

РЕПУБЛИКА СРБИЈА МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА Сектор за аналитику, телекомуникационе и информационе технологије Одељење за информациону безбедност Одсек за сертификациони систем

УПУТСТВО ЗА ПОТПИСИВАЊЕ ЕЛЕКТРОНСКЕ ПОШТЕ

1. Потписивање у Outlook 2010

Да потписивање мејлова било могуће неопходно је да адреса електронске поште са које се шаље мејл буде идентична адреси електронске поште која је уписана у сертификату.

Неопходно је извршити конфигурацију Outlook-а на следећи начин: Из менија **File** изабрати опцију **Options.**



Слика 1.

Затим изабрати опцију Trust Center и притиснути дугме Trust Center Settings...



Слика 2.

Изабрати секцију E-mail Security где је потребно чекирати Add digital signature to outgoing messages и Send clear text signed message when sending signed messages.

Слика 3.

Затим притиснути дугме Settings након чега се отвара форма Change Security Settings .

Change Security Settin	gs	×
Security Setting Preferences Security Settings Name:		
My S/MIME Settings (spa	vicinf@mup)	*
Cryptography Format:	5/MIME	Y
Default Security Settin Default Security Settin Security Labels	g for this cryptographic message format g for all cryptographic <u>m</u> essages <u>N</u> ew <u>D</u> elete <u>P</u> assword,	
Certificates and Algorithm	s	
Signing Certificate:	Choose	
Hash <u>A</u> lgorithm:	×	
Encryption Certificate:	Choose	
Encryption Algorithm:	×	
Send these certificates	; with signed messages	

Слика 4.

Притиском на дугме **Choose...** добија се листа сертификата одакле је потребно изабрати одговарајући сертификат за потписивање. Означити сертификат и притиснути дугме **View Certificate.**

	•			
Issued to	Issued by		Friendly na	Expiration
	MUPCA Gra	Secure Ema	None	19.5.2015

Сертификат за потписивање мора имати непорецивост (Non-Repudiation) у детаљима сертификата (Details) у делу употреба кључа (Key Usage).

Conser	Details	Contification Date	Trust	
ueneral	Dotails	Ceruncation Fath	TTUSt	
<u>S</u> how:	<all></all>		~	
Field			Value	^
Ce Ce CF Ba	3.6.1.5.5.7 ithority Kej ittificate P }L Distribu isic Consti	?.1.3 y Identifier olicies ition Points raints	30 14 30 08 06 06 04 00 8e 46 KeylD=9e 80 c1 b9 d9 65 f5 c4 [1]Certificate Policy:Policy Identi [1]CRL Distribution Point: Distrib Subject Type=End Entity, Path	
Ke	y Usage		Digital Signature, Non-Repudiat	
Th Th	iumbprint i iumbprint	algorithm	sha1 49 f9 9c 0b 43 37 02 a0 ba d3	~
Digital	Signature,	Non-Repudiation (c0)	
		E	dit Properties	

Слика 6.

Након избора сертификата притиснути дугме ОК (слика 5.) На исти начин потребно је изабрати сертификат за шифровање. Притиском на дугме **Choose...** добија се листа сертификата одакле је потребно изабрати одговарајући сертификат за шифровање. Означити сертификат и притиснути дугме **View Certificate.**

ATAH MURCA Gra Secure Ema None 19.5-20
AnAnim Morca aram Decore ciliam None 19.3.20
A MAILINE MORCA GIGIN SOCOLO E LINGINE MONO 19,3720.

Слика 7.

Сертификат за шифровање мора имати **Key Encipherment** у детаљима сертификата **(Details)** у делу употреба кључа **(Key Usage).**

				<u>.</u>
General	Details	Certification Path	Trust	
<u>S</u> how:	<alb< td=""><td>~</td><td>~</td><td></td></alb<>	~	~	
Field			Value	^
Ce CF Ba Ke Th Th	thority Ke rtificate P IL Distribu sic Constr y Usage umbprint umbprint	y Identifier olicies ition Points raints algorithm	KeylD=9e 80 c1 b9 d9 65 f5 c4 [1]Certificate Policy:Policy Identi [1]CRL Distribution Point: Distrib Subject Type=End Entity, Path Digital Signature, Key Encipher sha1 95 a3 9f c5 bc ce 8e 80 87 78	
Digital :	Signature,	, Key Encipherment	(a0)	
		E	dit Properties Copy to File	

Након избора сертификата притиснути дугме ОК (слика 7.) Када се заврши са избором сертификата за потписивање и шифровање, потребно је притиснути дугме ОК да би се затворила форма **Change Security Settings** са слике 4.

Када се заврши са конфигурисањем треба притиснути дугме ОК (слика 3). Након завршене конфигурације могуће је слање дигитално потписаних мејлова.

) 🖬 י	9 (° ÷	↓ ↓	Untitled - Me	essage (HTML)		
File	Message	Insert Options Format Text Review				
aste	🖌 Cut 🗎 Copy 🍠 Format Pa	・11 ・A* A* 三・三・ 受 B I U 砂・A・ 重 重 重 準律	Address Check Book Names	Q Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z	 Follow Up High Importance Low Importance 	Q Zoom
Cli	pboard	ra Basic Text ra	Names	Include	Tags 🗔	Zoom
	To ₂	spavicinf@mup				
= •	<u> </u>					
ente	Subject	proba				

Слика 9.

После креирања мејла изабрати **Options** где је потребно да дугме **Sign** буде укључено.

PROBA

Слика 10.

Притиснути дугме Send.

9 🖬 🖬	9 (° +	∞ -			proba - Message (HTML)	
File	Message	Insert	Options	Format Text Revie	w	
Aa Themes	Colors * A Fonts * Effects * Themes	Page Bcc Color * Sho	From w Fields	Permission	Use Voting Request a Read Receipt Buttons *	Save Sent Delay Direct Item To * Delivery Replies To More Options
	To <u>.</u>	<u>Sladjana Pavic</u>				
Send	<u>C</u> c					
20000	S <u>u</u> bject:	proba				

PROBA

Слика 11.

Након тога се захтева унос лозинке за личну карту.

Smart Card PIN	
<u>P</u> IN:	OK Cancel

mart Car	1 PIN		Ge	
<u>P</u> IN:	×××××*			1
		ОК	Cancel	
		ОК	Cancel	

Уношењем лозинке и притиском на дугме оК потписан мејл је послат.

Да мејл садржи дигитални потпис може се видети на основу иконице *која се налази у доњем десном углу мејла.* Кликом на ову иконицу може се проверити валидност потписа. За проверу валидности потписа неопходно је да на рачунару буде инсталиран ланац сертификата MUPCARoot и MUPCAGradjani и да се може приступити CRL листи.

From: Sladjana Pavic Signed By: spavicinf@mup	
Signed By: spavicinf@mup	
The dated states as the concerns to the date of the set way	
	isted.
For more information about the certificate used to d the message, click Details.	igitally sign
	etails
Warn me about errors in digitally signed e-mail before messa	ige opens.

2. Потписивање у Outlook Express-у

За потписивање email-ова у Outlook Express-у потребно је подесити Account на следећи начин.

Из менија одабрати Tools/Accounts...

Затим Internet Accounts/ Properties

У следећем прозору одабрати Security, а затим Select...

aeneral	Servers	Connection	Security	Advanced	
Signing	certificate	,		C.	
Selec ID us	t the sign ed when :	ing certificate l signing messag	below. This ges with thi	: will determi s account.	ne the digital
Certifi	icate:				Select)
Encrypti	ing prefere	ences —			
Selec	t the enci	ryption certifica	ate and alg	orithm. Thes aes so othe	e are rs can send
encry	pted mail	to you with the	ese settings	—	
encry Certifi	ipted mail	to you with the	ese settings		Select
Certifi Algori	ipted mail icate: ithm:	3DES	ese settings		Select
Certifi Algori	icate: ithm:	3DES	ese settings		Select
Certifi Algori	icate: ithm:	3DES	ese settings	(Select

Извршити избор сертификата и кликнути ОК.

Из менија одабрати Tools/Options/Security. Чекирати опције као на слици.

😭 Options			? ×							
General R Spelling	ead Receipts Security	Send Co Connection	mpose Signatures Maintenance							
Virus Protection Select the Internet Explorer security zone to use: Internet zone (Less secure, but more functional) Bestricted sites zone (More secure) Warn me when other applications try to send mail as me. Do not allow attachments to be saved or opened that could potentially be a virus. Download Images Block images and other external content in HTML e-mail										
Secure Mail Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions. Tell me more To digitally sign messages or receive encrypted messages, you must have a digital ID. Digital IDs Encrypt contents and attachments for all outgoing messages Encrypt contents and attachments for all outgoing messages										
OK Cancel Apply										

Кликнути на Advanced...

У следећем прозору извршити чекирање као на слици.

Advanced Security Settings								
Encrypted messages								
<u> </u>	Warn on encrypting messages with less than this strength:							
	168 bits							
	Always encrypt to myself when sending encrypted mail							
Digitally	Signed messages							
Ö	✓ Include my digital ID when sending signed messages							
-	Encode message before signing (opaque signing)							
	Add senders' certificates to my address book.							
Revoca	tion Checking							
	Check for revoked Digital IDs:							
<u>,</u>	Only when online							
	○ Never							
	OK Canc	el						

Након тога Account је подешен за потписивање порука. Пре слања поруке потребно је притиснути **Sign**

👔 New Message											_	
	<u>F</u> ile	<u>E</u> dit	⊻iew	Insert	F <u>o</u> rmat	<u>T</u> ools	<u>M</u> essa	ge <u>H</u> elp				_ 🥂
	=		Ж		G	5	<u></u>	ABC	Û	↓! 🤇		×
_	Send		Cut	Сору	Paste	Undo	Check	Spelling	Attach	Priority	Sign	

или из менија изабрати Tools/Digitally Sign.

👔 New I	Mess	age							_	
File	Edit	View	Insert	Format	Tools	Message	Help			
		X		P I	Spel	ling		F7		»
Send		Cut	Сору	Paste U	Req	uest Read R	Sign			
From: spavicinf@mup (mail1.mup)		Che Sele	ck Names ct Recipient«	Ctrl+K		•				
🛐 To:	Í				bbA	ress Book		Ctrl+Sbift+B		
🛐 Cc:	Γ				Eper	vot		Carronnero		
Subject	: [Digit	ally Sign				
					Req	uest Secure	Receipt			
			<u> </u>			<u>x 0</u>	<u>- 5</u>			

На тај начин је порука потписана и спремна за слање.