Лабораториска вежба 9	**Безбедна email комуникација**		
Име и презиме	Индекс	Група	Датум

Целта на оваа лабораториска вежба е да се запознаеме со два начина на кои можеме да постигнеме безбедна email комуникација преку потпишување и шифрирање на пораките.

Првиот начин кој ќе го разгледаме е S/MIME, кој нуди широка поддршка за огромен број на email клиенти, а пак вториот е PGP (Pretty Good Privacy). Иако ја имаат истата функција, овие два стандарди имаат некои фундаментални разлики, со кои ќе се запознаеме во текот на изработката на вежбата. Дополнително, PGP не ужива толку широка поддршка кај email клиентите, па најчесто е потребно да се инсталираат додатоци или трети апликации за да се овозможи работата со овој стандард.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) стандардот е опишан во RFC8551. Она што го нуди S/MIME е безбедна email комуникација која се базира на приватни и јавни клучеви, каде идентитетот на корисникот е потврден од страна на трета страна - certificate authority. Со цел да ви биде издаден ваков S/MIME сертификат, вие мора да го потврдите вашиот идентитет, а нивото на проверки кои мора да бидат направени зависат од тоа каков сертификат барате. Па така, за сертификати кои ќе се користат за лична употреба и се бесплатни, најчесто е доволно само потврда за сопственост на email адресата, додека пак за сертификати за комерцијална употреба кои се асоцирани со домен на фирма, потребно е верификација на сопственост на фирмата.

Во делот кој следи ќе се користи Microsoft Outlook и Mozilla Thunderbird за демонстрација на начинот на издавање и користење на S/MIME сертификатот.

Во случај да користите оперативен систем на кој не е поддржан Office пакетот, слободно можете да продолжите со користење на соодветен email клиент за таа платформа, откако ќе се уверите дека има поддршка за S/MIME. Mozilla Thunderbird е најчесто добар избор, но треба да се земе предвид дека во тој случај ќе мора да се најавите со вашиот личен email, а не со студентскиот.

Напомена: Изберете само еден клиент по ваша желба во делот за S/MIME и продолжете ја работата со него.

Најава на Microsoft Outlook

За да ја додадете вашата студентска email адреса во Outlook, потребни се следниве чекори:

- Изберете File -> Add Account.
- Во полето кое ќе ви се појави, внесете ја единствено вашата студентска email адреса.
- Во прозорецот за дополнителни информации за автентикација, како корисничко име внесете „broj_indeks@students.finki.ukim.mk“, додека пак како лозинка вашата CAS лозинка со која се најавувате и на останати сервиси на ФИНКИ, како на пример Courses. Доколку не сакате да бидете прашувани за лозинката при секое стартување на програмата, изберете „Remember my credentials“.

- По ова вашата email сметка треба да е додадена и целосно функционална, а тоа може да го тестирате со испраќање на порака на самите себеси.

Најава на Mozilla Thunderbird

За да ја додадете вашата email адреса во Microsoft Thunderbird, потребни се следниве чекори:

1. При првото стартување на Mozilla Thunderbird, по инсталацијата, ќе бидете прашани за внес на email сметка и лозинка. Доколку веќе имате инсталирано Mozilla Thunderbird, тогаш изберете го „хамбургер“ менито во горниот десен агол, Options -> Account Settings -> Account Actions (Долен лев агол) -> Add mail account.
2. Внесете ја вашата **приватна** email адреса **(не факултетската, не е поддржана)**. Потребните сервери за примање и праќање на пораки би требало автоматски да бидат пополнети.
3. По ова вашата email сметка треба да е додадена и целосно функционална, а тоа може да го тестирате со испраќање на порака на самите себеси.

Издавање на S/MIME сертификат

Неколку certificate authorities нудат издавање на бесплатни S/MIME сертификати. Еден таков пример е https://extrassl.actalis.it/portal/uapub/freemail?lang=en. Листа со дополнителни опции за S/MIME сертификати може да најдете на http://kb.mozillazine.org/Getting_an_SMIME_certificate.

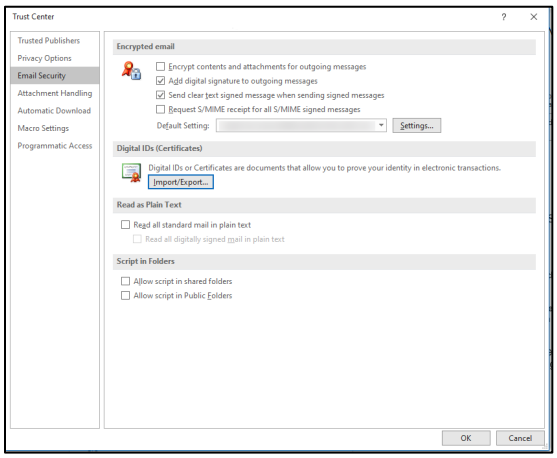
1. Посетете ја https://extrassl.actalis.it/portal/uapub/freemail?lang=en и аплицирајте за издавање бесплатен S/MIME сертификат.
2. На прикажаната форма внесете ја само својата email адреса за која сакате да биде издаден сертификатот.
3. Треба да добиете email со потврда кој ќе содржи уникатен код. На овој начин, како што беше спомнато и во воведот, certificate authority врши валидација на сопственост на email адресата.
4. Откако ќе го внесете клучот, ќе ви биде дадена лозинка со која ќе може да го импортирате сертификатот во вашиот оперативен систем, а пак самиот сертификат ќе ви биде пратен во .zip датотека во посебна email порака.

Импортирање на S/MIME сертификатот во Microsoft Outlook

По преземањето на .zip датотеката која го содржи сертификатот и нејзиното отпакување, следете ги следниве чекори со цел да го импортирате во Microsoft Outlook и да го подготвите за понатамошно користење:

1. Изберете File -> Options. Од левата страна изберете го Trust Center менито.
2. Trust Center Settings … -> Email Security. На екранот кој ќе ви се појави, изберете Import/Export во Digital IDs (Certificates) подгрупата, наведете ја локацијата на сертификатот и лозинката која ја добивте при валидација на сопственоста на email сметката.

3. По импортирање на сертификатот, осигурајте се дека опцијата „Add digital signatures to outgoing messages“ е штиклирана (слика бр. 1).



Слика 1: Нагодувања за S/MIME сертификат

4. Со ова треба да е завршен процесот на конфигурација. Доколку сè е во ред, можете да го тестирате вашиот потпис со испраќање на порака на некоја ваша email адреса. Многу email сервиси покажуваат визуелна потврда на некој начин во случај кога дадена порака е потпишана. Доколку вашиот email сервис не го прави тоа, секогаш можете преку View Source опцијата да ги видите сите заглавја на email пораката. Доколку е присутно заглавјето „Content-Type: multipart/signed;“ во тој случај вашиот потпис функционира како што треба (слика бр. 2).

```
x-ms-exchange-transport-forked: True
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature";
MIME-Version: 1.0
X-OriginatorOrg: students.finki.ukim.mk
```

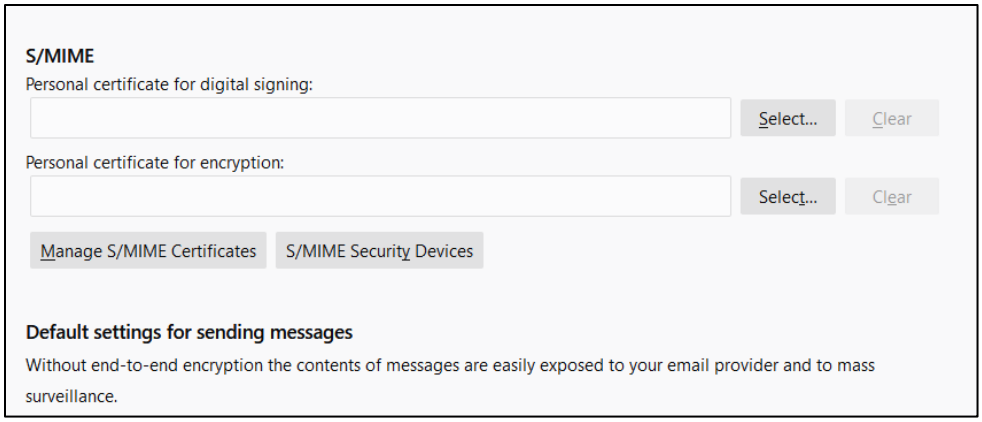
Слика 2: Email загјалвје кое потврдува дека пораката е потпишана

5. Како последен чекор од овој дел, на вашиот асистент испратете му S/MIME потпишана порака со наслов „[KMIB-LAB] SMIME-<BR_INDEKS>“.

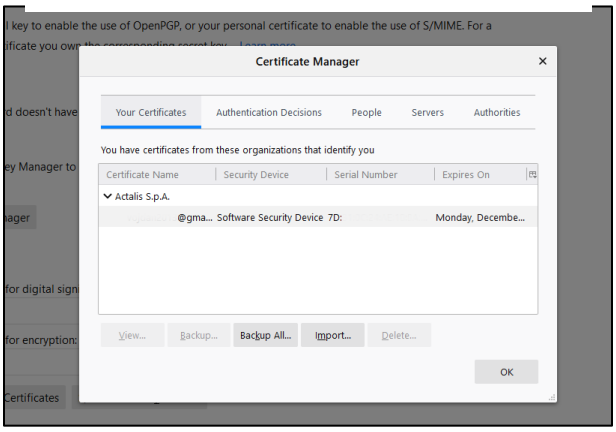
Импортирање на S/MIME сертификатот во Mozilla Thunderbird

По преземањето на .zip датотеката која го содржи сертификатот и нејзиното отпакување, следете ги следниве чекори со цел да го импортирате во Mozilla Thunderbird и да го подготвите за понатамошно користење:

- Изберете го „хамбургер“ менито во горниот десен агол, Options -> Account Settings.
- Изберете го „End-To-End encryption“ менито за вашата email сметка и кликнете на „Manage S/MIME Certificates“ (слика бр. 3).
- Одете во „Your Certificates“ табот и импорирајте го отпакуваниот сертификат кој го добивте како атачмент на вториот email, притоа внесувајќи ја лозинката која ви беше дадена при издавање на сертификатот (слика бр. 4).



Слика 3: Security мени за email сметката



Слика 4: Селектирање на преходно импортираниот сертификат

- Во S/MIME од претходната „End-to-End-Encryption“ секција, изберете го новиот сертификат (слика бр. 4) за *„Personal certificate for digital signing“* и *„Personal certificate for encryption“*.
- При прашањето дали сакате да го користите истиот сертификат за енкрипција и декрипција на пораки пратени до вас, изберете Yes.
- За крај, штиклирајте ја опцијата „Add my digital signature“ by default.
- Со ова треба да е завршен процесот на конфигурација. Доколку сè е во ред, можете да го тестирате вашиот потпис со испраќање на порака на некоја ваша email адреса. Многу email сервиси покажуваат визуелна потврда на некој начин во случај кога дадена порака е потпишана. Доколку вашиот email сервис не го прави тоа, секогаш можете преку View Source опцијата да ги видите сите заглавја на email пораката. Доколку е присутно заглавјето „Content-Type: multipart/signed;“ во тој случај вашиот потпис функционира како што треба.
- Како последен чекор од овој дел, на вашиот асистент испратете му S/MIME потпишана порака со наслов „[KMIB-LAB] SMIME-<BR_INDEKS>“.

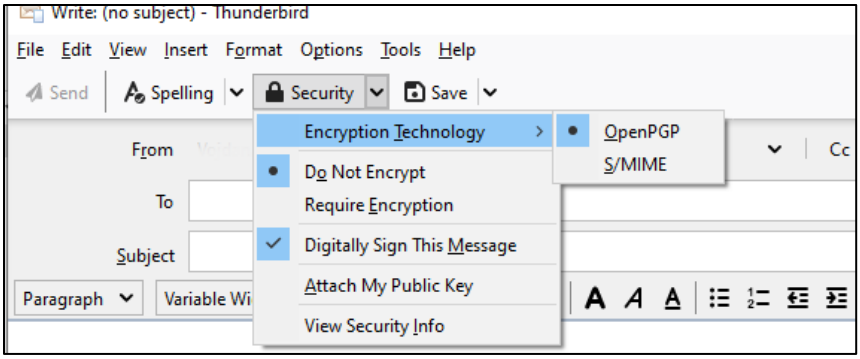
PGP

Во вториот дел на вежбата, целта ќе биде да изгенерираме PGP јавен и приватен клуч, кој потоа ќе може да ги користиме за потпишување и шифрирање на пораки. За разлика од S/MIME, PGP не се потпира на централен авторитет кој треба да го потврди идентитетот на корисникот преку потпишување на сертификатот, туку корисниците сами си ги објавуваат своите јавни клучеви на т.н. key servers (https://keyserver.ubuntu.com/, http://keys.gnupg.net/...) . Во случај кога сакате да испратите шифрирана порака на некое лице за кое не го знаете јавниот клуч, голема е веројатноста дека клучот бил јавно објавен и споделен на некој key server. Без разлика на кој key server вие иницијално ќе го објавите вашиот клуч, тој ќе биде достапен на сите останати преку процес на синхронизација меѓу различните сервери.

PGP е опишан во RFC4880. За креирање и употреба на PGP клучевите ќе користиме Mozilla Thunderbird, email клиент кој работи на сите популарни оперативни системи (https://www.thunderbird.net/en-US/).

Подготовка на работната околина

1. Доколку во првиот дел од вежбата користевте Microsoft Outlook и немате инсталирано Mozilla Thunderbird, направете го тоа сега и следете го упатството за додавање на вашата сметка во email клиентот. Повторно важи истото предупредување, **треба да користите приватна email сметка, а не факултетската, бидејќи не е поддржана**.
2. Mozilla Thunderbird во најновата верзија доаѓа со вградена поддршка за PGP, па не е потребна инсталација на екстра додатоци. Во случај да работите со стара верзија на Thunderbird или ажурирајте ја или преземете го додатокот Enigmail.
3. Откако ќе ја додадете вашата сметка во Thunderbird и ќе проверите дека можете успешно да испраќате пораки, одете во „Account Settings“ менито, во „End-To-End Encryption“ секцијата. Кликнете на *„Add Key“* копчето во OpenPGP подсекцијата.
4. Ќе бидете прашани дали сакате да увезете постоечки клуч или пак да генерирате нов. Изберете ја опцијата за генерирање на нов клуч.
5. Добра безбедносна практика е клучевите да траат што е можно пократко, за во случај на крадење или губење на клучот, напаѓачот да нема голема временска рамка во која би можел непречено да го користи. Во полето за избор на времетраење на клучот, внесете 1 година. Од паѓачкото мени „Key size“ изберете 4096. Останатите полиња оставете ги на нивните предефинирани вредности и кликнете на синото копче „Generate key“.
6. Процесот на генерирање на клучот може да потрае неколку минути за кое време прозорецот може да изгледа како да е замрзнат. Стрпливо почекајте и не ја исклучувајте програмата.
7. По креирањето на клучот, може да го тестирате потпишувањето на пораки користејќи го PGP методот со пишување на нов email. Внимавајте, доколку и во претходниот чекор на вежбата го користевте Mozilla Thunderbird како email клиент за испраќање на S/MIME потпишани пораки, во овој момент може да ги користите и двата метода – вие треба да изберете кој го преферирате. За таа цел, од прозорецот за пишување на нова порака изберете ја „Security“ опцијата и како „Encryption Technology“ штиклирајте„ OpenPGP“ (слика 5).



Слика 5: Избирање на метод за потпишување и шифрирање

8. Доколку сакате да го прикачите вашиот јавен клуч на некој од key server-ите, тоа можете да го сторите со одење во хамбургер менито -> Account Settings -> End-To-End Encrpytion -> OpenPGP Key Manager. Кликнете со десен клик на вашиот клуч и одберете „Copy Public Keys to Clipboard“. Потоа, посетете ја https://keyserver.ubuntu.com/ страницата, одберете „Submit Key“ и внесете го претходно копираниот јавен клуч.
9. Пробајте да си испратите самите на себеси порака, треба да имате визуелен приказ откако ќе ја примите, кој потврдува дека email-от е навистина потпишан (слика 6).
10. Испратете PGP потпишана порака до вашиот асистент со наслов „[KMIB-LAB] PGP-<BR_INDEKS>“.

Слика 6: Потврда дека дадена порака е потпишана