Syllabus

1. Program information

1.1. Institution	ACADEMY OF ECONOMIC STUDIES
1.2. Faculty	Economic Cybernetics, Statistics and Informatics
1.3. Departments	(Departament) INFORMATICA SI CIBERNETICA ECONOMICA
1.4. Field of study	Economic Informatics
1.5. Cycle studies	Master Studies
1.6. Education type	Full-time
1.7. Study program	IT&C Security
1.8. Language study	English
1.9. Academic year	2016-2017

2. Course information

2.1. Name	**Electronic Signature**								
2.2. Code	**16.0241IF1.1-0002**								
2.3. Year of studies	**1**	2.4. Semester	**1**	2.5. Assessment type	**Exam**	2.6. Course type	**O**	2.7. Number of ECTS	**5**
2.8. Instructors									

3. Total estimated time

3.1. Number of weeks	14.00		
3.2. Number of hours per week	2.00	of which	
		C(C)	1.00
		S(S)	1.00
3.3. Total hours from curriculum	28.00	of which	
		C(C)	14.00
		S(S)	14.00
3.4. Total hours of study per semester (ECTS*25)	125.00		
3.5. Total hours of individual study	97.00		
Time distribution for individual study			
Study the textbook, course support, bibliography and notes			
Further reading in the library, on the online platforms and field			
Preparing seminars, labs, homework, portfolios and essays			
Tutoring			
Examinations			
Other activities			

4. Prerequisites

4.1. About curriculum	Cryptography Basis
4.2. About skills	The course assumes no prior compenteces.

5. Requirements

C(C)	Course lectures take place in rooms with multimedia teaching equipment.
S(S)	Laboratories are held in rooms that have PCs with Internet access. The development environment used is Microsoft Visual Studio 2010 or 2012, Ubuntu in virtual machines with GCC, Java plus necessary tools.

6. Skills covered

	C3	Using modern computer technologies for developing components that ensure maximum IT security
	CT1	Applying the rules and values of professional ethics for decision making and independent or team implementation of complex tasks / objectives at work

7. Course objectives

7.1. General objective	Presentation of the electronic signature technology and public keys infrastructures.
7.2. Specific objectives	Cunoasterea semnaturilor electronice calificate, duale, de grup si XML. Cunoasterea modalitatilor de implementare a semnaturilor electronice calificate cu tokenuri speciale/carduri inteligente de catre autoritati de certificare acreditate prin lege.

8. Course contents

8.1. C(C)		Teaching methods	Advices
1	1. ELECTRONIC SIGNATURES OPERATION •Functional objectives of the electronic signatures •Public key cryptography based signature •Public key infrastructure •Examples of electronic signatures use and the ckassification of the digital signatures schemes •RSA and DSA signature scheme •Group, dual, blind, proxy and udeniable signatures •Eliptic curves based signatures and XML signature standards		
2	2. CERTIFICATES INFRASTRUCTURES Necessity of certificates infrastructures, Digital certificates, Components of a PKI, Certificate validity evaluation, PKI architectures, PKI interoperability, Case studies, PKI components for Windows operating system, PKI implementation methodology		
3	3. ATTACHED SERVICES OF THE ELECTRONIC SIGNATURES State validity of the digital certificates, Temporal marking, Electronic signature archivation, Electronic signatures format, Secure sistems used in electronic signatures creation, WYSIWYS concept , Document signing policy		
4	4. SMART CARDS AND ELECTRONIC SIGNATURES Short history of the smart cards, Smart cards applications, The hardware of a smart card, Smard card security, Communicationg with the card, The software of the smart card, Smart card readers and terminals, Smart cards standards and industrial initiatives, Smart cards for digital signatures, Windows authentication with smart cards		
5	5. BIOMETRIC AUTHENTICATION AND ELECTRONIC SIGNATURES Signatures creation sistems and secure signatures creation devices, Biometric methods classification, Using biometric systems for electronic signatures, Keys management		

Bibliography

- Patriciu V., Bica I., Pietrosanu M, Securitatea comertului electronic, All, 2001
- Patriciu V., Bica I., Pietrosanu M, Internet-ul şi dreptul, All, 1999
- Ford W., Secure Electronic Commerce, Prentice Hall, 2001

8.2. S(S)		Teaching methods	Advices
1	1. ELECTRONIC SIGNATURES OPERATION •Functional objectives of the electronic signatures •Public key cryptography based signature •Public key infrastructure •Examples of electronic signatures use and the ckassification of the digital signatures schemes •RSA and DSA signature scheme •Group, dual, blind, proxy and udeniable signatures •Eliptic curves based signatures and XML signature standards		
2	2. CERTIFICATES INFRASTRUCTURES Necessity of certificates infrastructures, Digital certificates, Components of a PKI, Certificate validity evaluation, PKI architectures, PKI interoperability, Case studies, PKI components for Windows operating system, PKI implementation methodology		
3	3. ATTACHED SERVICES OF THE ELECTRONIC SIGNATURES State validity of the digital certificates, Temporal marking, Electronic signature archivation, Electronic signatures format, Secure sistems used in electronic signatures creation, WYSIWYS concept , Document signing policy		
4	4. SMART CARDS AND ELECTRONIC SIGNATURES Short history of the smart cards, Smart cards applications, The hardware of a smart card, Smard card security, Communicationg with the card, The software of the smart card, Smart card readers and terminals, Smart cards standards and industrial initiatives, Smart cards for digital signatures, Windows authentication with smart cards		
5	5. BIOMETRIC AUTHENTICATION AND ELECTRONIC SIGNATURES Signatures creation sistems and secure signatures creation devices, Biometric methods classification, Using biometric systems for electronic signatures, Keys management		

Bibliography

- Patriciu V., Bica I., Pietrosanu M, Securitatea comertului electronic, All, 2001
- Patriciu V., Bica I., Pietrosanu M, Internet-ul şi dreptul, All, 1999
- Ford W., Secure Electronic Commerce, Prentice Hall, 2001

9. Course contents corroboration with the demands of epistemic community representatives, professional associations and representative employers

Taking into account the best practices from IT&C field applied by big companies such as: Intel, Oracle, Microsoft, IBM, HP and professional consortiums such as: Apache, Red Hat, ISO/IEC and national agencies in charge .with the implementation of the information security.

10. Assessment

Activity	Assessment criteria	Assessment methods	Percentage in the final grade
10.1. S(S)			40.00
10.2. Final assessment			60.00
10.3. Grading scale	Whole notes 1-10		
10.4. Minimum performance standard	Knowledge required: electronic, blind, dual and group signatures creation using cryptiographic algorithms. The point granted by default is included in the weights assigned to the types of assessments.		

Completion date,

07/10/2016

Instructors,

Approval date of department

Director of department,