BASIC INFORMATION:

	Code	*Content*
Organizational unit	01.07.300.	College of Information Technologies
Abbreviation	**FIT-CIT**	
Department	01.06.050.	Department of Computer Communications, Networks and Protection
Subject/module	1.02.01.04.027.	**PKI systems**
Broader/additional title	1.02.01.04.027.	Public Key Infrastructure systems

TYPE OF SUBJECT:

Functional area	**Specialist**
Level of abstraction	**Advanced**
Type of course-obligation	**Mandatory**

COURSE REGISTER:

	Code	*Content*
Scientific area	1	Natural sciences
Scientific field	1.02	Computers and IT
Narrow scientific area	1.02.01.	Computer sciences
Scientific sub-area	1.02.01.04.	Information technologies
Scientific discipline	1.02.01.04.027.	PKI systems (Public Key Infrastructure)

COURSE DESCRIPTION:

Educational and professional goals	To present the basic and introductory considerations regarding the PKI (Public Key Infrastructure) system and electronic certificates on which the most modern systems of electronic business, electronic banking and electronic administration are based today.
Competences/educational outcomes	The student understands the infrastructure of the Public Key Infrastructure (PKI) system and why this infrastructure provides an environment for reliable application of electronic business. The student can explain the need and manner of combined application of asymmetric and asymmetric cryptographic systems. The student is able to list all components of the PKI infrastructure, and to work operationally with applications that form part of that infrastructure. The student is able to interpret the documents and procedures that define the way of realization of PKI infrastructure. The student is able to explain the four basic cryptographic functions in e-business, as well as to explain how to achieve these functions: the authenticity of the parties in communication, data integrity, the impossibility of subsequent denial of transactions and protection of data confidentiality. The student understands the role, structure and way of using digital certificates and knows how to explain why these certificates are unambiguous electronic identifiers of authorized participants in the computer network. The student is familiar with other components of the PKI system, especially the role of the certification body (CA) and registration bodies (RA).

	The student understands the practical applications of the relevant European and domestic legislation in the field of digital signature and PKI system.
Mastered skills:	The student is able to work operationally with applications that form part of the PKI infrastructure. The student is able to independently prepare and complete the application of a legal entity for obtaining digital certificates and to implement the PKI system with the employer.
Course content:	The following topics will be covered within the subject PKI systems: PKI systems - introduction PKI system components Basic documents of the PKI system Certification Body (CA) CA - security aspects Registration body Contents of the digital certificate Extensions in digital certificates Digital certificates, structure and standards Certificate lifecycle management Certificate distribution systems PKI applications PKI security aspects Generic model of CA implementation as a software-hardware system for generating digital certificates Examples of PKI system implementation Law on Electronic Signature Characteristics of the application of electronic signature law in Europe Criteria for forming a qualified electronic signature Criteria for a means of forming a qualified electronic signature Criteria for certification bodies that issue qualified electronic certificates Establishment of the National PKI infrastructure with examples from Serbia and BiH Aspects of the PKI system within the eIDAS regulations Certification bodies as trusted PKI service providers Time Stamping services Electronic signature and electronic certificate validation services

COURSE METRIC: Regular

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
5	**30**	30	24			60	6	**150**

COURSE METRIC: Extramural

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
5	**15**	30	24			75	6	**150**

Lecture languages	**Languages of the people of BiH**			

PREREQUISITES FOR ACCESS

Code	Course/module title	Grade	Description of conditions (additional)
2.09.11.011.	Fundamentals of cryptography		
2.09.04.001.	System software (operating systems)		
1.02.01.02.001.	Network computing		
2.09.11.122.	**Protection of computer and business systems**		

COURSE METHODOLOGY

During the course, the following activities are envisaged

- ☑ 45 contact hours of interactive lectures;
- ☑ 30 hours of exercise in the field of PKI systems implementation;
- ☑ 24 hours for writing and defending a seminar paper on PKI systems implementation.
- ☑ 60 hours of individual learning for full-time students;
- ☑ 75 hours of individual learning for extramural students;
- ☑ 6 hours of research.

Lectures according to the established schedule with the use of modern presentation and demonstration tools and techniques with the application of interactive methods of working with students, which provides insight into their prior knowledge and specific experiences based on the issues, but also insight into the continuity of mastering the material. 45 contact hours of interactive teaching are planned for the subject "PKI systems".

Lectures are conducted using didactic and educational content in electronic and digital form (which includes recorded lectures and mentoring exercises) on various video presentation media (interactive multimedia optical media).

Application of **information and communication technologies** (ICT) that enable students through Computer Assisted Learning & Research to achieve an active relationship in the process of acquiring knowledge with the help of computer and communication technology, to achieve deeper interaction with teaching content and application of research techniques the very process of acquiring knowledge.

Exercises are intended to acquire practical skills and elaborate practical aspects of various software and hardware technologies for the protection of computer and business systems by applying PKI technology. The content of the exercises is accompanied by thematic units of lectures. During the exercises, the student is obliged to consult with the heads of the competent Department of Computer Communications, Networks and Protection. As specific forms of exercises, **repeaters** are used where assistants/demonstrators prepare students for the exam by offering them a concise overview of the main points of a particular subject. 30 contact hours of exercises are planned for the subject "PKI systems".

Exercises will be performed in the computer room of the Pan-European University or in the Laboratory for Information and Communication Technologies and Distance Learning: (ICT-information & communication technologies & DL-distance learning) or. in university laboratories or in authorized laboratories and/or institutions with which the Pan-European University has concluded agreements on teaching-scientific and business-technical cooperation in which the name and status of the partner institution, teaching base, i.e. university clinical center and university laboratory.

In addition to the planned individual and group learning for the planned duration, it is planned that the student will spend 6 hours researching the source.

STUDENT EVALUATION

No.	Evaluation type	Partial/ Final	Optional/ Mandatory	Perc. of part.
01	Exercise	Final	Mandatory	15%
02	Two colloquiums	Partial	,,	30%
03	Seminar paper	Final	,,	15%
04	Final exam	Final	,,	40%
05				

LITERATURE/RESOURCES (listed in order of importance)

Author (name and surname)	Publication title	Publ. seat	Publisher	Issue year	Type of publ.*
a/ Basic literature					
Buchmann, Johannes A., Karatsiolis, Evangelos, Wiesmaier, Alexander	Introduction to Public Key Infrastructures		Springer	2013	coursebook
Suranjan Choudhury, Kartik Bhatnagar, and Wasim Haque	Public Key Infrastructure Implementation and Design	New York	M&T Books An imprint of Hungry Minds, Inc.	2002	coursebook
Prof. Dr.Milan Marković	PKI systems – Lecture materials	Banja Luka	Apeiron	2021	script
b/ Additional literature					
Prof. Dr.Milan Marković	PKI systems			2021	presentations
c/ Other resources - journals					
Author name and surname *(if the resource is an article)*	Journal title	Publ. seat	Publisher	Issue year	Type of journal

d/ Other resources – WEB

Website	Webpage	Paper title/hyperlink	Read

(*)Type of publication (coursebook, script, compendium, multimedia)