Development of authentication services for system access

An analysis of the requirements of the users including national specifics and a concept for the rights management and access control component

Prof. Dr.-Ing. Robert Tolksdorf

Dipl.-Inform. Lutz Suhrbier

Dipl.-Inform. Ekaterina Langer

1. Introduction

In this paper we summarize the results of work in objective D1.2 of the project SYNTHESYS from the European Sixth Framework Programme. It reports on an analysis of the requirements of the users including national specifics and a concept for the rights management and access control component.

This document firstly gives an account about our activities during the requirements analysis. For that, we decided to develop a questionnaire and sent it to all partners of the SYNTHESYS project. Thus Chapter 2 comprises the requirement investigation, and the requirements analysis and specification for authentication and rights management components in the context of SYNTHESYS.

Based on the requirements specification, Chapter 4 subsequently describes the concepts for the realisation of the authentication and rights management components and their integration within the present environment. Therefore, relevant XML standards are discussed and necessary functional adaptations of the present BioCASE protocol specifications and the PyWrapper component are elaborated.

Finally, this document closes in Chapter 5 with a discussion of further possible extensions to the authentication and rights management components towards additional security services and the installation of a single-sign-on biodiversity expert portal.

2. Analysis

The number and the distribution of the office locations all over Europe make it impossible to meet all project partners for reasons of time and resource consumption. Thus, we decided to

develop a questionnaire and to send it via email to all partners. The following clauses describe the process leading to the final requirements specification.

2.1. Requirements investigation

The usage of a questionnaire possesses multiple advantages relating to analysis purposes: It saves resources, enables direct comparison of different opinions in single aspects and provides the chance to establish a kind of dialog outlasting the whole development process. Particularly the last aspect appears considerably important for us regarding the further development process of security services. So, the intention behind the forwarding of questionnaires is to integrate as many partners as possible in the discussion process, and to get the necessary information from them to plan or push forward the development process.
Before starting the development process we researched questionnaires developed for similar environments or objectives. Within the scope of the EU funded project “Framework for European Services in Telemedicine” (FEST) [FESWeb], a question set [FEST95] was designed broadly covering all relevant aspects regarding the integration of new components in an existing environment. This question set was taken as a basis for the questionnaire development. It includes some dozen questions grouped in nine logical sections asking them for opinions and suggestions, functional and operational preferences as well as legal, administrative and economical constraints regarding the introduction of those components.
In a first step, all questions were analysed regarding their relevance in relation to IT-security aspects (rights management and access control), the biodiversity context, an overview of the currently established system workflows and generally important environmental information.
We decided to subdivide the questionnaire into two parts. The first part should contain preliminary and general questions, which will become more specialised and refined in further parts when necessary, taking into consideration the responses to the corresponding previous part. The preparation of the questionnaires took place through the completion of the questionnaires on a trial basis by biodiversity experts, several discussions and revisions of equivocal questions taking into account the desired (IT-related) information and the potential knowledge of the probable respondents, consignment of the final revisions to a selected circle of test responders and finally, the evaluation and revision of erroneous or ambiguous questions from the responses returned from the test responders. After these steps, the final versions of the questionnaires were sent via email to all project partners. The provisional final version of the second questionnaire was left open until the termination of the analysis of the first questionnaire, enabling us to refine aspects coming up for discussion.

2.2. Requirements analysis

The final version of the first questionnaire was then sent by email to 93 partners within the projects SYNTHESYS, BioCASE and GBIF-D. The commented results of the responses have been omitted in this report summary and can be viewed within the deliverable D1.2 [ToSL04]. The feedback to both questionnaires is presented in table 1 and table 2.

table 1 Feedback to the first questionnaire

Project	Contacts	Institutions	Responses	% contacts	% institutions
SYNTHESYS	27	19	11	40,74%	57,89%
BioCASE	48	35	17	35,42%	48,57%
GBIF-D	18	16	9	50,00%	56,25%
Total	93	61	37	39,78%	60,66%

table 2 Feedback to the second questionnaire

Project	Contacts	Institutions	Responses	% contacts	% institutions
SYNTHESYS	27	19	5	18,52%	26,32%
BioCASE	48	35	10	20,83%	28,57%
GBIF-D	18	16	6	33,33%	37,50%
Total	93	61	21	22,58%	34,43%

2.2.1. Technical preconditions

The security components to be developed must be adapted around a given software architecture evolved from the prior project BioCASE [DöGü03]. Thereby, unit-level data providers are accessible on the internet via the XML hard-coded BioCASE protocol. This protocol abstracts from the real data to be queried for or transmitted and defines activities or methods understood by a database wrapper or a client application. On the provider domain a CGI/XML database interface written in Python (PyWrapper) enables the connection of an arbitrarily structured database to the BioCASE network. The PyWrapper implements the BioCASE protocol to respond to compatible queries in a standard XML format like ABCD [BABWeb]. On the client side, the Unit Loader is a freely available Java API from the BioCASE developers providing the necessary BioCASE communication protocol functionality to client application developers.
Currently the BioCASE protocol defines the methods search, scan and capabilities. The search method wraps simple SQL SELECT statements into a XML format. Actually, the select part of the statement is static and all matching data for this statement will be returned. The scan method essentially wraps a SELECT DISTINCT SQL statement and lists all unique values of one concept referenced by an XPath expression to the respective concept schema. The capabilities method allows a client to get information about the defined concepts mapped in a provider's database.

2.3. Requirements specification

The analysis of the responses to both questionnaires goes beyond the scope of this paper. Thus, the following sections will sum up the results of the conclusions of the analysis in the form of a short requirements specification.
The activities of the respondent project members are spanning a broad and diversified spectrum of tasks and capabilities. So, the variety of internal and external data flows does not correspond to a more or less common scheme, hence disallowing the implementation of commonly known solutions.
From the functional point of view the most wanted features are the allocation of access rights and access control mechanisms. A relatively high demand also exists for the ownership attribution and data integrity during the transmission of documents. Further requested is the saving of the confidentiality of (partial) sensitive data (e.g. localisation of endangered species) and topics regarding intellectual property rights of documents.
From the organisational point of view the implementation of a hierarchical rights management and access control architecture is necessary, where the final determination of valid access rights policies remains in the hands of every institution. Nevertheless, every institution must be enabled to inherit policies from higher hierarchical levels (e.g. regional, national or project wide nodes) and thus, add them to their local access rights decision process. An open and probably political question concerns organisational aspects regarding the assignment of responsibilities for the definition and distribution of corresponding high-level policies and also for the maintenance of a project wide user and/or provider certification authority. The installation of one or more certification authorities, to build up a Public Key Infrastructure, will be mandatory regarding the implementation of access control and authenticity mechanisms.

From the technical point of view the implementation should leave the given software architecture untouched as much as possible. So nobody should be burdened to take on unwanted tasks or responsibilities potentially going beyond organisational capabilities. Further aspects concern the often lower IT knowledge of the operators and users of the provider software and client applications to be expected. For these reasons, the installation, configuration and maintenance processes should be kept as simple as possible and should be integrated into the installation process of the provider software as much as possible. Thus, the rights management and access control components should provide predefined access rights and rules as well as roles and user groups. Configuration and maintenance purposes should be supported by easy to use administration tools.
From the legal point of view the European data protection and telecommunication acts have to be respected. Through the necessary usage of a PKI, also the European Directive for digital signatures [ECSI99] has to be respected. The responses of the questionnaires include special university guidelines and new laws concerning collections in general (Switzerland, France). This requires the implementation of hierarchical policy structures allowing the definition and inheritance of national specifics into the local decision process. These requirements have been covered and elucidated within the organisational requirements formulated above.
From the economic point of view the results reflect that in general no more than 5% to 10% of available funds could be expected for the development, installation and maintenance of security services. This means that the application of license free and even better open source software components is mandatory to save costs and allow future adaptations of software components. Therefore, it has to be considered that the more complex the security service wished, the greater the effort that will be required for the establishment and maintenance of needed structures, e.g. legal constraints such as the requirement for security equipment like chip cards and readers or regular expenses such as certification authorities issuing valid certificates.

3. Evaluation of relevant XML standards

Regarding the project's requirements, the following standards have been evaluated and are described: XACML, SAML, XML Signature, XML Encryption, XKMS, and XrML.
XACML (eXtensible Access Control Markup Language) [OAXWeb] is an OASIS standard specifying XML based languages for the definition of policies and access control decision requests and responses. The policy language describes general access control requirements and provides extension points to define new functions, data types or combining logic. Policies allow defining rules specifying who may execute what kind of action on which resource.
The access control decision protocol allows the description of queries concerning the permission to execute a specific action. The result of such query will be generated based on the defined policies and may have one of the values permit, deny, indeterminate (decision cannot be made), and not applicable (request cannot be answered). Such a request is directed to any system component responsible to protect any system resources (Policy Enforcement Point, PEP). Based on the attributes of the inquiring partner, the PEP formulates a request addressing the desired action, resource and further information. Then the PEP directs this request to the Policy Decision Point (PDP), which analyses the request, investigates based on the defined policies if the demanded access will be allowed and retransmits the result back to the PEP. The PEP then responds to whether the access will be permitted or not. Both PEP and PDP may cooperate in single applications as well as be distributed over different servers. The only known freely available standard implementation is from SUN and comprises an Open Software Java API based on the mandatory features of the XACML standard version 1.1 [SUXWeb].
SAML (Security Assertion Markup Language) [OASWeb] is an OASIS standard defining a framework for the exchange of security information between online communication partners.

The purposes are the creation and exchange of authentication and authorisation information. This is mainly achieved by the approach to exchange trustworthy assertions about a subject within a network. To realise that, SAML introduces the concepts asserting party and relying party. The asserting party could be represented by a system or administrative domain, which asserts information about a subject. They are also called SAML Authorities. The relying party is a system or administrative domain relying on information offered by an asserting party. It is the task of the relying party to trust the offered information or not. For that, SAML provides a couple of algorithms enabling the relying party to determine her level of trust. Even if the relying party trusts the provided information, in the end local access policies will decide on the access to local system resources. Actually, the most important use case for SAML consists in the solution of the single-sign-on problem in the web. So, SAML will be very suitable regarding the implementation of web portal systems. Profiles describe the SAML information flows for particular purposes, derive from use cases. Version 2.0 of SAML will contain a profile for the usage of XACML within SAML protocol messages. The OpenSAML project [IOSWeb] provides open source libraries in Java and C++ for creating, transporting and parsing SAML messages.

To ensure the secure exchange of XML data the World Wide Web Consortium (W3C) [W3CWeb] has defined the specifications XML Signature [BBF+02] and XML Encryption [IDS02] to provide digital signature and encryption within the XML context. Apache provides with its XML Security library [ASFWeb] a free open source Java implementation of the XML Encryption and XML Digital Signature specifications.

XML Encryption specifies the process of data encryption and its representation within XML. It provides selective encryption which allows the selection of several parts of a XML document for encryption, so that each part may be readable by one or more specific subjects. Selective encryption is also useful to ensure end-to-end security in a communication path where many intermediaries should only be able to read parts of a message. XML Encryption has the capability to encrypt arbitrary binary data, whole XML documents, elements or element content [Dour02].

XML Signature is the W3C specification for digitally signing XML documents. It has the advantage to allow the signing of specific parts of a XML document. These parts could be signed by multiple signers or several parts could be signed with one signature. Conventional Digital Signature standards do not provide this fine grained signing. Finally XML Signature offers the methods enveloping signature, enveloped signature and detached signature to provide the signature along with a document. An enveloping signature contains the signed data as a sub element, an enveloped signature as a child element of the signed document and a detached signature separates the signature from the signed data.

XKMS (XML Key Management Specification) [HALL04] defines protocols for public key management services. It supports sharing public keys needed for signature verification or decryption of a message. The key management and trust issues are solved traditionally by using digital certificates, specialized protocols and PKI services (Public Key Infrastructure). The disadvantage of these technologies is that the verifier of a signature has to support operations like validation of the certificate chain, certificate revocation checking and policy mapping. XKMS defines the protocols XML Key Registration Service Specification (XKRSS) and the XML Key Information Service Specification (XKISS) to obtain public keys and trust assertions, including key registration, revocation and updates. In this way the key management issues and the complex certification path validation processing are shifted from the client application to the trusted server. Due to the diversity the clients in SYNTHESYS and the need to keep the applications as simple as possible, the use of a XKMS system would be a suitable choice. But, actually no freely available implementation of this standard exists. The Apache XML Project aims to include XKMS in a future release of its XML Security library.

The eXtensible rights Markup Language (XrML) [XRMWeb] is a XML-based specification language for expressing rights and conditions associated with digital content, service or any digital resource. Using XrML, the owner of a digital resource can identify who is allowed to access it how and under which conditions. XrML is contributed to the international standard community OASIS. In the project's context XrML could be used to enforce the compliance with the Intellectual Property Rights (IRP) of the published biodiversity data. Currently, an open source implementation of XrML is unknown. ContentGuard provides a MPEG related Java SDK for non commercial use [CGXWeb].

4. Concept

The second task to perform within this report is the presentation of a concept for the rights management and access control component. Because the existing software architecture is based on XML, it is a natural progression to build up the security components on security related XML standards also. Based on the evaluation of relevant XML security standards in chapter 3, the following clauses describe concepts for rights management and access control. Finally, the integration into the present BioCASE architecture and necessary adaptations to support this process will be outlined.

4.1. Concept for rights management

Due to the need for a very flexible architecture to define, manage and enforce policies, the concept for rights management is founded upon the properties of the XACML standard. Therefore, the rights management functionality will be realised from the XACML components PEP and PDP, which will have to be integrated into the present provider scenario. Every request will be processed from the PEP first, which delegates the final decision process to its related PDP. Dependent on the PDP decision, the PEP rejects, permits or constrains access to the requested resources. Through the definition of corresponding rules, access right policies will be defined describing to whom (e.g. user or role) will be granted what kind of access (e.g. read, write) to which data elements (resources). Resources are expressed using XPath statements within the BioCASE protocol requests.
To meet the requirements specified in the requirements specification the XACML mechanisms to include multiple policies into the decision process of the provider's PDP will be used. Thereby, the policies to be included may also reside on locations internal or external to the system boundaries of the current PDP (e.g. on an intranet or Internet server). Thus, the underlying policies of the access right decision process may be updated at every decision request from the corresponding server or regularly e.g. by importing and integrating policy configuration files into the local provider software configuration (or caching of requests for performance reasons).
In a further step, the linking process between the provider's PDP and other nodes could be realised introducing SAML authorities, performing policy services accessible via standard SAML requests implementing the SAML Profile defined within XACML V2.0 [ANLO04]. The benefit of this approach is in its combination with access control components restricting policy access e.g. to specific providers. So, provider specific policies could be prepared e.g. from higher-level nodes on behalf of "security or IT aware" providers. On the other side national nodes could take over policy maintenance e.g. to incorporate national (e.g. legal) specifics into national-wide policies. Assuming a linked configuration beside the providers, these policies would be automatically included in the policy decision process of their PDPs (see figure 1).

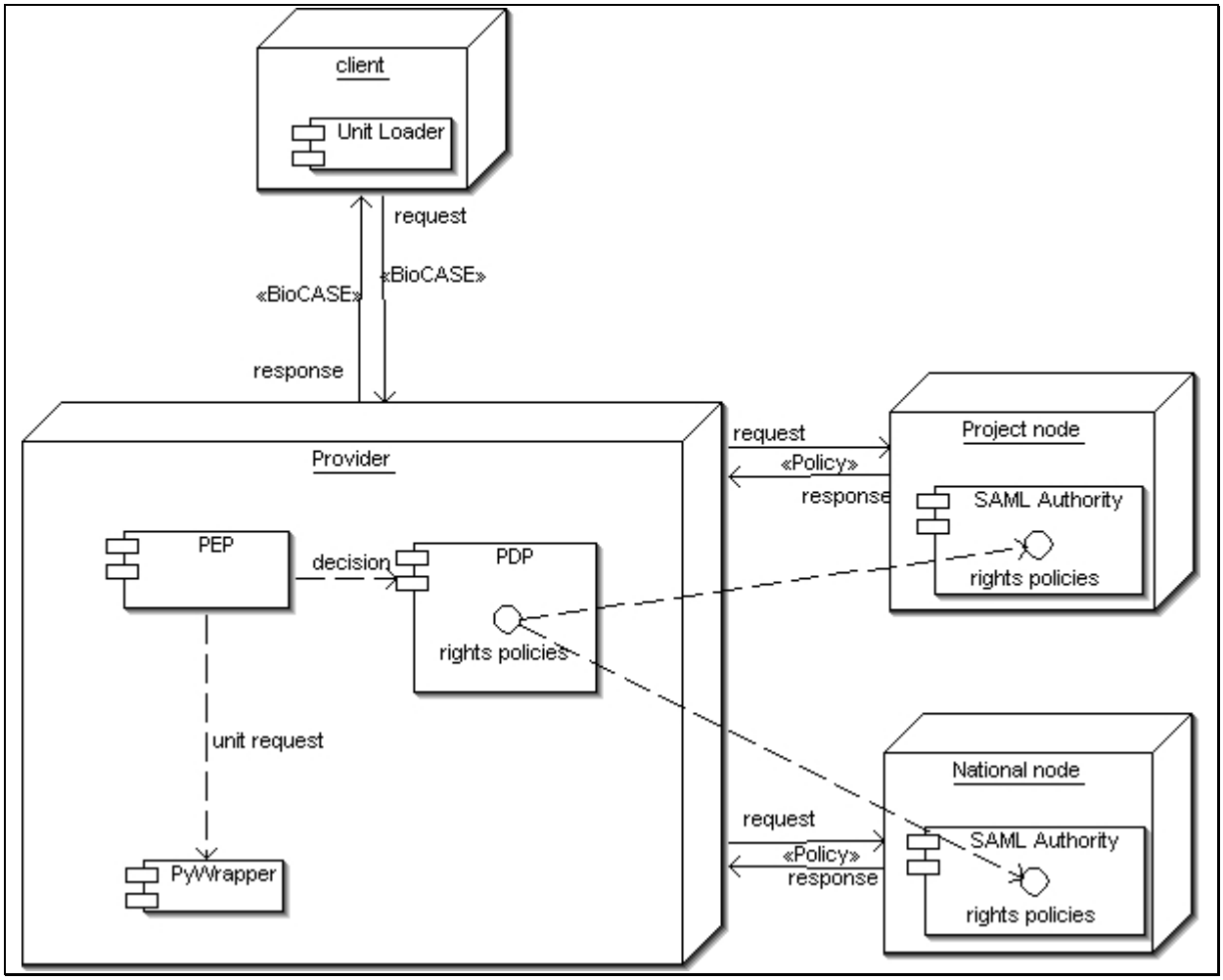

figure 1 Access right management concept

4.2. Concept for Access Control

The XACML standard is also suitable for the implementation of a role based access control component into the present scenario. The main objective of an access control component is the surveillance of the compliance with the specified access right policies defined within the access rights management component for a given subject. This comprises the authentication of the related subject demanding for access, the assignment of roles to the identified subject and execution of access rights decision processes.

Regarding the assignment of subjects to specific roles and vice versa, version 2.0 of the XACML standard provides a role based access profile allowing the specification of roles and their mapping to the related policies [ANDE04]. Concepts about the mapping between users and roles are also covered within this profile. The definition of the subject/role-mapping takes place within the access control policies. Due to the usage of the same XACML based system architecture as within the rights management concept, the same mechanisms become usable for the (hierarchical) distribution of correspondent access control policies. So, e.g. a national node may prepare access control policies automatically included in the decision process through the mapping of roles and thus, access rights to specific subjects or user groups.

The analysis of the questionnaires has offered highly diversified understandings regarding the interpretation of roles. So, only a few roles will be implemented first, serving for the derivation of similar roles and access control policies later. In the case of an incoming request from an unauthenticated subject, the access control policy assigns him the role of an anonymous guest. This represents the role with the minimum access rights allowing only access to publicly available data sets or information. This behaviour would then comply with

the present access control situation of the system. Any request from a known subject (guest, normal user) will be assigned the client role. This role allows the subject access to resources available for registered users within the network. The expert role will only be assigned to known subjects with the expert attribute set. This role includes access to sensitive information also.
The authentication process reflects the identification of a given subject (e.g. user or client system). The authentication has to be done before any subjects may send requests to the PyWrapper component. For that, the PEP will be extended by an authentication (commonly called login) component responsible for the correct identification of requesting subjects (see figure 2).

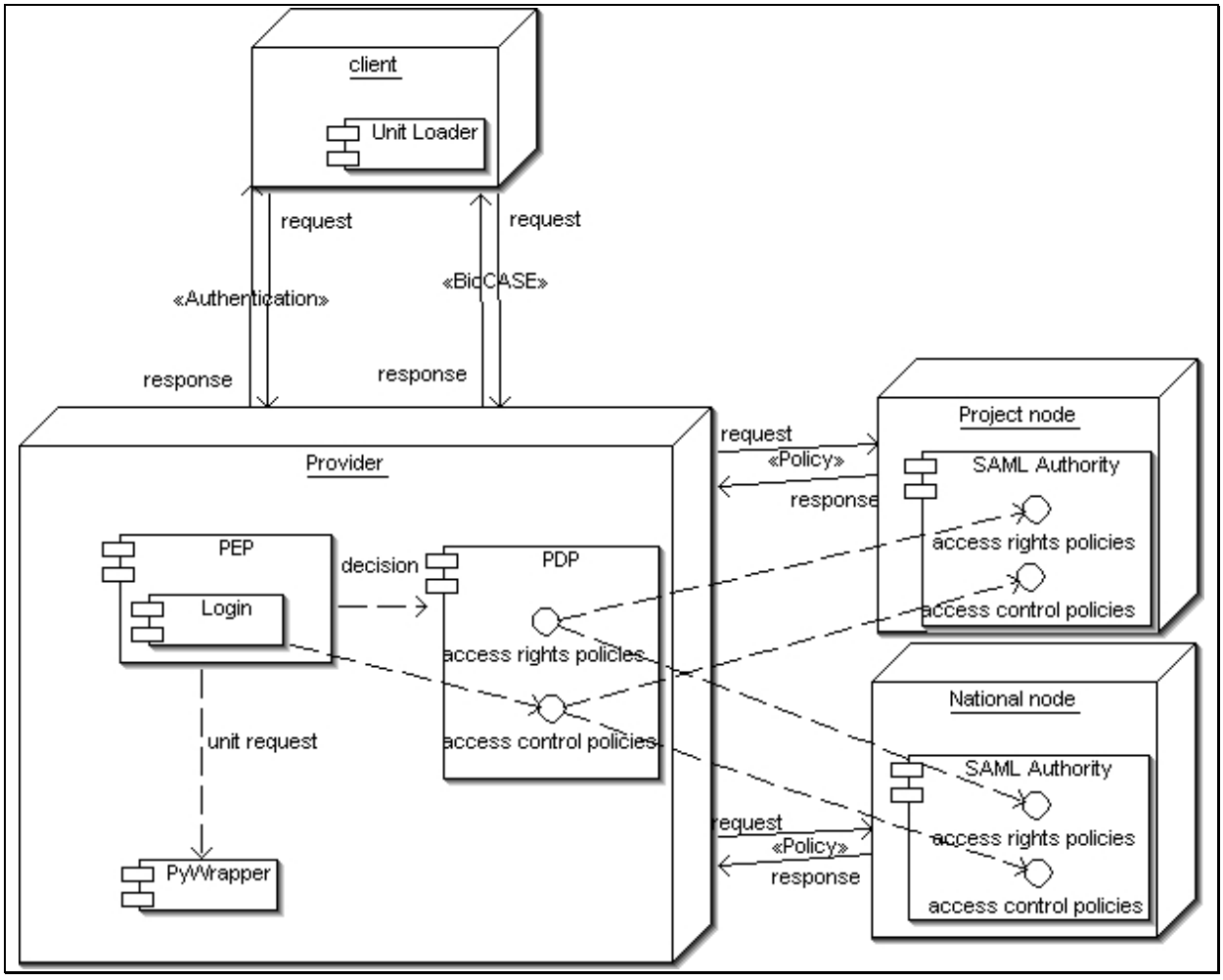

figure 2 Access control management concept

The login process may be based on a Password or Public Key Infrastructure (PKI). This concept plans to integrate both methods into a common login component. For that, the PEP functionality will be integrated into a SSL [DIAL99] based access service realising authentication using the commonly known SSL handshake process. The SSL server authentication mode will be used to transmit user and password information securely, whereas the bi-directional authentication serves to authenticate clients to a PKI based login component. The credentials of the subjects to be authenticated (passwords, certificates) will be stored within the provider's access control policies and thus included in the access control decision process of its PDP.
The integration of SAML authorities into the login process would pave the way for a project wide single-sign-on solution. Through the usage of SAML authentication requests, the provider's PDP will be enabled to demand other trusted providers or higher level nodes in the

project context to prove the authentication state for a given subject. This concept requires the implementation of a correspondent PKI, because the received assertions must be verified before they could then be included into the access control decision process of the provider's login component.

4.3. BioCASE Integration

To integrate the rights and access control management components into the present project scenario, the PyWrapper will logically be relocated behind a XACML Policy Enforcement Point (PEP). The PEP deduces from the decision of its related Policy Decision Point (PDP) if it has to reject the request or to permit some kind of access to the requested resource. The permission to access a resource may be granted completely or partially. In the first case, the request will be transmitted completely to the PyWrapper component. In the latter case the request will be modified by the PEP so that the XPath expression only describes these parts of the resource to which access can be granted. Then, the PEP redirects the request to the PyWrapper, which processes the transmitted request and generates the corresponding response, an ABCD document [BABWeb] or an error message. The response will be received from the PEP, possibly further processed and finally delivered to the requesting client.
Notice that for the previously drafted scenario, some adaptations to the present BioCASE protocol and software architecture [DöGü03] will be necessary.
The BioCASE Protocol will need adaptations concerning the scanning of security capabilities and the request format extension regarding a subject authentication identifier. To indicate the security capabilities of a provider implementation to requesting clients and to provide possible future negotiations about the security context to be used, the possible responses to the BioCASE protocol request method "Capabilities" should be extended by a placeholder reserved for security properties, simply named "Security". When the provider implementation also comprises security services, then the access control component will transmit any capabilities requests to the PyWrapper, enrich its response with the available security attributes and finally retransmit it to the requesting client.
After a successful login process, the authenticated subject should be able to send further BioCASE requests without the need to send further authentication requests. For that, the request format should be extended with a subject authentication identifier. The client gets this identifier in response to a successful authentication process. To avoid further authentications, this identifier should be included in subsequent BioCASE requests from this client. This identifier could also be used as artefact in the context of an SAML single-sign-on scenario. Thus, the relying XML Schema should provide an optional placeholder security element, whose content will be specified at an appropriate time.
The current PyWrapper implementation of the BioCASE protocol methods search and scan is static and returns all matching data for the corresponding SQL SELECT statement to the requester. This behaviour must be updated towards a complete XPath evaluation, so that the response document only contains those data elements explicitly expressed by the transmitted XPath search or scan parameter. This is necessary to support modified requests from the PEP described above.
To provide support for these newly introduced security features, the Unit Loader will have to be extended to support the extended security capabilities, the SSL or SAML based authentication protocols and the necessary cryptographic mechanisms (e.g. Key/Certificate and password handling, PKI support) needed to process them.

5. Outlook

The concept presented in the last chapter is geared to the objectives of access control and rights management according to clause D1.2 of the project SYNTHESYS. However the results of the analysis of this report have shown that further enhancements are expected from the security components in the medium-term future like authenticity of data source and data integrity, (partial) confidentiality of documents, copyright protection or a Single-Sign-On expert portal. In consideration of activities of similar projects in that direction (e.g. partial signing and encryption of XML documents in GBIF-D), the integration of these features within SYNTHESYS would make sense.
Also, further security enhancements to the concept presented in this document could be reached through the strengthening of security to a higher level. This could also be done in subsequent steps e.g. through the usage of security tokens (e.g. chip cards) facilitating the application of credentials (e.g. private key) required for a secure processing of authentication protocols. Finally, the following clauses will present a short discussion of some security related aspects deduced from demanded enhancements within the analysed responses.

5.1. Authenticity of data source and confidentiality

Authenticity of the data source represents together with data integrity is an enhancement concerning the data quality of the transmitted information. Using the XML-Signature standard, a provider could digitally sign every document generated from the PyWrapper. The usage of Digital Signature assures the authenticity of the sender and the integrity of the received information to the clients, which could be important for the trust in the submitted data and the image of data provider.
The confidentiality would be realised using encryption technology according to the XML Encryption standard. It could be used to assure that sensitive information, e.g. about protected species, can not be intercepted by hackers and is readable only by the intended recipients.
To realise that, the PEP could be extended by an additional component realising the signing and encryption of documents. The corresponding cryptographic processes would be applied on the response documents received on request to the PyWrapper. The required credentials could be obtained from the same policies also used for the implementation of access control management functionality. The delivered documents would be secured through the related XML Signature and/or XML Encryption formats. Necessary adaptations to the formerly presented access control concept outlines figure 3.
To support these security features on the client side, the Unit Loader or other client software must be updated and should additionally provide a user interface supporting the new security functionality. Presuming a robust implementation of current client applications, these client applications should be usable as before by simply ignoring the unknown XML Signature or Encryption data elements.
Other future extensions could make use of the features of multiple and partial encryption and signing of documents. The benefits are that sensitive and non-sensitive information could be mixed within one document, where the protection of the sensitive elements of a document would be guaranteed through the usage of partial encryption, i.e. only accessible to specific subjects.
However, the implementation of these features requires a very careful analysis of their influence on the current data formats and applications. The development and integration of these security features to the biodiversity network are objectives of our further work.

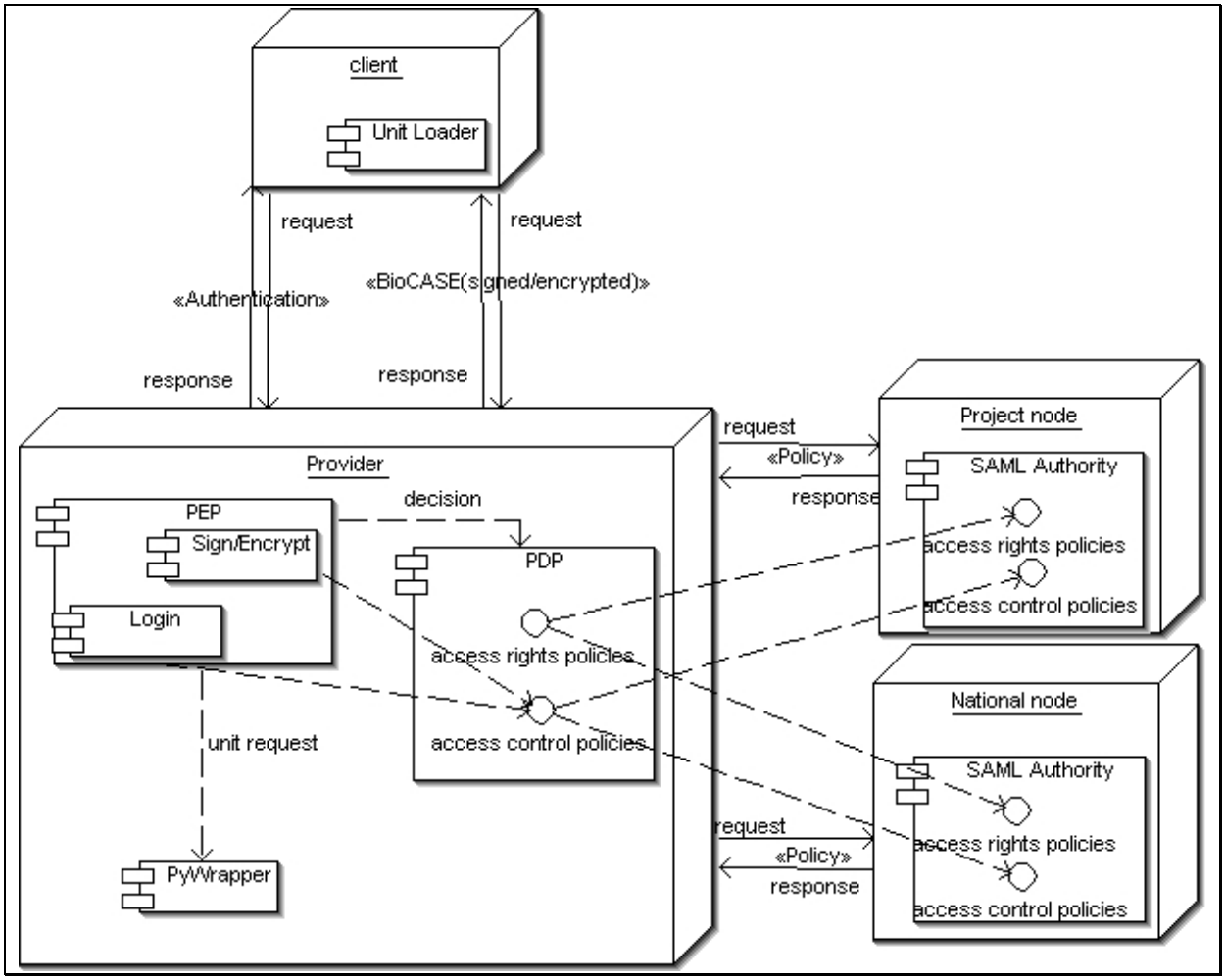

figure 3 Possible extension towards data source authenticity and confidentiality

5.2. Copyright protection

The realisation of the copyright requirements may prove problematic, taking into account the present discussion surrounding digital media copyrights. Using the features of the XML-Signature standard regarding partial document signing e.g. the marking of copyright information for every data element in a document would become feasible. But it fails, when protection against unlicensed dissemination of this document is required. Even if there is an existing XML standard dealing with this problem (XrML), the available API from ContentGuard supports only the marking of copyright issues. Furthermore, there is not any known working system implementation.

The actual discussions and first products concerning media based solutions for e.g. music or videos are calling for the usage of special hardware components or proprietary software "players". Thus, further developments in this area should be observed before making any further considerations about this issue.

5.3. Single-Sign-on biodiversity expert portal

As stated in chapter 3, to pave the way for a biodiversity portal system basing on the drafted concept within this report, the functionality of the login component within the PEP must be updated to support the required functionality of a SAML authority beside the providers. Once authenticated, the client would be able to request any information without the need for further explicit logins, switching from one connected provider to another.

5.4. Acknowledgements

This work was in part supported by the EU's Sixth Framework Programme and the German Federal Ministry of Education and Research (BMBF) in the projects SYNTHESYS and GBIF-D.
More information can be found at http://nbi.inf.fu-berlin.de/research/SYNTHESYS.

6. References

[ANDE04] Anne Anderson: OASIS Core and Hierarchical Role Based Access Control (RBAC) profile of XACML, Version 2.0; Committee Draft 01, 30 September 2004.

[ANLO04] Anne Anderson, Hal Lockhart: OASIS SAML 2.0 profile of XACML Committee Draft V2.0, 16 September 2004.

[ASFWeb] The Apache Software Foundation: Apache XML Security; http://xml.apache.org/security/Java/index.html, last seen 15 October 2004.

[BABWeb] Walter Berendsohn: ABCD Schema - Task Group on Access to Biological Collection Data; http://www.bgbm.org/TDWG/CODATA/Schema/default.htm, last seen 15 October 2004.

[BBF+02] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon: XML Signature Syntax and Processing; W3C Recommendation, 12 February 2002.

[BioWeb] BioCASE Secretariat: A Biological Collection Access Service for Europe; http://www.biocase.org, last seen 15 October 2004.

[CGXWeb] Content Guard: XrML 2.0 Specification; http://www.xrml.org/XrMLSpecChooseUser.asp; last seen 15 October 2004.

[DIAL99] T. Dierks, C. Allen: The TLS Protocol Version 1.0; Network Working Group Request for Comments: 2246, January 1999.

[Djaj02a] Ray Djajadinata: Yes, You Can Secure Your Web Services Documents, Part 1; http://www.javaworld.com/javaworld/jw-08-2002/jw-0823-securexml.html, 23 August 2002, last seen 15 October 2004.

[Djaj02b] Ray Djajadinata: Yes, You Can Secure Your Web Services Documents, Part 2; http://www.javaworld.com/javaworld/jw-10-2002/jw-1011-securexml.html?, 11 October 2002, last seen 15 October 2004.

[DöGü03] Döring, M. & Güntsch, A. 2003: Technical introduction to the BioCASE software modules. 19th annual meeting of the Taxonomic Databases Working Group (TDWG 2003), Oeiras, Lisbon 2003.

[Dour02] Blake Dournaee: XML Security; ISBN 0-07-219399-9, McGraw-Hill, 2002.

[ECSI99] Official Journal of the European Communities: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Community framework for electronic signatures, 13 December 1999.

[FEST95] FEST Consortium (A 2011); FEST Guide Appendix A: The Question Set; ftp://ftp.cs.tu-berlin.de/pub/local/kit/documents/KIT-Reports/r123/FG-AA.fm.ps, March 1995, last seen 15 October 2004.

[FESWeb] FEST Consortium: The FEST project; http://www.cee.hw.ac.uk/Databases/lachs/fest.html, last seen 15 October 2004.

[HALL04] Phillip Hallam-Baker: XML Key Management Specification (XKMS 2.0) Version 2.0; W3C Candidate Recommendation, 5 April 2004.

[Hirs02] Frederick Hirsch: Getting Started With XML Security http://www.fjhirsch.com/xml/xmlsec/starting-xml-security.html, 2002, last seen 15 October 2004.

[IDS02] Takeshi Imamura, Blair Dillaway, Ed Simon: XML Encryption Syntax and Processing; W3C Recommendation, 10 December 2002.

[IOSWeb] Internet2: OpenSAML 1.0 - an Open Source Security Assertion Markup Language implementation: http://www.opensaml.org, last seen 15 October 2004.

[OASWeb] OASIS: OASIS Security Services TC: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, last seen 15 October 2004.

[OAXWeb] OASIS: eXtensible Access Control Markup Language TC; http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, last seen 15 October 2004.

[OBWeb] Susanne Oehlschlaeger, Walter Berendsohn: GBIF-Deutschland; http://www.gbif.de, last seen 15 October 2004.

[SUXWeb] SUN Microsystems Inc.: Sun's XACML Implementation; http://sunxacml.sourceforge.net/, last seen 15 October 2004.

[SYNWeb] SYNTHESYS project: http://www.synthesys.info, last seen 15 October 2004.

[W3CWeb] W3C: World Wide Web Consortium (W3C); http://www.w3.org, last seen 15 October 2004.

[XRMWeb] Content Guard: XrML 2.0 Specification; http://www.xrml.org/XrMLSpecChooseUser.asp; last seen 15 October 2004.

[ToSL04] Robert Tolksdorf, Lutz Suhrbier, Ekaterina Langer: Develop authentication services for system access; SYNTHESYS Deliverable D1.2 Report; Berlin, 31 July 2004.