.3 Post-cooperation phase

During the post-cooperation phase data will be collected of all cooperation partners, the knowledge seeker as well as (one or more) knowledgeable persons, and of the cooperation event as summarized in table 3.

Data to be collected	Necessity	Occasion	Reason for data collection
Suitability of tool(s)	Nice-to-have	Future	pre-selecting cooperation tool
Rating cooperation success	Nice-to-have	Future	pre-selecting cooperation tool pre-selecting knowledgeable persons
Rating cooperation support	Nice-to-have	Future	Overall measurement for quality of APOSDLE contextualized cooperation
Rating the expertise of KP	Nice-to-have	Future	pre-selecting knowledgeable persons
Outcome artifact	Must-have	This	Publication in cooperative authoring space
Outcome artifact	Nice-to-have	Future	Could be used as cooperation object

Table 3: Data collection and its impact for APOSDLE services within post-cooperation phase