

Cyberbezpieczeństwo

Laboratorium 2

## Szyfrowanie poczty - S/MIME

W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.

0

Taki symbol oznacza, że trzeba w sprawozdaniu dodać zrzut ekranu (najczęściej 1) z wyniku działania polecenie.

Taki symbol oznacza, że należy dodać opis (najczęściej 1 zdanie) z wyniku działania polecenia.

# Wstęp

Protokół S/MIME, obsługiwany przez wszystkie główne aplikacje poczty elektronicznej, umożliwia wysyłanie podpisanych i/lub zaszyfrowanych wiadomości, chroniąc w ten sposób pocztę elektroniczną pod dwoma ważnymi względami:

- **poufność** wysłana wiadomość nie może zostać przechwycona przez nieuprawnione osoby, ponieważ nie może zostać odszyfrowana, a tym samym odczytana tylko przez zamierzonych odbiorców;
- **autentyczność i integralność** odbiorca może zweryfikować autentyczność nadawcy oraz czy wiadomość nie została zmieniona po wysłaniu.



Źródło: https://trustzone.com/news/what-is-s-mime/

## I. Przygotowanie środowiska pracy

1. Przygotuj maszynę wirtualną z systemem Windows.

Ta instrukcja opiera się na systemie Windows 10, ale oczywiście, możesz również przygotować środowisko według własnych preferencji.

- 2. Zainstaluj klienta pocztowego Mozilla Thunderbird.
- 3. Połącz się ze swoim kontem pocztowym.

$\boxtimes$		Studiaj	≡ -	ø ×
A	🌳 🕂 Nowa wiado 🚥	Et st_cyber@prz.edu.pl	(Q) Ustaw	vienia konta
	V De test_cyber@prz.edu.pl	🕲 Przeczytaj wiadomości 🖋 Napisz nową wiadomość 🔍 Wyszukaj wiadomości iłł Zarządzij filtrami wiadomości 🎤 Scyfrowanie "end-to-end"		
Q	<ul> <li>Wysłane</li> <li>Niechciane</li> </ul>	Skonfiguruj następne konto		
	<ul> <li>ickale fokery</li> <li>ickale</li></ul>	🖻 Poczta 🔋 Książka adresowa 📑 Kalendarz 🖓 Komunikator 🧬 Sernis przechowywania plików 🐊 Aktualności 🔮 Grupy dyskusyjne		
		Import z innego programu		
		Thunderbird umożliwia zaimportowanie wiadomości, wpisów książki adresowej, substopycji aktualności, ustawień i filtów z innych programów pocztowych i popularnych formatów książek adresowych.		
		Importuj		
		O programie Mozilia Thunderbird		
		Thunderbird to viodacy micetyputiformovy liken poechy i kalendraze pene source, bezeletny dia prodetlepionti viuty usohistos, Concern, aly nadad by bezierczy jest z dia unodliwi nam zatrudnienie programistów, opłacenie infrastruktury i kontynuowanie ulepszania programu.		
		Więcej informacji		
		Pomos     Polesz do nas     Dekumentacja dla programistów		
© ©				
-	(**) <i>P</i> Wpisz tutaj, aby wyszukać	🗮 🛚 📃 🚊 🖨 🗢 💿	스 탑 예 <sub>11</sub>	18:49 .10.2024

## II. Certyfikat S/MIME firmy Actalis

Actalis oferuje certyfikaty S/MIME zaufane na wszystkich głównych platformach i obsługiwane przez aplikacje pocztowe zgodne ze standardem S/MIME. Dzięki certyfikatom Actalis S/MIME możesz sprawić, że Twoja poczta e-mail będzie naprawdę bezpieczna, niezależnie od funkcji usługi poczty e-mail, z której korzystasz. Actalis zapewnia różne usługi certyfikatów S/MIME zgodnie z różnymi obowiązującymi zasadami.

- 1. Certyfikat należy pobrać ze strony: <u>https://extrassl.actalis.it/portal/uapub/freemail?lang=en</u>
  - a. W pierwszym kroku należy zarejestrować się na stronie. Następnie wybierz Continue with activation

What are th	ne next steps?	
To proceed with activation is essential to verify your	n, enter an email address to asso email address to complete the ac	ciate with the certificate. It trivation process.
1	2	3
Enter the email to verify	Click on the verification link you receive via email	Install the certificate in your email client
Continue with activation	n	

b. W kolejnym kroku wpisz adres e-mail, dla którego chcesz wygenerować certyfikat, a następnie wyślij go do weryfikacji.

# Attiva il tuo certificato Per quale email vuoi chiedere la verifica? Inserisci l'indirizzo email che desideri verificare. Insert an email address Conditions of supply of SSL server and code signing certificates Securer and Code Signing certificates Information on the processing of personal data Verify

c. W kolejnym kroku powinno to wyglądać jak poniżej.

HOSTING SERVER CLOUD SSL	Q	English v D @ test_cyber@prz.edu.pl
ACTALIS Products • Resou	urces and support 👻 Company Contact us	European Certification Authority and member of the CAB Forum
Customer area / Dashboard Customer area		test_cyber@prz.edu.pl 쥔 Logout
Dashboard	Your certificates:	
ACCOUNT SETTINGS	S/MIME - Mail Validated • verity Certificate status	
Owner profile     Change password	Complete the required checks, we will keep you informed of the outcome and any subsequent steps.	⑦ What do I have to do now?
Payment methods	Associated email: test_cyber@prz.edu.pl	O     O     Verify Active Expiring Expired

d. Przejdź do swojej poczty, aby zweryfikować meila.

Dear test_cyber@prz.edu.pl,
We have received a request to issue an Actalis S/MIME certificate to this email address.
Please verify that this email is correct by confirming it at the following link:
Confirm email
By installing and using the certificate, you are agreeing to <u>Actalis' terms of</u> use
Thank you for choosing our services.
Kind regards
The Actalis team

- e. Po krótkiej chwili powinieneś otrzymać kod weryfikacyjny na podany adres e-mail,
- f. W tej chwili powinieneś już móc pobrać swój klucz.

S/MIME - Mail Validated • Active	
Expiration: 11/10/2025	
Associated email: test_cyber@prz.edu.pl	
Download file .p12	Ocertificate revocation

## 2. Importowanie i eksportowanie certyfikatu.

a. Otrzymany certyfikat nalży zaimportować systemu. W tym celu otwieramy certyfikat i postępujemy zgodnie z kreatorem.

		X
		🗧 😼 Kreator importu certyfikatów
		Kreator importu certyfikatów — Zapraszamy!
		Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.
		Certyfikat, wystawany przez u rząd certyfikacji, stanówi potwierdzenie tozsamoso użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń siedowych. Magazyn certyfikatów jest obszarem systemowym, w kłaświm przedokuwana o zwieńkiejsty nertyfikatów jest obszarem systemowym,
		Lokalizacia orzechowywania
		Bieżący użytkownik
		◯ Komputer lokalny
		Aby kontynuować, kliknij przycisk Dalej.
		Dalej Anuluj
b.	Zaznacz okienko Oznac	z ten klucz jako eksportowalny
		×
		🗧 🧈 Kreator importu certyfikatów
		Ochrona klucza prywatnego
		W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.
		Weier back dis kluera provatago
		hipsz hasio do kacza pryma kgo.
		Hasło:
		•••••
		Wyświetl hasło
		Opcje importu:
		Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez policienie w przez
		apinauyę. ✓ Oracz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykonanie kopii zapasowej lub transport kluczy.
		Chroń klucz prywatny, używając zabezpieczeń opartych na wirtualizacji
		mieckadortowalne) ☑ Dołącz wszystkie właściwości rozszerzone.
		Dalej Anuluj

c. Następnie należy wyeksportować certyfikat z kluczami w formacie PKCS # 12. W tym celu należy uruchomić Microsoft Management Console.



d. Następnie dodajemy nową przystawkę.

🚟 Konsola1 - [Katalog główny konsoli]										
-	Plik	Akcja	Widok	Ulubione	Okno	Pomoc				
•		Nowa Otwórz Zapisz Zapisz ja	iko		Ctrl+N Ctrl+O Ctrl+S	2				
		Dodaj/U Opcje 1 perfmo	suń przys on.msc	tawkę	Ctrl+M					
		Zakończ	:							

#### e. W kolejnym kroku dodaj przystawkę zarządzania certyfikatami.

Dodawanie lub usuwanie przystawek

Możesz wybrać przystawki dla tej konsoli spośród przystawek dostępnych na komputerze i skonfigurować wybrany zestaw przystawek. Dla przystawek rozszerzalnych możesz określić, które rozszerzenia mają być włączone.

Dostępne przystawki:				Wybrane przystawki:		
Przystawka	Dostawca	^		Katalog główny konsoli	Edytuj rozszerzenia	
Certyfikaty	Microsoft Corp			Certyfikaty - bieżący użytkownik	112	
Edytor obiektów zas	Microsoft Corp				Usun	
🚞 Folder	Microsoft Corp					
👸 Foldery udostępnione	Microsoft Corp				Przenieś w góre	
🕒 Harmonogram zadań	Microsoft Corp					
🚡 Konfiguracja i analiz	Microsoft Corp				Przenieś w dół	
🛁 Kontrolka ActiveX	Microsoft Corp		Dodaj >			
🔮 Link do adresu intern	Microsoft Corp					
🌆 Menedżer autoryzacji	Microsoft Corp					
📕 Menedżer urządzeń	Microsoft Corp					
🔊 Monitor wydajności	Microsoft Corp					
le Monitor zabezpiecze	Microsoft Corp					
🛃 Podgląd zdarzeń	Microsoft Corp					
🗃 Sterowanie usługą	Microsoft Corp				Zaawansowane	
E Szahlony zahaznieczeń	Microsoft Corn	~		< >>	Zaanansomane	

#### f. Następnie wybierz wcześniej zaimportowany certyfikat i wyeksportuj go.



#### g. Postępujemy zgodnie z kreatorem wybierając opcje eksportu klucza prywatnego



×

## 3. Konfiguracja programu pocztowego.

a. Uruchom Mozilla Thunderbird i kliknij Ustawienia, a następnie Szyfrowanie "end-to-end".

🗟 Odebrane - test_cyber@prz.edu.pl	Ronfiguracja kont	x
✓ ☑ test_cyber@prz.edu.pl	Konfiguracja kon Nazwa konta: test_cyber@prz.edu.p Domyślna tożsamoś Poniższe dane określaja	ta - test_cyber@prz.edu.pl Kolor:
Szyfrowanie "end-to-end"	Imię i nazwisko:	Michał
Potwierdzenia Szyf	frowanie "end-to-end"	test_cyber@prz.edu.pl
<ul> <li>Lokalne foldery</li> <li>Niechciana poczta</li> </ul>	Zwrotny adre <u>s</u> e-mail:	inny adres, na który odbiorcy wiadomości powinni wysyłać odpowiedzi
Miejsce na dysku	<u>F</u> irma/Organizacja:	
🕼 Poczta wychodząca	Sygnatur <u>k</u> a:	Używaj <u>H</u> TML (np. <b>pogrubiony tekst</b> )

b. Przewiń okno do sekcji S/MIME kliknij Zarządzaj certyfikatami S/MIME.

S/MIME		
Certyfikat osobisty do podpisywania cyfrowego:		
	Wybier <u>z</u>	Wy <u>c</u> zyść
Certyfikat osobisty do szyfrowania:		
	Wybi <u>e</u> rz	W <u>y</u> czyść
Zarządzaj certyfikatami S/MIME		

c. Wybierz zakładkę Użytkownik, a następnie Importuj....

Menedżer certyfikatów											
Użytkownik	Decyzje uwierzyte	elniania	Osoby	Serwery	organy	certyfikacji					
Masz identyfikujące	Masz identyfikujące certyfikaty z następujących organizacji:										
Nazwa certyfikatu	u Urządzenie	zabez	Numer se	ryjny	Wygasa d	nia	E.				
Wyświetl	<u>&lt;</u> opia zapasowa…	K <u>o</u> pia zap	pasowa wszy	stkich	I <u>m</u> portuj	<u>U</u> suń					
							ок				

d. Znajdź swój certyfikat S/MIME w formacie PKCS#12 lub PFX, a następnie kliknij przycisk Otwórz.

Plik certyfikatu do zaimportowania										
$\leftrightarrow \rightarrow \cdot \uparrow$	→ ↑ Ten komputer > Pulpit Przeszukaj: Pulpit									
Organizuj 🔻 🛛 N	lowy folder				== -	?				
	Naz	wa	Data modyfikacji	Тур	Rozmiar					
Pulpit Pobrane Dokumenty Cbrazy	* * *	certificate_s_mime	11.10.2024 19:20	Wymiana informa	7 KB					
<ul> <li>OneDrive</li> <li>Ten komputer</li> <li>Sieć</li> </ul>										
	Nazwa pliku:	certificate_s_mime		V Pliki PKC	rz Anuluj	~				

e. Podaj hasło, które otrzymałeś wcześniej w meilu.

~

X
ertyfikatu:
Anuluj
Usuń
ОК

f. Powinieneś teraz móc przeglądać szczegóły swojego pliku certyfikatu S/MIME w Menedżerze certyfikatów. Kliknij ok, aby kontynuować.

-		Menedżer o	ertyfikatów			
Użytkownik	Decyzje uwierzyteln	iania O	soby Sei	wery C	rgany certyfikacji	
Masz identyfikujące	e certyfikaty z następuja	ących organiz	acji:			
Nazwa certyfikatu	u Urządzenie za	bez N	lumer seryjny	Wy	gasa dnia	E.
∨ Actalis S.p.A.						
test_cyber@	prz.e Urządzenie zab	ezpiecz 53	:5E:A4:CA:E2:68	:39:16 sobo	ta, 11 październik	
Wyświetl	(onia zanasowa	Konia zanasi	owa wszystkich	Import	ui Usuń	
<u>wy</u> swieti			owa wszystkich.		<u>o</u> sum	_
						ОК

g. W sekcji S/MIME kliknij przycisk wybierz..., aby wybrać certyfikat do podpisywania cyfrowego i szyfrowania.

#### S/MIME

Certyfikat osobisty do podpisywania cyfrowego:	 _	
	Wybier <u>z</u>	Wy <u>c</u> zyść
Certyfikat osobisty do szyfrowania:		
	Wybi <u>e</u> rz	W <u>y</u> czyść

h. Kliknij przycisk ok.

wybierz c	путікат				
Certyfikat:	test_cyber@prz.ed	lu.pl [53:5E:A4:CA:I	E2:68:39:16:95:	26:00:BC:A2	:4D:4C:E9] 🗸
Szczegóły w	ybranego certyfikatu	:			
Wystawion 53:5E:A4:C Ważny od E-mail: tes Wystawion Pietro,ST=E Przechowyw	· dla: CN=test_cyber( A:E2:68:39:16:95:26:0( piątek, 11 październił t_cyber@prz.edu.pl · przez: CN=Actalis C ergamo,C=IT vany w: Urządzenie za	©prz.edu.pl D:BC:A2:4D:4C:E9 (a 2024 do sobota, ' 'lient Authenticatio abezpieczające	11 października n CA G3,0=Act	2025 alis S.p.A.,L=	Ponte San

i. Pojawi się okno komunikatu z następującą treścią. Kliknij Tak, aby potwierdzić, że będziesz używać tego samego certyfikatu do szyfrowania wiadomości e-mail.

🍯 Thund	erbird	×
?	Zanim będzie możliwe cyfrowe podpisywanie wiadomości, należy określić certyfikat, który będzie używany przez inne osoby przy wysyłaniu szyfrowanych wiadomości do użytkownika tego konta. Czy użyć tego samego certyfikatu do szyfrowania i deszyfrowania wiadomości wysyłanych do użytkownika tego konta?	
	<u>I</u> ak <u>N</u> ie	

j. Pola dla podpisywania cyfrowego i szyfrowania zostaną automatycznie wypełnione danymi Twojego certyfikatu. W sekcji "Domyślne ustawienia wysyłania wiadomości" możesz włączyć lub wyłączyć szyfrowanie nowych wiadomości oraz podpisywanie niezaszyfrowanych wiadomości.

S/MIME		
Certyfikat osobisty do podpisywania cyfrowego:		
test_cyber@prz.edu.pl [53:5E:A4:CA:E2:68:39:16:95:26:00:BC:A2:4D:4C:E9]	Wybier <u>z</u>	Wy <u>c</u> zyść
Certyfikat osobisty do szyfrowania:		
test_cyber@prz.edu.pl [53:5E:A4:CA:E2:68:39:16:95:26:00:BC:A2:4D:4C:E9]	Wybi <u>e</u> rz	W <u>y</u> czyść
Zarządzaj certyfikatami S/MIME		
Aby uzyskać nowy osobisty certyfikat S/MIME, wygeneruj żądanie podpisania certyfikatu (CSR) i p certyfikacji (CA). <u>Więcej informacji</u>	rześlij je do orga	inu
Wygeneruj i zapisz plik CSR jako		
Domyślne ustawienia wysyłania wiadomości		
Wyłącz szyfrowanie nowych wiadomości		
🔿 Włącz szyfrowanie nowych wiadomości		
Będzie można wyłączać szyfrowanie dla poszczególnych wiadomości.		

k. Po ustawieniu preferencji możesz teraz używać swojego certyfikatu S/MIME do podpisywania i szyfrowania wiadomości e-mail w programie Thunderbird.

# III. Zadanie do wykonaniaCertyfikat S/MIME firmy Actalis

Zanim przystąpisz do wykonania zadania upewnij się, że certyfikat jest prawidłowo zaimplementowany.

- 1. Kliknij przycisk + Nowa wiadomość.
- Skomponuj swój e-mail, wypełnij pole Temat, a następnie wpisz adres e-mail odbiorcy w tym wypadku wyślij meil do samego siebie. Po dodaniu adresu kontaktu, Thunderbird powiadomi Cię, czy szyfrowanie jest możliwe. Kliknij przycisk Zaszyfruj, aby zaszyfrować wiadomość email.

Tworzenie: test — Thunderbird	- 🗆 ×
Jik <u>E</u> dycja <u>W</u> idok W <u>s</u> taw <u>F</u> ormat <u>O</u> pcje <u>B</u> ezpieczeństwo <u>N</u> arzędzia Pomo <u>c</u>	- //
🛙 Wyślij 📓 Zaszyfruj 🕕 S//MIME 🗸 💩 Pisownia 🗸 さ Zapisz jako 🗸 圏 Adresy	🕖 Załącz 🗸
Nagawca Michał <test_cyber@prz.edu.pl><math>test_cyber@prz.edu.pl \lor</math> Kopia Ukryta kopia <math>\gg</math></test_cyber@prz.edu.pl>	
Do test_cyber@prz.edu.pl	
Temat test	
Akapit $\checkmark$ Zmienna szerokość $\checkmark$ 💭 $\neg$ T T+ T+ B $I$ $\sqcup$ $\land$ $\bowtie$ $\Xi$ $\Xi$ $\Xi$ $\boxtimes$ $\bowtie$ $\bowtie$ $\checkmark$	
est	

3. Oprócz szyfrowania możesz także podpisać cyfrowo swoją wiadomość e-mail, klikając zakładkę S/MIME i zaznaczając opcję Podpisz cyfrowo.



 Po ustawieniu szyfrowania i/lub podpisu wiadomości e-mail kliknij wyślij. Thunderbird poprosi o potwierdzenie chęci użycia certyfikatu S/MIME do szyfrowania i/lub podpisywania. Kliknij przycisk οκ, aby potwierdzić.



5. Jeśli odbiorca będzie również korzystał z przeglądarki Mozilla Thunderbird do przeglądania Twojej wiadomości e-mail, będzie mógł zobaczyć, że wiadomość została podpisana i zaszyfrowana, klikając przycisk S/MIME.



### ZADANIE

Wyślij zaszyfrowanego i podpisanego maila na adres test cyber@prz.edu.pl

**UWAGA:** Jeśli planujesz wysłać zaszyfrowaną wiadomość e-mail, upewnij się, że posiadasz klucz publiczny odbiorcy. W przeciwnym razie pojawi się komunikat z opcją wysłania wiadomości w formie niezaszyfrowanej. Aby umożliwić szyfrowanie, poproś odbiorcę o przesłanie certyfikatu zawierającego jego klucz publiczny, który należy zaimportować do programu pocztowego. W przypadku korzystania z Thunderbirda wykonaj następujące kroki:

- Przejdź do Konfiguracja konta -> Szyfrowanie "end-to-end".
- Wybierz Zarządzaj certyfikatami S/MIME -> Osoby.
- Kliknij Importuj i wskaż otrzymany klucz publiczny \*.crt.

Po zakończeniu tych kroków, szyfrowanie wiadomości będzie możliwe.

0

0