

The Implementation of a National Student Exclusion Register in Norway

Asbjørn Reglund Thorsen, USIT, University of Oslo, Norway, a.r.thorsen@usit.uio.no

Geir Magne Vangen, USIT, University of Oslo, Norway, g.m.vangen@usit.uio.no

Agnethe Sidselrud, FS Consortium, Norway, agnethe.sidselrud@usit.uio.no

Keywords

National register, best practice, exclusion, cheating, processes, common system

1. INTRODUCTION

There is a high awareness in the Higher Education sector in Norway that cheating, plagiarism and other academic misconduct must be dealt with early in the students' education cycle, in order to prevent the serious consequences of plagiarism in scientific publishing and scientific fraud. The Ministry of Higher Education in Norway introduced the Universities and University Colleges Act in 2005, making it mandatory for the Higher Education institutions (HEIs) to inform each other about decisions concerning formal exclusion of students. In the following years HEIs developed a number of different routines to comply with the new regulation. The different routines and big variation of communication channels that were used, neither ensured accuracy of information, nor the necessary level of personal data security in the information exchanged amongst institutions. To cope with this complex challenge, the Ministry initiated the process of establishing a national student exclusion register. The register is supposed to contain data about students excluded due to cheating and plagiarism/attempted cheating, use of false documents or other academic misconduct. The register is expected to provide better procedures for informing third parties (i.e. other universities and colleges) and to prevent excluded students from gaining admission to another HEI in Norway. Another objective is to prevent admission to a HEI based on false documents.

This paper aims to present the technical solution for the Exclusion Register as well as the challenges in the implementation process due to complex legal and regulatory requirements.

2. BENEFITS AND OPPORTUNITIES

Benefits of the national register

Common IT-solutions are widely applied in the public sector in Norway and the benefits are highly valued: common systems are cost-effective, assure data quality and common procedures for the administrative processes in the public sector. The policy for common IT-systems in the HE-sector in Norway has clearly proved over the course of past few years that the added value of common IT-solutions is bigger for each new system implemented in the sector. However, common solutions demand a higher level of information security due to the greater number of stakeholders, and considerably negative consequences for the reputation of the HEIs as well as the IT-system itself in case of security incidents.

The benefits of the common exclusion register are thus effective and secure dissemination of exclusion decisions, giving the HEIs a complete overview and ensuring quality control in the

admission process: it prevents excluded students from gaining admission to another HEI in Norway, as well as preventing admission to a HEI based on false documents.

Registration of the exclusion data in the common Exclusion Register satisfies the legal requirements for secure dissemination, and at the same time it provides a lower level of information dissemination, compared to manual registration in local systems (electronic or paper-based).

It is hoped that establishment of the National Exclusion Register will have a preventive effect. Establishment and implementation of the register provides an important opportunity for HE-sector authorities and management at the HEIs to emphasize the importance of academic integrity and promote the values of its ethical policy. All forms of academic misconduct that lead to exclusion will be registered, following notification to the student, making it evident that admission or further studies at other HEIs, is impossible.

Academic exclusion policy and contents in the Exclusion Register

The register receives and forwards data about two forms of exclusion that apply to all HEIs in Norway, i.e.:

1. Admission quarantine
2. Exam quarantine (exclusion from the institution and loss of the right to sit for the examination at the institution and also at other institutions)

Summary of the academic exclusion policy according to the Norwegian Universities and University Colleges Act:

Section and description of the violation	Penalty and registration in the Excl.Register
§ 3-7. (7-8) Student has applied for admission or recognition using false documents	-prosecution /criminal charges -exclusion by admission quarantine on a national level (registered in the Exclusion Register)
§ 4-8. (1) Misconduct	-exclusion by exam quarantine for 1 year (loss of the right to sit the examination at the institution and also at other institutions for 1 year) (registered in the Exclusion Register)
§ 4-8. (2) Misconduct, threatening behaviour, indecency, breach of the confidentiality agreement (in clinical education)	-exclusion by exam quarantine for up to 3 years from the clinical studies on a national level (registered in the Exclusion register)
§ 4-8. (3) Cheating, suspicion of cheating and or attempted cheating	-exclusion by exam quarantine for 1 year on a national level (registered in the Exclusion Register)

The Exclusion Register includes the following information:

- student's national identity number,
- HEI-id,
- exclusion period,
- exclusion category (admission/exam quarantine)
- classification of studies (all/clinical education/teacher education)
- initials for administrator's name

The contents of the register were defined as including a minimum set of information required to ensure that the excluded student will be prevented from gaining admission to another HEI, and at the same time ensure exposure of minimum information in case of a security incident.

Cheating

HEIs are expected to inform the students about the prevailing regulations for examination support materials and the rules for citing when writing assignments and theses. Anything that can be of academic interest beyond the permitted support materials is classified as an unlawful aid. Statistics from the biggest HEIs in Norway show a continuous increase in the number of cases of reported cheating/suspicion of cheating/attempted cheating in the period of the last three years. This tendency is explained by tougher policies for reporting cheating/attempted cheating as well as better IT-solutions and more systematic use of devices for plagiarism control (*Ephorus*). The average number of cases of cheating/suspicion of cheating reported during the last two years at the University of Oslo is 60 (per 27 000 students) and 30 at the University of Bergen (15 000). Most of the cases are reported to the appeals committee that takes the decision about the form of penalty (annulment of examination/recognition of courses or exclusion). Approximately 50% of the cases lead to exclusion from the institution. The appeals committees in Norway point out that the cases have become more complex and far-reaching. The administrative costs have increased, not only as a result of the higher number of cases, but also because of the use of attorneys (assisting the student) has escalated.

3. DATAFLOW

The most important system that delivers data to the Exclusion Register (*referred to in this section as RUST, Register for Uttestengte Studenter*) is FS.

FS

FS (*Felles studentsystem*) is a student information system for the administration of studies and students, used in higher education in Norway. FS administers roughly 90% of upper secondary studies annually. The system has been developed by a section of the University Centre for Information Technology at the University of Oslo, called SUN (section for development of national information systems - *Seksjon for Utvikling av Nasjonale informasjonssystemer*). This section also develops systems for admission and documentation of research for higher education, and a data warehouse solution. Using FS, one can administer students, applicants and studies at all levels of higher education. FS contains 14 modules, among which are admission, teaching and evaluations. For more information, see <http://fellesstudentsystem.no>

Source information for RUST

When a student has been expelled from an institution or a study, this will be registered into FS. For each exclusion, the following information has to be recorded:

- Student identity
- Period for exclusion
- Type of exclusion (exam or admission, local or national)
- Study classification

In addition, it is possible to register a specific study programme (only for local exclusions) and a reference number to the archive system.

Before a recorded exclusion can be exported to RUST, another administrator has to control the record and accept the registration. This is a part of the registration procedures, and FS supports these procedures.

Id: 015361 12185 Stud.num: 80008 Name: TS-Svendsen Beate Ready for export to RUST																													
<table border="1"> <tr> <td colspan="2">Exclusion</td> <td colspan="2">Registration / Rust</td> </tr> <tr> <td>Institution:</td> <td>185 Universitetet i Oslo</td> <td>Imported from RUST:</td> <td>N</td> </tr> <tr> <td>Period:</td> <td>01.01.2013 - 31.10.2013</td> <td>Recorded:</td> <td>25.10.2013 TMS</td> </tr> <tr> <td>Type of exclusion:</td> <td>EKSAMENN Exam quarantine</td> <td>Changed:</td> <td>25.10.2013 FS2</td> </tr> <tr> <td>Study classification:</td> <td>ALLE All studies</td> <td>Controlled:</td> <td>J 25.10.2013 FS2</td> </tr> <tr> <td>Study programme:</td> <td></td> <td>Exported to RUST:</td> <td></td> </tr> <tr> <td>Archive num:</td> <td></td> <td>Remove:</td> <td>N</td> </tr> </table>		Exclusion		Registration / Rust		Institution:	185 Universitetet i Oslo	Imported from RUST:	N	Period:	01.01.2013 - 31.10.2013	Recorded:	25.10.2013 TMS	Type of exclusion:	EKSAMENN Exam quarantine	Changed:	25.10.2013 FS2	Study classification:	ALLE All studies	Controlled:	J 25.10.2013 FS2	Study programme:		Exported to RUST:		Archive num:		Remove:	N
Exclusion		Registration / Rust																											
Institution:	185 Universitetet i Oslo	Imported from RUST:	N																										
Period:	01.01.2013 - 31.10.2013	Recorded:	25.10.2013 TMS																										
Type of exclusion:	EKSAMENN Exam quarantine	Changed:	25.10.2013 FS2																										
Study classification:	ALLE All studies	Controlled:	J 25.10.2013 FS2																										
Study programme:		Exported to RUST:																											
Archive num:		Remove:	N																										
Id: 075664 90042 Stud.num: 191 Name: Åkselsen Catharina Must be controlled																													
<table border="1"> <tr> <td colspan="2">Exclusion</td> <td colspan="2">Registration / Rust</td> </tr> <tr> <td>Institution:</td> <td>185 Universitetet i Oslo</td> <td>Imported from RUST:</td> <td>N</td> </tr> <tr> <td>Period:</td> <td>18.03.2013 - 14.10.2014</td> <td>Recorded:</td> <td>18.03.2013 GMV</td> </tr> <tr> <td>Type of exclusion:</td> <td>EKSAMENN Exam quarantine</td> <td>Changed:</td> <td>14.10.2013 FSRICHARD</td> </tr> <tr> <td>Study classification:</td> <td>ALLE All studies</td> <td>Controlled:</td> <td>N 11.10.2013 FSRICHARD</td> </tr> <tr> <td>Study programme:</td> <td></td> <td>Exported to RUST:</td> <td>14.10.2013 14:46</td> </tr> <tr> <td>Archive num:</td> <td></td> <td>Remove:</td> <td>N</td> </tr> </table>		Exclusion		Registration / Rust		Institution:	185 Universitetet i Oslo	Imported from RUST:	N	Period:	18.03.2013 - 14.10.2014	Recorded:	18.03.2013 GMV	Type of exclusion:	EKSAMENN Exam quarantine	Changed:	14.10.2013 FSRICHARD	Study classification:	ALLE All studies	Controlled:	N 11.10.2013 FSRICHARD	Study programme:		Exported to RUST:	14.10.2013 14:46	Archive num:		Remove:	N
Exclusion		Registration / Rust																											
Institution:	185 Universitetet i Oslo	Imported from RUST:	N																										
Period:	18.03.2013 - 14.10.2014	Recorded:	18.03.2013 GMV																										
Type of exclusion:	EKSAMENN Exam quarantine	Changed:	14.10.2013 FSRICHARD																										
Study classification:	ALLE All studies	Controlled:	N 11.10.2013 FSRICHARD																										
Study programme:		Exported to RUST:	14.10.2013 14:46																										
Archive num:		Remove:	N																										

Figure 1: Exclusion recorded in FS

All exclusions that affect all HEIs, will be exported to RUST, and the information will stay in RUST until the exclusion period is terminated. At this time, the data will be anonymised and kept for statistical purpose.

Subscription to RUST-information

To receive information about exclusions, each institution has to make a subscription for every active student. This is done by sending information to RUST about every active student, and their connection to studies and exams. This enables RUST to only send information to the institutions own students, and not everybody that has been expelled.

Use of RUST-information in FS

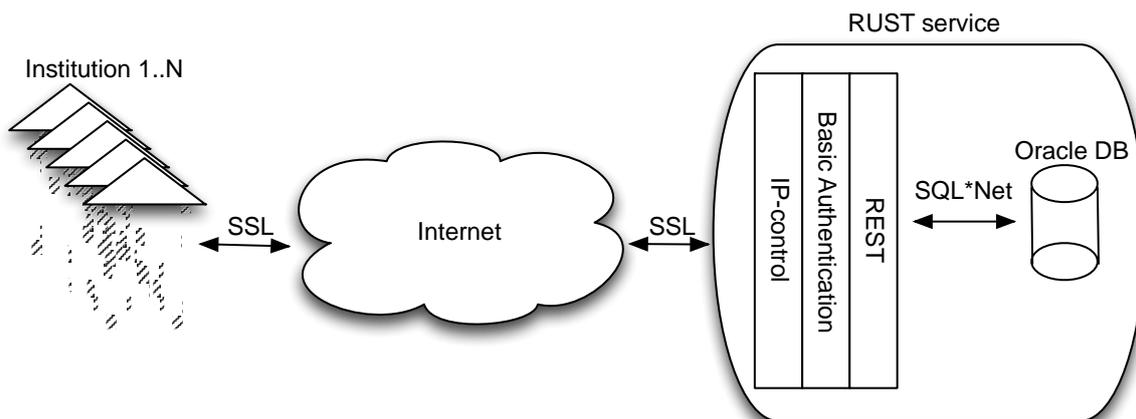
When information about an exclusion has been received from RUST, the executive officers will get an automatic warning about this. Further treatment of the information will be handled manually. In some cases, the student will not be able to register for exam via the national self service systems.

Technical

The Exclusion Register is a centralized database with a minimum of data content. This is an Oracle 11g database, placed at a secured network. The communication between local and central system is based on RESTful web services, JSON formatted, implemented in Scala. RUST offers a number of services for inserting, updating and deleting an exclusion, and for subscription of information. In this scenario, FS appears as a client system for RUST. The services run on a JBoss application server, and all traffic is SSL encrypted. Figure 2 shows the dataflow from institution A where a student has been expelled, and other institutions where the same student applies for studies or registers for an exam.

4. DATA SECURITY

It is important for these kinds of sensitive data to be stored in a secure way. The database is placed on a subnet which is only accessible from the application and a gateway. The gateway is the developer's access to production data.



All the traffic runs over encrypted HTTPS (SSL) and basic authentication is used to log in. By minimizing the amount and type of data running through this application, security is enforced even more. The web server has configured a whitelist in form of IP control which means that nobody is allowed to access except from the IPs from the whitelist. The user must provide a username and password through basic authentication to reach the RUST REST service. The REST based service connects to the database through encrypted connection using SQL*Net hence the data traffic in the wire between the web server and the database server at the server room also is encrypted. The web service is obviously reachable from the internet, however the database is only reachable from the production server and through a gateway. The Gateway is used by the developers e.g. to be able to read production logs. The gateway also has a whitelist IP control. An exclusion decision always contains the end date of the exclusion and the data will be deleted from the database automatically when this date is reached. Server logs and backup will be kept for no more than 1 year.

Through FS, an institution is only allowed to view their own applicants/students which prevents unnecessary information leakage. This means that Institution A cannot view applicants/students from Institution B.

The application has been tested for security vulnerabilities and load tested to gain the right amount of security quality. Safety procedures are also made to ensure security from the day-to-day use of the register. For example, it takes at least two individuals with the right authority from an institution to control the exclusion before submitting to the register.

The penetration test and load test is performed by two web application security experts testing the application after Open Web Application Security (OWASP) testing policies.

The penetration test was performed by setting up OWASP ZAP security scanner and proxy, to record all the requests and responses to and from the server. The test includes numerous different automated tests and a time consuming manual test. Experience shows that most of the vulnerabilities are found in the manual test, but the proxy scanner tool is priceless to fuzz input parameters with different types of data. An automated tool is very helpful with repetitive work like i.e. putting rubbish data into all possible input-fields while testing for numerous kinds of vulnerabilities.

The load test is performed using a cluster with a lot of bandwidth and nodes using Tsung as the load tool. Tsung is able, by a proxy to record the user interaction with the service. These recordings are distributed to the nodes in the cluster and Tsung is started configured to simulate users, even with

some time between actions. To get the most out of this test we cooperated with both the database administrators and web server maintainers so that they could audit the process from their point of view. This procedure often results in a better tuning of the database removing e.g. locks in the database and hardening of the web server.

5. RUNNING THE APPLICATION

A web service is a machine to machine "conversation" and in RUST (the Exclusion Register), a request can look like this:

```
curl --user I0185_RUST:PASSORD -i -H "Content-Type: application/json" -X
POST -d
' [{"fodselsdato":101112,"personnr":12345,"institusjonsnr":185,"vedtaksTypeK
ode":"P","studKlassifKode":"HELSEFAG"},
{"fodselsdato":101113,"personnr":12345,"institusjonsnr":185,"vedtaksTypeKod
e":"P","studKlassifKode":"HELSEFAG"}]' https://example.com/rust-ws/v1/requests
```

The response:

```
HTTP/1.1 200 OK
Expires: Fri, 16 Nov 2012 15:59:53 GMT
Content-Length: 761
Cache-Control: no-cache, private, no-store
Content-Type: application/json; charset=utf-8
Pragma: no-cache
Date: Fri, 13 April 2014 13:37:00 GMT
X-Lift-Version: 2.4
Server: Jetty(6.1.26)
[ {
  "fodselsdato":101112,
  "personnr":12345,
  "institusjonsnr":185,
  "vedtaksTypeKode":"P",
  "studKlassifKode":"HELSEFAG",
  "saksbehandler":"jonas",
  "datoFra":1355739798000,
  "datoTil":1450310961000
} ]
```

6. IMPLEMENTATION CHALLENGES

Political demand, high expectations and media attention to the project

There has been considerable attention paid to the project of establishing the National Student Exclusion Register. The issues of academic integrity, cheating and plagiarism are often on the political agenda both for the Ministry of HE and the HE-sector in Norway. The Ministry and the sector have both stated the need for measures to fight and reduce the scope of academic misconduct in the fields of education and research. The media attention in the early project phase contributed to considerable pressure on the project management as well as on the Ministry.

Common procedures for all HEIs

Implementation of the Exclusion Register requires a set of national guidelines and standard procedures which should be followed in the same way by all HEIs. The HE-sector in Norway is highly differentiated in regard to staff size and number of students, number of disciplines, IT-management structure and the annual budget. The biggest universities in Norway have rather complex

organizational structure and adjusting the administrative procedures to the national procedures is proving to be difficult.

System development and the organizational governance of the Register

The analyses and planning phase for the design of the Register have shown that the system to be developed requires rather simple IT-solution based on data transfer between centralized database and the local FS' What proved to be one of the biggest overall challenges in this project is the imbalance between the technical task to be solved and the extent of the legal requirements that had to be analyzed and met. Neither the authorities nor the project management were able to foresee the scope of the legal challenge and consequently were not able to work out an advanced, accurate time estimate for the project. The organizational governance of the Exclusion Register was not defined until a late phase in the project. As a result, communication with the many stakeholders was not consistently well coordinated.

Legal requirements and statutory authority

Establishment of the National Exclusion Register and the future success of the solution are highly dependent on the completeness of the data and common use of the register in the whole HE-sector. The legal authority at the time of establishing the project made it mandatory for HEI to exchange information about exclusion. It was unclear, however, if establishing a common IT-system for this purpose was a legally authorized solution. After thorough analysis of this issue, the Ministry decided to legally authorize the use of the Exclusion Register as the required way of dissemination of information about the formal exclusion. The authorization required that a new section in the Universities and University Colleges Act was passed. This legislative process takes usually up to six months, which added up to the total time estimate for the project.

Sensitive or non-sensitive data?

Another issue of major concern for the authorities (The Ministry and the Norwegian Data Protection Authority¹) and uncertainty for the project management was identifying the category of the personal data processed by the HEIs in the Exclusion Register. Is the data sensitive or non-sensitive? The Personal Data Act of 14 April 2000 Section 2 defines sensitive personal data as "*information relating to (...) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act*". The Personal Data Act also regulates conditions, which must be satisfied in order to process the data. Processing is defined as "*any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses*". As mentioned above, the information that is collected and stored in the exclusion Register is: the student's national identity number, HEI-id, exclusion period, exclusion category (admission/exam quarantine), classification of studies (all/clinical education/teacher education) and initials for administrator's name. The information does not contain explicit information about the reason for exclusion (i.e. cheating or suspicion of cheating), but merely the penalty - i.e. the exclusion. The register does not contain information about either the kind of violation, or the student's name (only the student's national ID-number). The minimum contents are, however, enough for the service to disseminate the exclusion information to the relevant HEI.

According to The Personal Data Act, section 8 and 9, personal data can only be processed if the data subject (the person) consents to the processing, or there is statutory authority for such

¹ The Norwegian Data Protection Authority facilitates protection of individuals from violation of their right to privacy through processing of their personal data. Keeps a systematic, public record of all processing that is reported or for which licence has been granted, verifies that statutes and regulations which apply to the processing of personal data are complied with, identifies risks to protection of privacy and provides advice on ways of avoiding or limiting such risks.

processing, or the processing is necessary to enable the controller to fulfill his/her obligations or exercise his/her right in the field of employment law. In addition, processing personal data requires a license from the Norwegian data Protection Authority as well as data processor agreements between the data controller (FS Consortium) and data processor (the user institutions).

From planning, analysis and design to implementation and maintenance

Implementation of the National Student Exclusion Register
1. The Ministry passes a new law: all HEIs must inform each other about formal decisions of exclusion
2. The Ministry establishes a national work group to design a solution for information dissemination for the HEIs. The work group consists of members from the Ministry, HEIs, USIT, FS Consortium, law professionals
3. The national work group puts forth a description of a common IT-solution, defines contents in the register and a set of national guidelines for information dissemination
4. The Ministry establishes a project for system development. Project leader is hired at USIT. The executive management and organizational governance of the register is not yet defined.
5. The Ministry states the need for a new section in the Universities and University Colleges Act: the use of a publicly owned IT-register for information dissemination must be legislated for.
6. USIT starts system development
7. The Ministry and the Norwegian Data Protection Authority (NDPA) discuss the contents of the register and assume that application for a licence from the NDPA is required. The organizational governance of the register is not yet defined. The application process is put on hold.
8. USIT completes development of the register. The register is ready to test and rollout.
9. The Ministry gives the executive management of the register to FS Consortium.
10. FS Consortium implements the following processes: -writing and submitting an application for a licence from the NDPA -writing and signing Data processor agreements with all user institutions (51) -performing Risk assessment for the Exclusion Register
11. The NDPA disputes the definition of sensitivity of the data in the register and thus the need for the licence. The NDPA suggests that the Ministry passes a new regulation relating to the University and University Colleges Act instead.
12. The Ministry passes the new regulation.
13. The HEIs test The Exclusion Register for functionality, performance and integration with FS.
14. The FS Consortium launches the Register and the national guidelines in the HE-sector in Norway.
15. The HEIs implement the national guidelines on campus.

8. CONCLUSION

The development and implementation of the National Exclusion Register was initiated by the Norwegian Ministry of Higher Education in order to provide national procedures for informing third party institutions about the exclusion and to prevent admission based on false documents. The establishment of the register is hoped to obtain a preventive effect with regard to academic misconduct and gives the HE-sector an opportunity to emphasize the importance of academic integrity. Additional benefits of the national solution are ensuring good data quality and introducing common procedures for the administrative processes in the HE-sector.

The solution is based on a simple IT-system that was developed by standard procedure and within estimated frame of time. The formal establishment of the register included however some complex legal and regulatory issues that had to be analyzed and solved. Our project required close dialogue and cooperation between The Ministry of HE, The Norwegian Data Protection Authority and the project management at the University Center of Information Technology in Oslo.

9. ACKNOWLEDGEMENTS

The authors acknowledge the contributions of all associated with the project. Particular mention goes to Geir Harald Hansen, Kai Quale, Richard Edvin Borge and Thomas Solvin (all University Center of Information Technology in Oslo) who developed and tested the solution and developed the system documentation.

10. REFERENCES

The Universities and University Colleges Act

<http://lovdata.no/dokument/NL/lov/2005-04-01-15> last accessed on 13 April 2014

The Personal Data Act

<http://lovdata.no/dokument/NL/lov/2000-04-14-31> last accessed on 13 April 2014

“Utestenging og RUST”

<https://www.fellesstudentsystem.no/dokumentasjon/brukerdok/> last accessed on 13 April 2014

University of Oslo website <http://www.uio.no/english/studies/about/> last accessed on 13 April 2014

11. AUTHORS BIOGRAPHIES



Asbjørn Thorsen Asbjørn Reglund Thorsen works at the University Center for Information Technology in Oslo. He is head of group and development leader of a development team consisting of 12 developers making tailored applications for Universities and Colleges Admission Service (UCAS). He has a background as a programmer and also work as a web application pen-tester. He is co founder, chairman and manager of Awareness Security AS, working as a hands-on web application security trainer, pen-tester and security advisor.

Asbjørn Thorsen graduated as Cand.Scient from the University of Oslo, Institute of Informatics in 2005.

Asbjørn Thorsen is a security enthusiast.



Geir Vangen has more than 20 years experience in developing nation wide systems within higher education in Norway. At USIT, the University of Oslo University Center for Information Technology, he works as development manager for the student information system FS. FS is in use at 51 higher education institutions in Norway. Geir Vangen is also responsible for architecture and methods for the section within USIT that develops systems for student information (FS), research information (CRISTin), national admission (SO) and data warehouse.

He participates in national and international standardization work, and has been a member of the groups developing the MLO and ELM-standards. He is a member of the steering committee of RS3G. He has been member of national committees appointed by the Ministry of Education and Research, and has lead projects on behalf of the Ministry.

Geir Vangen graduated from University of Oslo, Institute of Informatics in 1989.



Agnethe Sidselrud is a Deputy Manager for FS Consortium. Graduated from Adam Mickiewicz University in 1996 as Master of Scandinavian Studies, and from University of Oslo in 2001 as Master of Nordic Medieval Studies. Since 1998 she has been working in the Norwegian HE-sector in student and research affairs and in the university management. She has lead the national implementation project for the Current Research Information System in Norway. She is currently involved in the implementation projects for several national information systems: The National

Exclusion Register, The National Credentials Recognition Database and a new BI solution for student information analytics.