A DISTRIBUTED ARCHITECTURE FOR THE MANAGEMENT OF DATA FLOWS WITHIN THE BOLOGNA PROCESS USING EGOVERNMENT STANDARDS

Hermann Strack[1], Christoph Karich[1]
[1]Hochschule Harz, University of Applied Sciences, Friedrichstr. 57-59, D-38855 Wernigerode, Germany
hstrack@hs-harz.de
ckarich@hs-harz.de

Published in: Yves Epelboin et.al. (ed.): Proceedings of EUNIS 2007, Grenoble Univ., 2007

Abstract

The introduction and implementation of bachelor/master study programs within the Bologna Process Framework in Europe will need the exchange of transcripts of records of students (TOR) and the management of administrative data for student mobility (MOST) between universities in Europe. Obviously these exchanges of data could be done more efficiently and securely via (standardized) electronic communication services than within the "plain old paper world (POPW)". Even, in the future, for the support of huge numbers of data exchanges and/or of participating universities, it would be necessary to use (secure) electronic services only, to process the data in time and to validate the authenticity of transcript of records data.

We propose a security architecture framework and a prototype implementation to process TOR and MOST data in an efficient and secure manner, based on internet and/or eGovernment standards, open for connections to different local campus management systems of universities. At first, according to the Bologna Process Framework, we propose a XML based format (scheme) for an electronic TOR (eTOR), which can be signed electronically by universities in a secure and legally accepted manner within the EU. At second, we propose a distributed (security) architecture for secure exchange of eTOR between universities within EU, which is based on internet standards, like SOAP and Web Service Security, and/or eGovernment standards like OSCI (Online Services Computer Interface), in an open manner.

As an example, we present typical functionality and security features of a prototype architecture based on SOAP and/or OSCI. Using OSCI or other eGovernment standards would offer the opportunity for universities to use eGovernment synergies and frameworks at low costs.

The Bologna Process

To establish the European higher education area (EHEA) within the so called Bologna process, the participating countries set mutual goals concerning restructuring universities, study courses and academic degrees [1,2,3]. Especially the introduction of international compatible, tiered study programs and academic degrees (bachelor/master), the modularizing of those study programs combined with an improved international acceptance of exams- and study-achievements considering module specific work load of students by introduction of the ECTS-credit point system and thus improving international mobility of students as well as of instructors. Furthermore an improved international transparency and compatibility of

academic degrees is achieved by issuing a so called “diploma supplement” in addition to the diploma certificate of the national university.

Concerning the administration of the implementation of the Bologna Process we summarize in short some instruments of the administration of the Bologna Process:

- *Modularization of study programs* including the introduction of a credit point system compatible to ECTS, specifying for each module of the study program the specific work load of the student during studying this particular module.

- *ECTS*: by introducing the European Credit Transfer System (ECTS), the extent of work load of the student, which is required to study the respective module successfully, can be specified in examination certificates. Additionally, the ECTS Grade points out, how the examination grade of the student can be classified relatively within his class – independent from the national grading system.

- *Acceptance of examination results of study programs and support for the mobility of students*: students and alumni are given an improved international acceptance of their achievements in exams and study programs from abroad studies.

The exchange of external examination results from abroad studies are currently handled using paper forms e.g., a form for the transcript of records (here in short: “TOR”), which is signed manually and stamped by the appropriate departments of the guest university (abroad). An exemplary form for the exchange of transcripts of records (TOR) is shown in figure 1. Main problems of this paper based transfers of TOR between universities are the inefficiency of the data handling and the insecurity of the data exchanges. Especially, TOR transfers across EU member states borders could be suffering by threats and frauds concerning the authenticity and the integrity of the exchanged data. Therefore, universities in the EU cannot rely in a trustworthy manner on such paper forms for TOR exchanges. Even, an European register service for the validation of university signs, stamps and seals does not exist.

Regarding administrative and data management aspects, sufficient methods for the secure exchange of examination results, TOR and study achievements as well as of academic degree certificates (testamurs) are of substantial interest. This paper will present an approach for the secured and legally binding exchange of such data (like TOR) between European universities.

ECTS - EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM

TRANSCRIPT OF RECORDS

NAME OF SENDING INSTITUTION: .....
Faculty/Department of .....
ECTS departmental coordinator: .....
Tel.: ..... Fax: ..... e-mail: .....

NAME OF STUDENT: ..... First name: .....
Date and place of birth: ..... (sex) :.....
Matriculation date: ..... Matriculation number: .....

NAME OF RECEIVING INSTITUTION: .....
Faculty/Department of .....
ECTS departmental coordinator: .....
Tel.: ..... Fax: ..... e-mail: .....

Course Unit code (1)	Title of the course unit	Duration of course unit (2)	Local grade (3)	ECTS grade (4)	ECTS credits (5)
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
					Total:
	to be continued on a separate sheet				.....

(1) (2) (3) (4) (5) see explanation on back page

Diploma/degree awarded:
.....

Date Signature of registrar/dean/administration officer Stamp of institution:

Fig. 1: ECTS-form, resp. transcript of records (TOR) for European Universities [4]

The Bologna process workflow

Usually, the two involved universities – the home university, where the student is regularly matriculated, and the host university, where the student will go for studying of modules abroad – are signing in advance an student specific exchange-contract before in order to agree on terms of the acceptance of the students course programs and examinations performance thereof.

After a successful nomination and matriculation of the student at the host university the respective student will go abroad to the host university to attend the appropriate courses and to pass the appropriate exams, hopefully. The results of the examinations are then compiled within the transcript of records specifying the particular students data - e.g., name, date of birth, etc. - the data of the universities (home university as well as host university), and the courses, which the student attended at the host university, together with the study achievements according to the Bologna process framework (the local/national grades, the

earned ECTS credit points, and the ECTS grades). Then, this transcript of records will be manually signed and stamped by the appropriate departments, e.g. this will be done by the dean of the faculty and/or the particular ECTS coordinator and/or the department for foreign affairs (the particular departments or roles may differ between different universities – especially between universities in different EU member states).

The TOR paper will be transferred to the student, who then relocates back to the home university handing over the transcript of records to his home university. The home university checks the TOR-form appropriately and then accepts the students study achievements according to the study-exchange-contract, contracted in advance. Even, if no such contract was closed in advance, the home university will check, if the presented TOR could be accepted according to the home study program of the student.

Figure 2 presents and summarizes the described workflow:

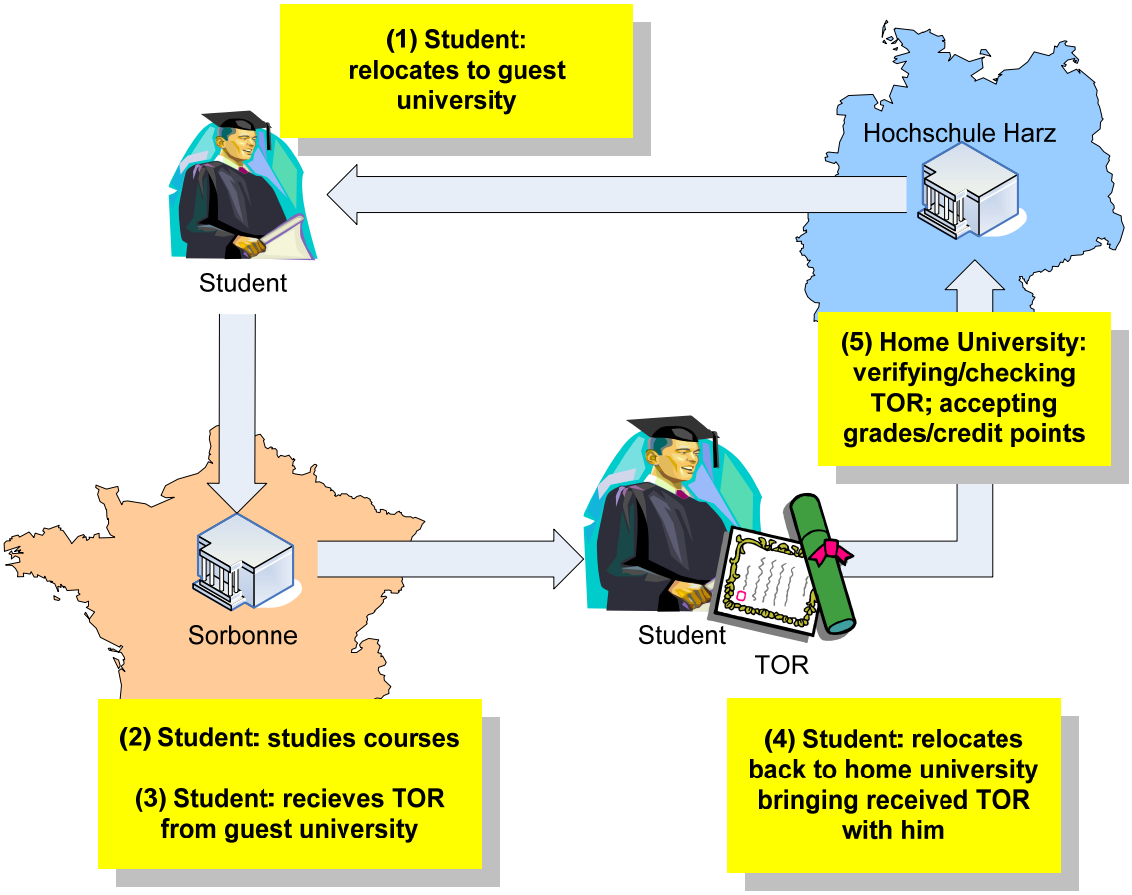

Fig. 2: Bologna process: studying abroad and TOR workflow (originally)

In practice, the workflow execution may be fraught with problems:

- *Inefficiency and media disruptions*: Many of the host universities may use campus management software to compile the transcripts of records (TOR) and to print it on

paper certificates - on this base, the resp. home university will have to rerun the data entry into the own campus management software.

- *Limited authenticity, integrity and trustworthiness of manually transferred documents*: As described above, there exists no overall register or procedures for the validation of European university signs, seals and handwritten signatures. Therefore, the checks of the authenticity of the manually signed and stamped/sealed transcript of records will be of limited trustworthiness and will be suffering from inefficiency, in practice. Even, integrity checking of the TOR documents (paper based documents) may be much more difficult and inefficient, in practice, as generally known.

The eBologna/eTOR approach

While some of the problems of the TOR exchanging workflow within the Bologna process workflow, shown above, could be improved, e.g. by changing the method of the TOR delivery (e.g. by regular mail, instead), however some main problem would remain: the inefficiency, the costs and also still some security problems, concerning the authenticity and the integrity because of the (paper based) documents, because of their vulnerability.

Similar problems are known from administration scenarios within public administrations. To compensate such problems, appropriate designs of fully electronically egovernment workflows with integrated security functions (based on the reuse of egovernment and security infrastructures and standards) were developed in the past, e.g. initially within the MEDIA@Komm pilot project in Germany ([16], mediakomm.difu.de),. Facing the security goals of authenticity and integrity of exchanged data and documents (e.g. for transcript of records) within such a fully electronic workflow, adequate (security) measurements must be taken to fulfill those goals: not only on the data (protection) level, but also on the (security) architecture level, used for the exchange of the data. Furthermore, the legally binding of the data exchange procedures must be fulfilled.

By facing the similarity of the problems and by analyzing experiences from eGovernment projects, the authors of this paper, hereby, propose an approach for the secure, legally binding and electronic exchange of TOR documents within the Bologna Process framework, which is based on the reuse of known security infrastructures, especially public key infrastructures (PKI). In addition, the proposal includes to use as much synergies from established eGovernment infrastructures, as possible.

The XStudy Framework

The development of reusable structured electronic data management procedures and reusable structured electronic data representation, generally, would profit from the reuse of standards like XML and XML based service architectures (goals and experiences from the web service standardization WS, LIT), especially also in this case of management procedures and representations for TOR data .

Therefore, the “XStudy Framework”, based on XML schemata was introduced [5,6,7] as a set of interdependent XML schemata (XML = Extensible Markup Language) describing the process management data for the administration of students within a stuy program, like the study program itself, the student data, the examination certificates, etc.. By figure 3 an overview about the interdependency of these student centric administrative and organizational structures for the XML schemata based representation of a study lifecycle at a university is given.

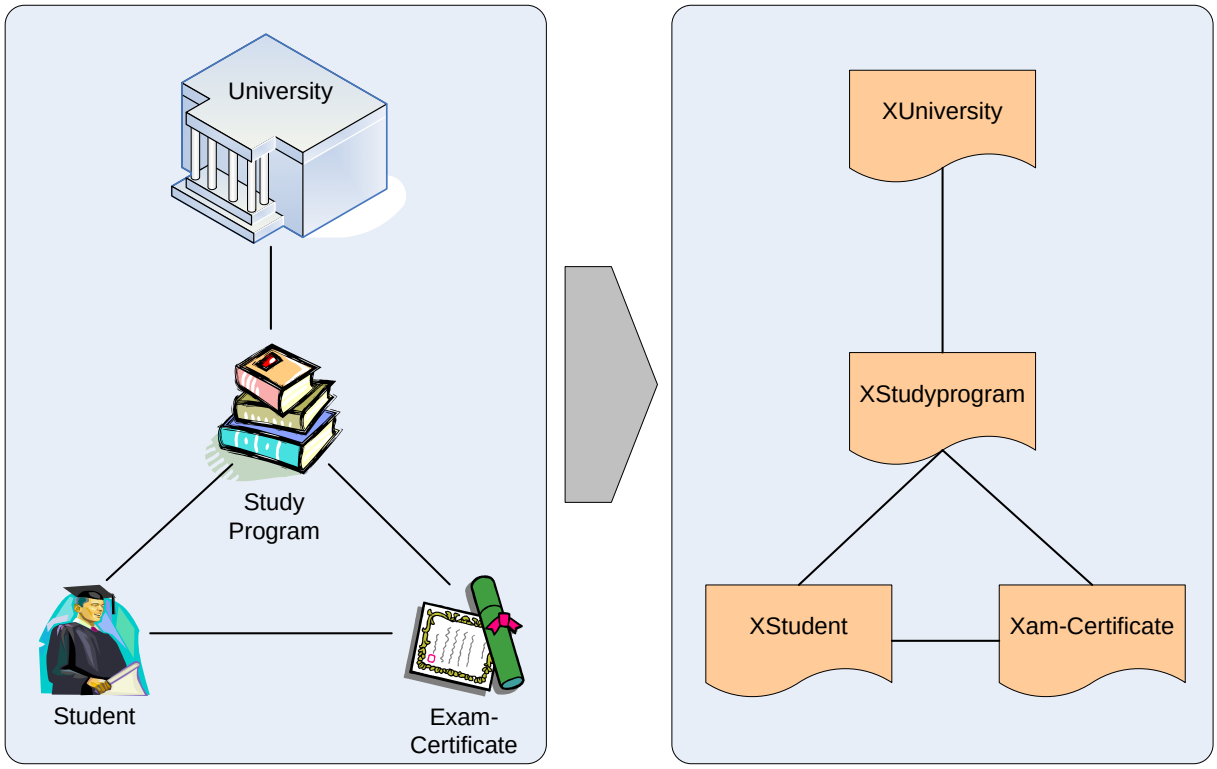

Fig. 3: XStudy Framework

XML technology is used because of its various benefits concerning electronic processing e.g., strongly structured and typed, easy exchangeable, mutual interpretation, allowing standardization, and the possibility to inherit features to new document families. Furthermore, the use of XML technology allows the reuse of various architecture concepts and interfaces e.g., Web Services. The mapping and integration of processes into service oriented architectures (SOA) is possible as well as the integration of various security technologies e.g., of XML-Signatures for applying electronic signatures to support the data authenticity and integrity, or of XML-Encryption to support the data confidentiality and privacy, for some parts of the XML document or for the whole XML document.

While modeling and implementing the XStudy Framework, important synergies from the eGovernment standardization experiences in Germany, namely from the OSCI standardization (Online Services Computer Interface,), could be reused, especially concerning the data representation and the data transfer aspects. OSCI means an eGovernment protocol framework standard in Germany, which is managed by the “OSCI Leitstelle” [9], on behalf of all levels of the public administration in Germany (OSCI Leitstelle, located at the government of Bremen).

Two standardization levels are distinguished: at first, the contendata level - to standardize application specific process data structures by appropiate XML-schemata, established within the German administration (e.g., the XMeld-schemata for the local registration of citiziens in towns, the XJustiz-schemata for the judiciary administration). These application standards are summarized within the family of XÖV standards (XÖV = Standards for the public administration), the so called XÖV Framework [8,10,11]. The framework has been developed aiming at the reusability of generic parts of those known standards when creating new application standards, i.e. to represent the structure of person specific data within other application standards. The integration of the XStudy Framework into the XÖV Framework is still ongoing work.

The second level of OSCI standardization is focused on the level of communication protocols for the transfer of application level data between peers in an public administration scenario, in a secure and legally binding manner, using established communication standards like SOAP and established security standards like XML signature and XML encryption. Using of these integrated standards allows to adapt the coupling of OSCI to a broad variety of application legacy systems. While the international WS standardization efforts focused in a late phase on security aspects, only (WSS, in 2004, [13]), already, during the first steps of OSCI standardization, the security aspects were integrated.

A distributed architecture for eTOR-exchange

Using the described XStudy Framework, documents modeled thereafter and appropriate messages a distributed architecture for TOR exchanges is proposed. This architecture is characterized by the fact that it’s secure, legally binding and enables a fully automated connection of universities and their administrative systems.

This architecture is built upon the German eGovernment standard OSCI, being very similar to a Web Services architecture, but adding security functions onto of it, which are missing in a purely Web Services based environment, even, which are still partially missing in its extension “Web Service Security” (WSS). The proposed architecture is not strictly bound to be used throughout whole Europe, but could be integrated / coupled to other secure national (eGovernment) protocol standards, like PRESTO in France (even with WSS). For achieving the required set of security goals, the architecture and the OSCI infrastructure relies on public key infrastructures (PKI), especially for the building of security functions, like signatures, encryptions, authentications and authorization. To achieve the security goal of being legally binding security components according to the “European Directive on Community framework for electronic signatures” [] have to be used, especially the use of advanced signatures using qualified certificates as well as the use of certified security components like certified signature chip cards and chip card readers is necessary to fulfill the stated security goal.

The OSCI infrastructure was rolled out to a big scale throughout the country in 2006 because the federal German law enabled the exchange of data between administrations regarding registrations of residents electronically (denying any other possibility for the exchange and

thus forbidding paper or floppy disks to be send across the country) ordering the use of OSCI-Transport and OSCI-XMeld as means of transportation and data-representation. This law became effective on 2007/01/01, establishing the fully electronic communication of more than 5.000 registration offices via OSCI, successfully. The authors were also involved in this process of introduction, in an accompanying research project in cooperation with the county of Saxony-Anhalt [15]. The experiences concerning these successful and wide ranging implementation efforts of an OSCI infrastructure all over Germany, fulfilling all necessary security goals stated above, will support the proposal, to use the OSCI standard and infrastructure as an applicable base for an electronic architecture to exchange student data and study achievements, in a fully electronical, secured, and legally binding manner.

OSCI can mainly be described with the model of a twice-enveloped letter: data – structured as XML or unstructured – is signed by the originator (the letter) and encrypted for the recipient (first envelope); the encrypted data is then encrypted again but for a trustworthy third party (second envelope) – the OSCI intermediary; the twice encrypted (enveloped) message is sent to the intermediary decrypting the message and thus getting the still encrypted message for the recipient; the intermediary checks certificates and signatures and records the results of those checks together with date and time of receiving the message from the originator on a process card, which gets signed by the intermediary; the encrypted message for the recipient gets encrypted once again by the intermediary and are delivered then to the recipient together with the process card; the recipient can decrypt both encrypted messages gaining the original data signed by the originator. The process card can be used by all parties to provide proof of delivery (originator can ask the intermediary for respective process cards of sent messages). Figure 4 summarizes this model:

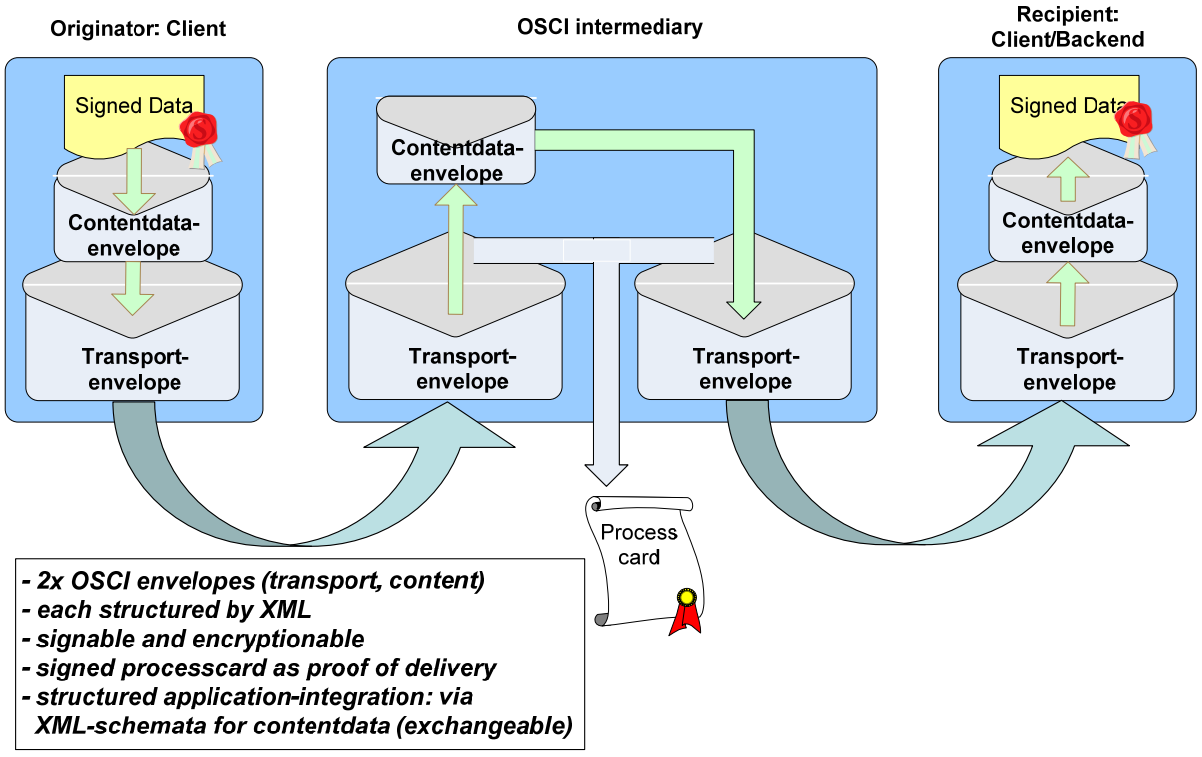

Fig. 4: The OSCI model (Online Services Computer Interface): a twice-enveloped letter

A vital part in the OSCI protocol is the role of the OSCI-intermediary, not only to support a centralized providing of security functions, like verifying of signatures and of certificates, but also to provide a communication platform mediating messages between peers in a reliable and secured manner, without getting the knowledge of the contents of the messages.

Applying the OSCI infrastructure to the process of exchanging student data and study achievements is shown in the following figure:

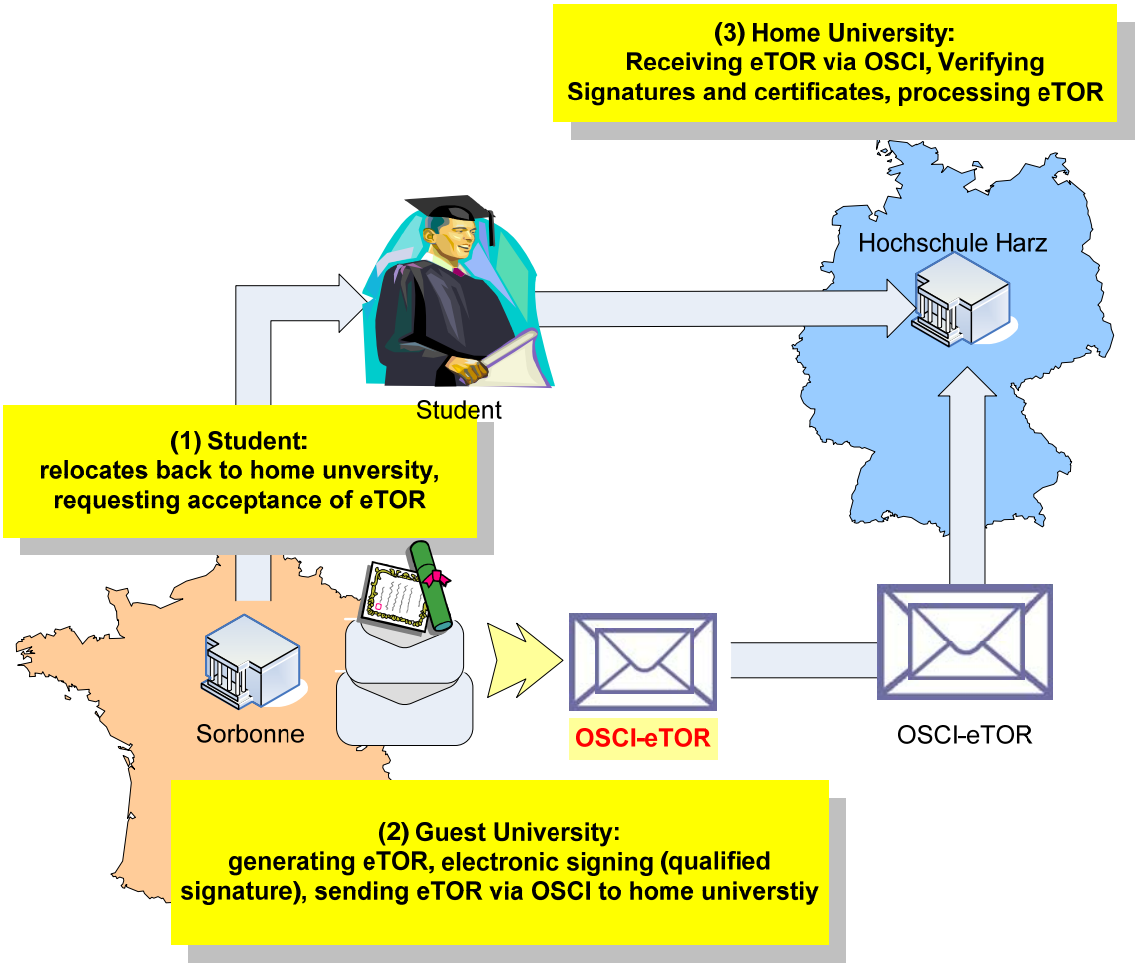

Fig. 5: An architecture for secure and legally binding electronic exchange of study achievements (eTORs) within the Bologna process framework

After studying his courses and modules at the host/guest university the student would just relocate to his home university. The transcript of records would be compiled electronically at the host/guest university as an XML document (eTOR), preferably automated using the university's student administration and organization software system, the appropriate persons/departments would sign this eTOR electronically using advanced electronic signatures relying on qualified certificates and send this signed eTOR to the home university via OSCI.

The respective students' home university would receive the eTOR together with the according OSCI process card signed by the intermediary containing signature and certificate validation results as well as time stamps concerning the delivery. Those validation results would have to be verified by the home university and if positive could process the electronic transcript of records (the XML document) preferably by means of automated data processing e.g., its own student administration and organization software system thus incorporating the exchanged data into its own set of the students' data. The originator (home/guest university) could check for the according process card later at the intermediary and after receiving the signed OSCI process card would hold a proof of delivery concerning the exchanged transcript of records.

This hereby proposed distributed architecture satisfies all set and above stated security goals and would render the exchange of student exam data/transcript of records within the Bologna process very efficient, especially when being used in a fully automated environment involving existing student administration and organization software systems installed in universities.

As stated above the OSCI standard(s) and infrastructure is mainly used within Germany and not yet adopted widely throughout Europe and that's why the here described approach does not strictly couple the data and message format to this infrastructure in order to allow other countries' eGovernment standards and infrastructures to be used. However, since the OSCI infrastructure does not rely on associating an own OSCI intermediary to each involved party (originator/recipient) it would be possible to reuse the already built OSCI infrastructure of Germany in order to implement the electronic exchange of eTORs within Europe for all European universities.

Prototype implementations using this proposed architecture have already been developed by the authors' research team with close cooperation to other partners. Early proof-of-concept prototypes are using already pre-developed, tested and maintained (generic) OSCI client software, which were developed for transporting general data via OSCI (data not bound to a specific application,) making it very easy for a variety of electronic applications to test and use the OSCI infrastructure (Figure 6). Another advantage for using this generic OSCI client is the fact, that it's free of charge in some counties of Germany. Other client implementations, which are seamlessly integratable into office systems, exist in parallel and could be used for the prototypes as well. At the moment, 2nd generation prototypes are being developed using the publically available OSCI application programming interface library (API, being open source) in order to build a specific eTOR/eBologna client, being able to meet the special requirements of the described eTOR exchange process e.g., validating the eTOR-document against the XStudy-Framework-Schemas. Furthermore, cooperation is sought to integrate the Xstudy Framework into campus management software systems, in order to implement a prototype with an increased level of automation.

Ongoing work is a research about the extent of the proposed architecture in order to exchange public school diplomas and certificates, especially, towards universities. The topic of new "electronic public school diplomas and certificates" is of special and increasing interest for universities, because matriculation and assortment procedures in advance of the matriculation,

depend highly on the extraction and grouping of certain grades of the school diplomas / certificates,, being nowadays a very resource consuming (manually driven) process, which can be rendered more efficiently when done in an electronic and automated way.

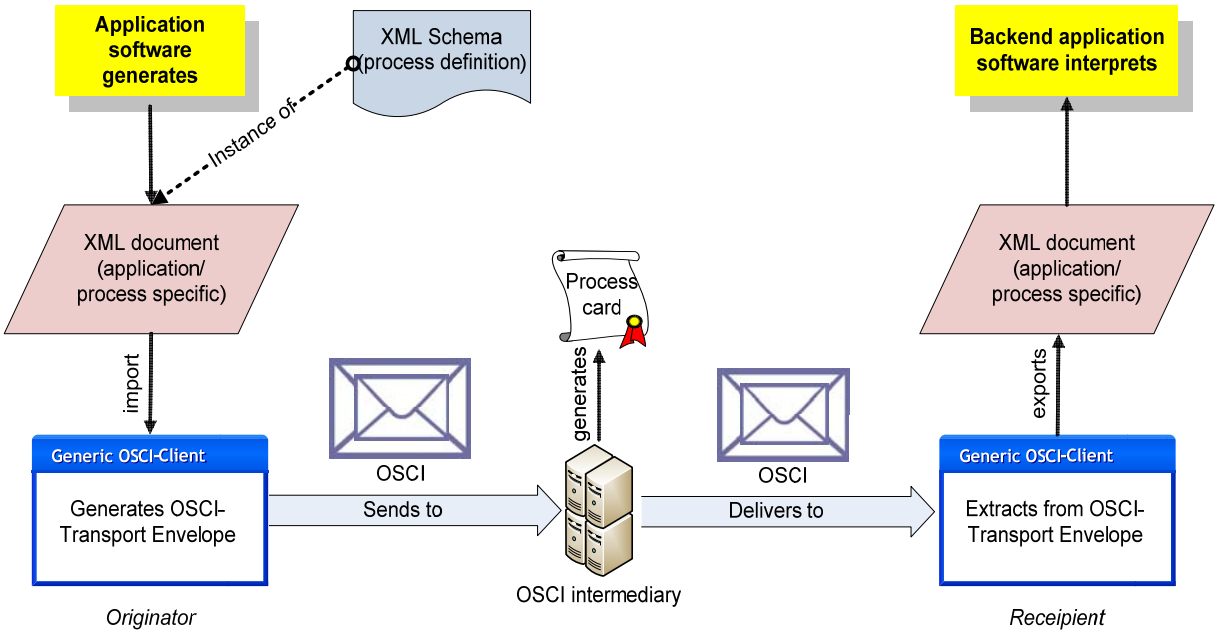

Fig. 6: Generic OSCI based architecture for application integration: exchanging XML-documents via asynchronous OSCI communication

Summary

The shown approach allows by reusing of established eGovernment standards to reach the relevant goals concerning security, legally binding and efficeny for eTOR data exchanges within the Bologna process framework. The approach is open for the adaption to the standardization efforts on secure web services or alternatively to other eGovernment protocol standards, as well as for the coupling to different legacy systems for the purpose of campus management. Therefore, different distributed provider models for eTOR exchanges are possible to be build up throughout the EU: purely OSCI based provider infrastructures as well as infrastructures based on a mix of eGovernment protocols, coupled by appropriate eGovernment protocol gateways.

References

[1] “Joint declaration of the European Ministers of Education convened in Bologna”; The Bologna Declaration of 19 June 1999; Bologna, Italy, June 1999

[2] Confederation of EU Rectors’ Conferences and the Association of European Universities (CRE): “The Bologna Declaration – on the European space for higher education: an explanation”; 2000

[3] European Commission: “European Credit Transfer and Accumulation System (ECTS) – Key Features”; 28 June 2004; online publication, 14 May 2007 (last access), http://ec.europa.eu/education/programmes/socrates/ects/doc/ectskey_en.pdf

[4] European Commission: “ECTS – European Credit Transfer And Accumulation System – Transcript of Records”; online publication, 14 May 2007 (last access), http://ec.europa.eu/education/programmes/socrates/ects/doc/form3.pdf
[5] H. Strack: “Models and an Architecture for secure and legally correct Process Communication for Students and Universities – according to the Bologna Process Infrastructure based on the eGovernment Standard OSCI”; moveon.net European-Workshop, Bologna, Italy, 18/19 January 2007
[6] H. Strack, Ch. Karich, P. Kußmann: “eGovernment und Signaturanwendungen für Hochschulen und Studierende”; 5th XML Signature Workshop, Koblenz, Germany, 11/12 May 2006
[7] Strack, Karich: „Models and an Architecture for secure and legally correct Process Communication for Students and Universities according to the Bologna Process Infrastructure based on the eGovernment Standard OSCI“; eGovernment workshop “eUnibol/eUniversity (Bologna Process)” collocated with “10th IFIP CMS (Internation Federation for Information Processing: Communications and Multimedia Security Conference)”, Heraklion, Crete, Greece, 19/21 October 2006
[8] OSCI Leitstelle: “OSCI Transport 1.2 – Specification – Final”; Bremen, Germany; June 2002; online publication, http://www1.osci.de/sixcms/media.php/13/osci-specification_1_2_english.pdf
[9] OSCI Leitstelle: “Homepage”; 14 May 2007 (last access), http://www.osci.de
[10] OSCI Leitstelle: “Projektauftrag OSCI-XÖV”; 19 December 2005; online publication, http://www1.osci.de/sixcms/media.php/13/2005-12-19_Projektauftrag%20XOEV.pdf
[11] OSCI Leitstelle: “XÖV-Framework V1.0 – Leitlinien für die XÖV Standardisierung”; 31 October 2006; online publication, http://www1.osci.de/sixcms/media.php/13/2006-10-31_X%D6V-Framework%20V1.0_final.pdf
[12] Terence Karran: “Pan-European Grading Scales: Lessons from National Systems and the ECTS”; Higher Education in Europe, Vol. 30, issue 1, p. 5-22; April 2005
[13] Oasis Open: “Web Service Security: SOAP Message Security 1.0 (WS-Security 2004)”; OASIS Standard 200401; March 2004; online publication, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
[14] The European Parliament and the Council of the European Union: “Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures”; 13 December 1999
[15] Strack, Karich: „BeGovSAH – Begleitforschung zur Umsetzung des eGovernment-Aktionsplans in Sachsen-Anhalt“; in: Jana Dittmann (Ed.): proceedings of „Sicherheit 2006, Sicherheit – Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)”, Feb. 2006 Magdeburg, Germany; Lecture Notes in Informatics (LNI), Volume 77, Springer-Verlag, 2006
[16] H.Strack: “MEDIA@Komm – the Pilot Project for E-Government and E-Commerce in Germany”, Proceed. ISSE 2001, Information Security Solutions Europe, London, 2001