All papers submitted for publishing to the **RECENT®** journal are subjected to the scientific review procedure.

The objective of scientific review is to ensure that all papers accepted for publishing meet the requirement of an adequate scientific level and provide original and significant contributions to the respective field.

The scientific review procedures practiced by the **RECENT®** journal are *"Expert Peer-Review"* (scientific review by experts, including the members of the Scientific Board of the journal) and *"Editorial Board Peer-Review"* (review, scientific included, by the members of the Editorial Board). All members of the Scientific Board and of the Technical Board of the journal are holders of PhD degrees, are members of the scientific community and experts in their respective fields of activity.

The complete scientific review procedure of submitted papers practiced by the **RECENT®** journal is available at http://www.recentonline.ro/PeerRew.htm.

RECENT®

REzultatele CErcetărilor Noastre Tehnice

Industrial Engineering Journal

Transilvania University of Brasov, Romania

Vol. 14 (2013), No. 4(40) **ISSN 1582 - 0246**

ICEEMS 2013
7th International Conference
on Economic Engineering
and Manufacturing Systems

- selected papers -

iceems

40

November 2013

CONTENTS

Vol. 14, no. 4(40), November, 2013

Authors Presentation 207

Sorin Adrian BARABAŞ, Adriana FOTA
Experimental Determination of the Hardness Curves in Deep Carburizing Heat Treatment 212

Adina BĂNCILĂ, Constantin BUZATU
Design of an Innovative Kitchen System for People with Physical Disabilities 216

Laura BOGDAN, Monika MOGA
The Role of Infrastructure in Economic Development 220

Constantin BUZATU, Iulian Alexandru ORZAN
Contributions at the Modeling Dimensions of the Gauges by the Wear of this and by the Number of Verified Pieces 226

Catrina CHIVU
Computer Aided Selection of Material Handling Equipment 231

Cătălin-Iulian CHIVU
Virtual Grade-Sheet Based on Electronic Signature 235

Tudor DEACONESCU, Andrea DEACONESCU
Medical Recovery System of the Upper Limb Muscles 242

Grigory DEYNICHENKO, Oleg TERESHKIN, Dmitry GORELKOV, Dmitry DMITREVSKY
Stabilization of Quality Cleaning Onion Innovative Way 246

Grigory DEYNYCHENKO, Inna ZOLOTUKHINA, Kateryna SEFIKHANOVA, Inna BELYAEVA
Resource-Saving Technology of Raw Milk Recycling 251

Elena EFTIMIE
Energy Simulation of a Solar Thermal System for Domestic Hot Water and Space Heating 255

Ovidiu FILIP, Tudor DEACONESCU
Pneumatically-Actuated Device for Wrist Rehabilitation 263

Adriana FOTA, Sorin Adrian BARABAŞ
Stochastic Modeling Applied for Inventory Optimization in Advanced Production Systems 267

Cătălin GHEORGHE, Flavius Aurelian SÂRBU
Art–Market for Cultural Products Having Investment Potential 271

Mihai IONESCU
Sequence Logic Modules 278

Dmitry KRAMARENKO, Irina GALIAPA, Grigory DEYNICHENKO
Effect of the Influence of Hydrolyzate of Molluscs on the Oxidation of Vegetable Oil 283

Dmitry KRAMARENKO, Elena KIREEVA, Grigoriy DEYNICHENKO
Investigation of the Influence of Mollusc Hydrolyzate on the Elastic Properties of Wheat and Rye Dough 288

Radu Mihai MAZILU
Fittings and Pipelines MAG Tandem Welding 292

Vladimir MĂRĂSCU KLEIN
Resource Planning in the Development of Maintenance Strategies 296

Doina NEGREA (ȚÂRLIMAN), Tudor DEACONESCU, Andrea DEACONESCU
Principles and Stages of New Gripper Systems Development 301

Gennady POSTNOV, Grigory DEYNICHENKO, Mykola CHEKANOV, Vitaly CHERVONIY, Oleg YAKOVLIEV
Physicochemical Basis for Intensification of the Process of Salting Fish 307

Notes 311

All papers submitted for publication to the **RECENT**® journal undergo a peer-review procedure.

The objective of peer review is to verify and endorse that all papers accepted for publication are of adequate scientific level and include original and significant contributions in their respective field.

The **RECENT**® journal provides *Expert Peer-Review*, including by members of the Scientific Panel as well as *Editorial Board Peer-Review* by the members of the Editorial Board. All members of the Scientific Panel and of the Technical Panel have PhDs, are members of the academic community and experts in their respective fields of activity.

The received papers undergo initial *Editorial Board Peer-Review* by the members of the Technical Panel of the **RECENT**® journal, conducted mainly by the scientific secretaries. Evaluation concerns with priority whether the paper matches the fields covered by the journal and meets its standards.

Complete scientific evaluation procedure is available at http://www.recentonline.ro/PeerRew.htm

Electronic version of **RECENT**® journal, ISSN 2065-4529, is available at www.recentonline.ro

VIRTUAL GRADE-SHEET BASED ON ELECTRONIC SIGNATURE

Cătălin Iulian CHIVU
Transilvania University of Brasov, Romania

Abstract. Transfer of documents in large institution is always a problem and affects the efficiency and accuracy of the information transfer. In a university there are different types of information that should be transmitted, correlated and took responsibility by signature. The present paper presents an easiest way for this process, the electronic signed documents.

Keywords: electronic signature, client application, server application

1. Introduction

In large companies, there are carried out important projects, in which are dynamically involved a large number of employees. Most of the time, the actions of any employee involved in such a project can totally change the perspective on the project and hence the actions of the other employees involved. In these cases to work with printed documents imply high costs with paper, toner, ink, printers, service, personnel, transport and transfer. Besides these economic aspects, almost always occurs overcoming the deadline of the project. All these aspects generate high level of stress, non-efficient team-work, a lot of hard non-paid extra work. Such negative aspects may be reduced if there are implemented the electronic signed documents that will determine significantly lowest costs and shortest deadlines, lowest level of stress and highest firm productivity.

Relative to universities, today, in many Romanian universities the exchange of documents is a difficult, time consuming process, because of the procedures that specify the necessity of paper printed and signed documents. In this category of documents is included the grade-sheet, which, today, should be generated and printed by faculties' secretariat, filled and signed by the teacher and then, in most universities, the grades are introduced by secretariat in an informatics data base, the printed version being classified.

As it can be remarked in Figure 1 the process of generating, filling and validating a grade-sheet is a time consuming process with some important step done manually and therefore subject of human error.

A very simple way to eliminate almost all steps is to introduce, internally, the electronic signature and therefore the electronic validation and taking responsibility.

Electronic signature or digital signature was officially recognised in Romania by law 455/2001 according to which, the documents electronically signed have the same legal value as signed and stamped paper documents. Even if information technology had an incredible evolution and there were implemented information interlocking systems, there still are institutions where the old bureaucratic system works. In such institutions is still necessary to print, sign, register and hand all documents and in some cases, supplementary, is necessary to send the electronic version of documents but without digital signature.

Present paper briefly presents the legal aspects of this electronic signature and a structure for an informatics application that may be implemented at university level. In Romania, there is only one university that have a fully integrated system: students data base, curriculum, grades, teachers, staffing schedule (Academy of Economic Science - Bucharest)

2. Legal aspects

Law 455/2001, which *"defines the legal status of electronic signatures and documents in electronic form and the conditions applied for certification of electronic signatures"*, provides that "*the document in electronic form, which includes attached to or logically associated advanced electronic signature, based on a valid, non-suspended or non-revoked qualified certificate, and generated using a secure-signature-creation device is treated, in terms of conditions and effects, similar to the document under private signature"*[1].

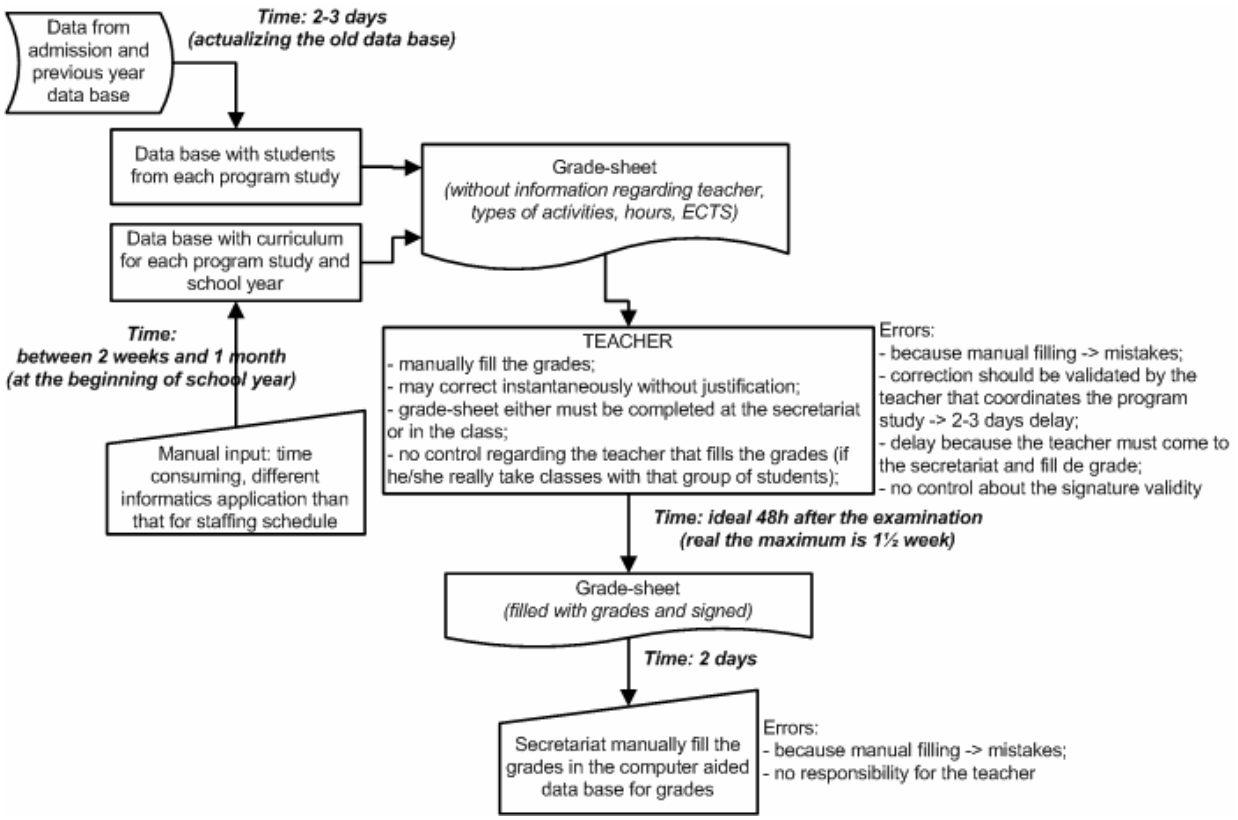

Figure 1. Information flow for developing, filling and validating a grade-sheet

Also, "*in cases where, by law, the written form is required as a condition of probation or validity of an act, a document, in electronic form, satisfies this requirement if it has included, attached to or logically associated an electronic signature, based on a qualified certificate and created by a secure signature creation device"*.

Qualified certificate is issued by a certification service provider, and "*will include identification data of the certification service provider, signatory, signer's personal identification code, signature-verification data which correspond to signature-creation data under the exclusive control of the signatory, indicate the beginning and ending of the validity period of the qualified certificate identification, identification code of the qualified certificate, advanced electronic signature of certification service provider*".

"*Each signatory will be assigned by the certification service provider a personal code to ensure unique identification of the signatory*" [1].

Electronic signatures are used to authenticate, non-repudiate and authorise.

Authentication is a technique by which a process verifies whether a communication partner is who should be, not an intruder. It also verifies if the signer communicates with the specific process.

Non-repudiation is a mechanism that certifies that an author may not claim, falsely, that he issued a certain document.

Authorisation decides the rights of a signatory or a process.

3. Method used in present

In case of internet transfer information, data could be easily intercepted, changed or even replaced by a third person and only after that sent to destination. This is a MITM attack (Man-in-the-middle attack) [3]. To avoid this type of attack it is necessary that the two persons that share information to have authentication qualified certificate. Besides this, the shared information must be encoded using public key encryption algorithm. In essence, in its simplest form, "the attack requires only that the attacker place himself between two parties that are trying to communicate and that he will be able to intercept the messages being sent and further have the ability to impersonate at least one of the parties" [3] (Figure 2)

The main idea of MITM attack is [2]: Alice wishes to communicate with Bob. Mallory intercepts the conversation between Alice and Bob and possibly modifies the messages. To initiate a dialog on a safe channel (encoded using public key

encryption algorithm), Alice sent a message to Bob requiring his public key. Mallory intercept the requirement and send it to Bob as it is coming from Alice. Bob send his public key to the Mallory, considering him as Alice. Mallory replaces Bob's public key with his own and send it to Alice. Thus, if Alice will send an encrypted message (using Bob's false public key), Mallory will intercept, decrypt, re-encrypt using Bob's public key and send to Bob. Thus, Mallory may decrypt all the messages between Alice and Bob and also being able to modify and encrypt them and send them as they are from Alice or Bob. If Alice could checks if Bob's public key is really his own, then Mallory would not be able to replace Bob's public key and therefore will not be able to dissimulate the identity. Thus, an MITM attack may be dissimulate if together with the public key the communication will use also an authentication certificate.

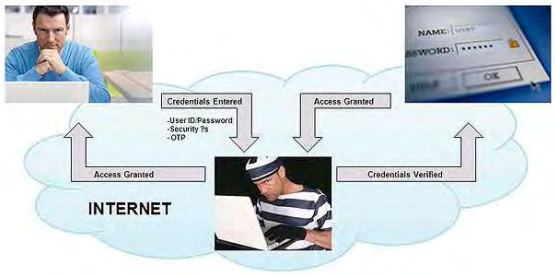

Figure 2. MITM attack representation according to [4]

An authentication certificate is based on SSL protocol (Secure Sockets Layer) [5] (Figure 3).

First step is initiation of logical connection and establishing its capabilities. The information exchange is initiated by the client that transmits a "client-hello" message with the following parameters [5]:

- version: the newest version of SSL understood by the client;
- random: random structure with 32 bits for generating time and 28 bits random generated numbers for secure;
- session ID: variable length (non-zero value signifies that application requires a refresh of connection parameters; zero value requires a new connection in a new session);
- cipher (a list of cryptographic algorithms used by the client application, in a descending order of preferences). Each element from this list contains both a key encrypting transfer algorithm and specifications;
- compression method (a list of compression methods known by client application).

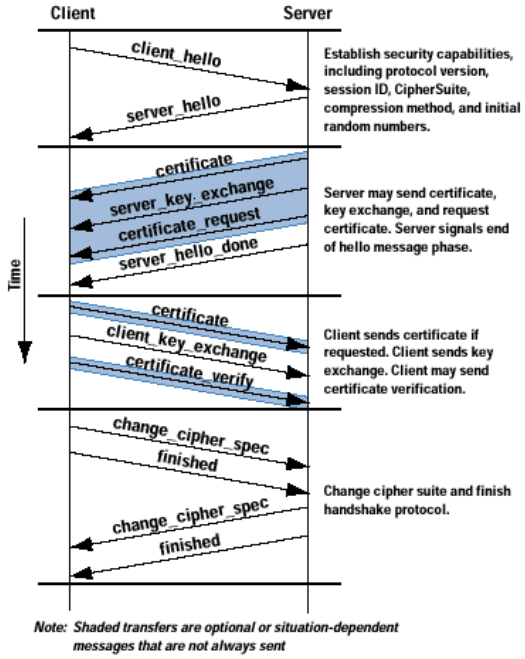

Figure 3. SSL protocol [5]

After the message "client-hello" is sent, the client waits "server-hello" from server. This message contains the same parameters list as that from the client message. For the "server-hello" message there are the following rules [5]:

- version field contains the weakest version sent by client application and the strongest one supported by the server;
- random field is generated by server application and is independent from the random field generated by the client application;
- if session identifier sent by client application is non-zero then the same identifier is sent also by server application. If this identifier is zero then server identifier corresponds to a new session;
- cipher field contains a single variant of encryption algorithm, chosen by server application from the client application list;
- compression field contains compression method chosen by server application from the client application list.

First parameter from the cipher field represents the encryption key transmission method (reciprocal transfer of cryptographic keys and MAC codes – media control address – inside client-server application). There are many transfer methods for encryption keys [5]:

- RSA (Ron Rivest, Adi Shamir and Leonard Adleman): secret key is encrypted based on public key of communication partner. In this case, there must be a public key validity certificate for the communication partner.

- Fixed Diffie-Hellman: in a Diffie-Hellman transfer server certificate contains Diffie-Hellman public key parameters signed and certificated by the Certification Authority (CA). Server application may ask client application to authenticate based on Diffie-Hellman public parameters as part of an authentication certificate if client application should be authenticated or as part of a public key reciprocal transfer. This method is used for an encrypted communication based on fixed secret key between the two partners, computed based on Diffie-Hellman public keys.

- Ephemeral Diffie-Hellman: a technique used to generate single-use secret keys (or short-time use). In this case, public keys are signed based on RSA or DSS (Digital Signature Standard) private keys of the communication partner. The partner may check the signature based on public key. The public keys are authenticated based on certificates. This version seems to be the safest option of the three Diffie-Hellman methods because it uses authenticated temporary keys.

- Anonymous Diffie-Hellman: a method based on Diffie-Hellman algorithm, without authentication. Each of two communication partners transmits to each other Diffie-Hellman public parameters without any authentication. This method is vulnerable to MITM attack, the attacker uses Anonymous Diffie-Hellman encryption method with each of the partners separately.

After choosing the method used to transmit the encryption keys there should be defined the cipher's parameters. These are used to define the encryption and hash algorithms and other specific parameters.

Second step [5] is when server application sends its own certificate (it should authenticate itself). Message contains one or more (a chain of) X.509 certificates. Message certification is required for any method used to transfer encryption keys, less for Anonymous Diffie-Hellman one. If it is used Fixed Diffie-Hellman transfer method, the certification message represents the server application key transfer because it contains server application Diffie-Hellman public parameters.

After this, if the server sent a certificate based on Fixed Diffie-Hellman parameters, it may be necessary to be transmitted a server-key-exchange message or it is used RSA keys transfer method.

An application that does not allow connections Anonymous Diffie-Hellman may require a certificate from the client application. Authentication request message, certificate-request, includes two parameters: the type of certificate and certification authority. Type indicates the type of certificate-based on encryption algorithm public key. The second parameter is actually a list of distinguished names of acceptable certificate authorities.

Last message of the second step, mandatory in all cases, is server-done signal, which indicates to client application that is the time to check the authentication of server application parameters.

In third step [5] client application send a message that contains its own certificate parameters (if those parameters were requested by server application). If client application has no certificate then it sends a no-certificate message.

Then client application sends the client-key-exchange message, which is mandatory. The message contains the type of transmission method for keys transfer.

The third step may end with a certificate-verify message for the client application. This type of message is sent only when client application certificate has a signature attached.

In Step four [5] is established the fully secured connexion. Client application send a change-cipher-specification message that transfer cipher's specifications to server application and a finished message, encrypted based on new algorithms, keys and secures. Finished message checks the success of the authentication process. As response, server application first sends its own change-cipher-specification message, which contains the current cipher's specification, then a finished message.

After this step is finalised, the client-server application secured communication protocol is ended and it can start the data level information exchange.

After all data were transfer the TCP session ends. Since there is no TCP-SSL direct link, SSL connection may be maintained in order to continue the client-server application dialog. Many of the secured connection parameters are kept. If the client or server application wants to resume the communication, it is not required renegotiation of encrypting algorithms or communication public keys. SSL specifications recommend that secured connection specification should not be stored more than 24 hours. If communication doesn't resume within 24 hours, all the specific information regarding secured connection will be erased and to reconnect it should be repeated all authentication steps. If, within 24 hours, client or server application does not accept to resume the old secured connection, then, to create a new secured connection is necessary to repeat the authentication process.

4. Implementation

Normally authentication is performed based on authentication certificate issued by a recognized certification provider.

To implement a communication system based on electronic signature, a company needs such a qualified certificate, certifying its identity and a number of qualified certificates equal to the number of company employees involved in the transfer of electronic signature information signed. A certificate can be obtained through a contract with a provider of certification services (surcharge).

According to Law 455/2001, the *provision of certification services is not subject to prior authorization and conducted in accordance with the principles of free and fair competition, compliance with laws in force* [1].

In these circumstances, any company can become its own certification service provider and issue certificates of authentication for its own identity and all its employees involved in the transfer of internal documents electronically signed by following all the conditions laid down in the law 455/2001.

Implementation of virtual grade-sheets involves implementing of a server application that runs on an institution's server (with an internet address or fixed IP) and a client application that runs on institution's PC.

When it started client application requires a username and a password. These login data are requested to eliminate the possibility that an unauthorised person that has access to a computer of an employee of the institution, to issue documents on behalf of him or to access confidential data.

Client application connects to institution's server, based on its address (address directly implemented in client application) and interacts with the appropriate server application. To start the communication it is requested a SSL connection authenticated based on certificates. Institution's server can validate client application based on employees' certificates, which were issued by the same institution and must have a correspondent in a certificates database permanently accessible by the institution's server.

Once satisfied these conditions, institution's employees may have secured access to internal documents, can change these documents. These actions (access, changes, etc.) will be automatically registered as time and person.

Based on the identity of the employee (it will be recognised the authentication certificate), server application will decide the rights of the employee relative to type of documents that will be accessed, and changes that may be done. These rights associated to the access level are provided to client application, which can enable or disable various functional modules, based on the employee's role in institution.

In the case of documents that should be signed by many people, the server can provide ascending hierarchical access to employees (ascending as responsibility), and even their notification to assume responsibility. If a document is rejected at a certain level, in order to eliminate an error, server will determine a descending hierarchical notification of the people that took responsibility of the document.

Implementing a virtual grade-sheet involves developing several modules for client application (at least three), one module for faculties' secretariat, which configures the grade-sheet, one for teachers (full-time or part-time) that have authentication certificate and another one for faculties' secretariat for data processing.

Software interface for the grade-sheet's configuration module (exclusively used by the faculties' secretariats) should allow to:

- create new grade-sheet;
- select the study program for which is generated the grade-sheet;
- select a study-year for the selected study program;
- select the discipline from curriculum for which is generated the grade-sheet;
- define the characteristics of the discipline: based on curriculum are the hours for each activity, ECTS and also the teacher;
- allocate the group or groups of students, to be included in grade-sheet;
- allocate the students to appear in the grade-sheet (this process may be a semi-automatically one, an authorised person may enable or disable one or more students in this list, based on different internal criteria – non-payment of tuition, new enrolled students or those expelled, etc.);
- allocate data for examination and re-examination according to the school year;
- allocate more than one date for the teacher to validate the marks (semi-automatically process if this application is correlated with the schedule of the examination period available for all university or entered once for all grade-sheets);
- be able to assign the teacher in any moment (based on the dean approval) to correct any faults found;
- allocate one or more teachers to one discipline, according to staffing schedule (this process may be an automatically or semi-automatically one).

The document that results from this interface will be both signed by the person responsible for generating it and electronic signature of the person / persons hierarchical superior (dean secretary).

Using the module interface for university teachers, the user must:

- be able to select from a predefined lists the faculty, study program, discipline and group of students that has been subject to examination results (the teacher, based on staffing schedule, will have access only to his/her disciplines);
- be able to select one of the entries examination sessions data (this may be semi-automated);
- be able to select, from a predefined list of student, only one student;
- be able to introduce a grade or mark for a prese-lected student (data of the mark and the mark will be automatically saved with the server time);
- after expiring the period for entering or changing a grade, all students that do not have a grade/ mark will appear absent;
- all the actions done by teachers in grade-sheet are automatically recorded, in chronological order (one a grade or mark is introduced it cannot be deleted but modified by adding new grade/mark and with justification and dean's approval of the change).

The application, as part of the same module, contains a user-supporting sub-module. From the interface of this sub-module the teacher may optionally:

- automatically or semi-automatically configures a schedule of attendance to the course, seminar, laboratory or project activities, with field for comments relative to each meeting;
- indicate a number of optional or mandatory tests that students must pass or a number of compulsory subjects for which the students will be graded during the written or verbal exam (indicate the type of assessment and the component of it);
- specify the weight of each component of the final grade (the final exam, the summative and formative aspects of the assessment);
- specify a correcting-subjecting weighting constant for all selected grades (same for all the students);
- introduce compulsory attendance requirements as condition for final grade;
- get a hint on the grade/ mark, according to the above defined criteria;
- be able to grant, or not, one point-grade by default;
- specify the transformation applied to the grade (applying a round or truncation operation);
- get a statistical distribution of the results (histogram distribution);
- be able to validate or non-validate the access to these information of other authorised persons (information regarding attendance to activities may be relevant to assessment).

Interface of the third module for data processing, used by the secretariat, should be able to

- view all results;
- view all changes made by teachers and also, their motivation;
- view all electronic signatures of all teachers and their assumption of any grade or mark;
- request a report of all changes made by the teacher from the last actualisation;
- validate last change done by the teacher in order to centralise the results;
- validate and centralised all the grade-sheet.

5. Conclusion

A major advantage of this type of communication, based on electronic signature is that, unlike the classic one, on printed paper, the documents may be presented as spread-sheets, of various types, having a structure that is controlled developed and assumed by electronic signature. Spread-sheets can be very easily verified because they may include automatic clearance and validation mechanism.

Another advantage of electronically signed documents is the significantly shorten time need for drafting, checking, validating and finalising such documents. The preparation time decreases, because the server will provide the person who needs to create a new document, all necessary data, including pre-filled document template with immutable data (data variables can be placed in the selection box). Verification time will be minimized by introducing automatic document template verification mechanisms, so the person who develops the document may know almost instantly whether partial or final version of the document is corrected by visually checking some marks. Because the verification process is easier, the time needed for this step is shortest. The person/ persons that should validate the document can simply check the visual marks that indicate the accuracy of the document and the final results and may check a box for validation. When the validation box is checked, automatically there are memorised the time of this validation and the electronic signature of the person that validated the document (Figure 4).

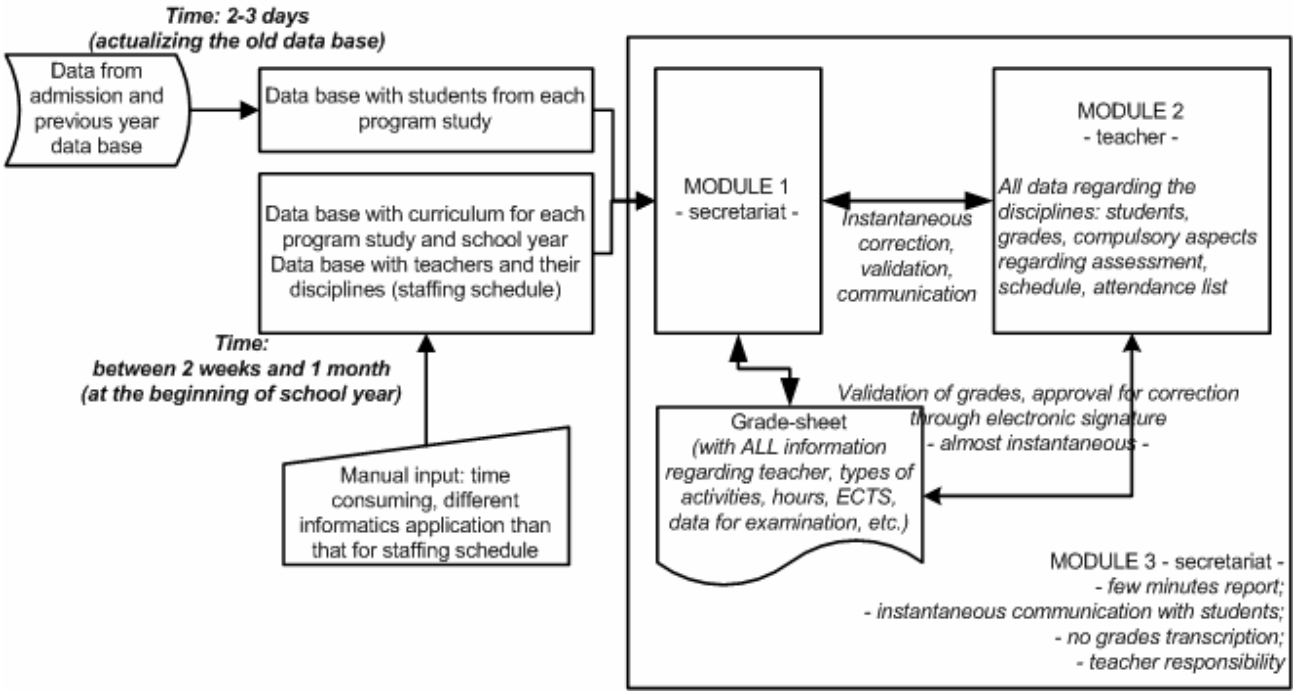

Figure 4. Structure of the application

As in can be seen in Figure 4, another advantage of this application is the bidirectional communication between management and teachers and instantaneous communication of grades to the students. Another important aspect is related to the person that is responsible to introduce the grade. In actual status (Figure 1) this responsibility is assigned to secretariat, which is not quite correctly. Implementing the suggested application the responsibility pass to the teacher.

Unfortunately, there still are some aspects, time-consuming, that should be corrected: one application for curriculum and staffing schedule. This will offer a data base to the secretariat without any delay, at the beginning of the school year.

References

1. *** *Legea nr. 455/ 2001 privindsemnăturaelectronică (Law 455/2001 regarding electronic signature - Romanian).* Available at: http://www.dsclex.ro/legislatie/2001/iulie2001/mo2001_429.htm#l455. Accessed: 20/02/2013
2. *** *Man-in-the-middle attack* Available at: wikipedia.org/wiki/Man-in-the-middle_attack, Accessed: 14/03/2013
3. *** *What is a Man-in-the-middle attack?* Available at: http://blog.kaspersky.com/man-in-the-middle-attack/. Accessed: 14/03/2013
4. *** *Indonetwork Security - Man-in-the-middle attack?* Available at: http://indonetworksecurity.com/network-security/man-in-the-middle.htm. Accessed: 14/03/2013
5. Stallings, W. (1998) *SSL: Foundation for web security*. The Internet Protocol Journal, ISSN 1944-1134, vol. 1, no. 1 (June, 1998). Available at: www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html. Accessed: 18/03/2013