COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Electronic Signature Infrastructure and Electronic Commerce	**PSEP7134**

Lecturer(s)	Department where the course unit is delivered
Coordinator: assoc. prof. dr. Valdas Undzėnas **Other lecturers:** **-**	Department of Software Engineering Faculty of Mathematics and Informatics Vilnius university

Cycle	Level of course unit	Type of the course unit
Second	-	Optional

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	Autumn semester, second year of study	Lithuanian, English

Prerequisites and corequisites	
Prerequisites: Requirement Engineering, Software Architecture and Design	**Corequisites (if any):** **-**

Number of ECTS credits allocated	Student‘s workload	Contact hours	Self-study hours
6	160	66	94

Purpose of the course unit: programme competences to be developed		
To deepen one’s knowledge of electronic data protection, methods of protection, electronic signature and Public Key Infrastructure (PKI); to form abilities of students to define the need of data protection and appropriate means in electronic commerce, public and private sectors.		
Learning outcomes of the course unit: students will be able to	**Teaching and learning methods**	**Assessment methods**
Substantiate electronic data protection against unauthorized exchange or disclosure to unauthorized persons, verification identity of persons.	Interactive lectures, Seminars, Individual reading.	Discourse in seminars (oral) and paper (written), Take an exam (written).
Deal with public key infrastructure (PKI) implementation issues and use electronic signature technology in electronic commerce, public procurement, internet voting, etc.		

Course content: breakdown of the topics	Contact hours							Self-study work: time and assignments	
	Lectures	Tutorials	Seminars	Practice	Laboratory work	Practical training	**Contact hours**	**Self-study hours**	**Assignments**
1. The reasons for emerging of electronic signature, the need for it in electronic commerce, the principles of signing and verification of electronic signature (e-signature), the required infrastructure.	4	1	3				**8**	**8**	Individual reading, preparation for discourse in seminars, paper preparation, problem solving.
2. Hashing and asymmetrical encryption algorithms that are most commonly applied in e-signature technology.	2		2				**4**	**10**	
3. The need for certificates as person identity documents in electronic space, requirements for certificate issuers and systems used by them.	8	2	6				**16**	**20**	
4. The structure of e-signature and information elements in it.	2		2				**4**	**8**	
5. The procedures and applications used for creation and verification of e-signature. Secure signature creation devices (e.g. smartcards).	8	2	6				**16**	**18**	
6. Time stamp, requirements for trustworthy systems of time stamp and what is required for ensuring long-time validity of e-signatures.	4	1	3				**8**	**10**	
7. Quality assessment of procedures and rules for e-signature certification services and systems.	4		4				**8**	**8**	
8. Preparation for the exam; exam in written form.							**2**	**12**	
Total	**32**	**6**	**26**				**66**	**94**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Discourse in seminars (oral) and paper (written)	40	During the semester	Assessment: 4 – a student has made excellent discourse in seminars and has prepared a paper, active participation in seminar discussions; 3 – good discourse in seminars and the paper, participation in seminar discussions; 2 – mediocre discourse in seminars and the paper; 1 – low discourse in seminars and no prepared a paper; 0 – a student has not made discourse in seminars and has not prepared a paper. Are not allowed to keep the exam.
Exam (written)	60	Exam session	Assessment: 6 - excellent knowledge and abilities; 5 – satisfactory knowledge and abilities; 4 – minimal knowledge and abilities; <4 – exam is not passed. Final assessment: assessment of discourse in seminars and paper plus result of passed exam.

Author	Publishing year	Title	Number or volume	Publisher or URL
Required reading				
1. Valdas Undzėnas	2003, 2008	Electronic signature infrastructure and electronic commerce. Teaching material		http://mif.vu.lt/~valund
2. The Seimas of the Republic of Lithuania	2000, 2002	Law on Electronic Signature	Nr.VIII-1822	http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=105849
3. Government of the Republic of Lithuania	2002-12-31	Resolution "Requirements for certification authorities issuing qualified certificates, requirements for electronic signature device, approval of rules for registration of certification authorities issuing qualified certificates and of electronic signature supervision regulation" (in Lithuanian)	Nr. 2108	http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198003&p_query=&p_tr2=2
Recommended reading				
1. ETSI	2003	ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.		www.etsi.org
2. ETSI	2006	ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.		www.etsi.org
3. ETSI	2005	ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).		www.etsi.org
4. CEN Workshop Agreements	2004	CWA 14171 General guidelines for electronic signature verification.		www.cen.eu