

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



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:

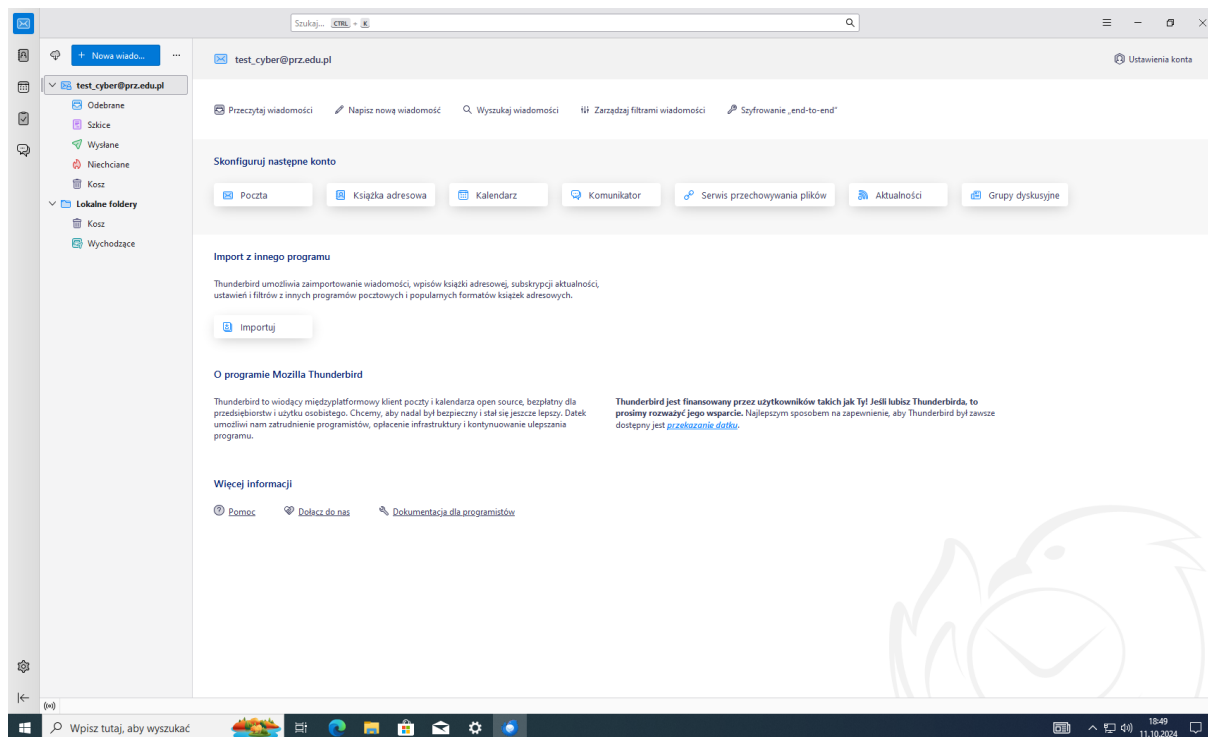
- **poufność** - wysłana wiadomość nie może zostać przechwycona przez nieuprawnione osoby, ponieważ nie może zostać odszyfrowana, a tym samym odczytana tylko przez zamierzonych odbiorców;
- **autentyczność i integralność** - odbiorca może zweryfikować autentyczność nadawcy oraz czy wiadomość nie została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



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

I. Przygotowanie środowiska pracy

1. Zainstaluj klienta pocztowego [Mozilla Thunderbird](#).
2. Połącz się ze swoim (uczelnianym) kontem pocztowym.



II. Certyfikat S/MIME firmy Actalis

Actalis oferuje certyfikaty S/MIME, które są zaufane na wszystkich głównych platformach i obsługiwane przez aplikacje pocztowe zgodne ze standardem S/MIME. Certyfikaty te zwiększają bezpieczeństwo, autentyczność oraz reputację firmowej poczty elektronicznej. Zapewniają ochronę poprzez poprawę prywatności i bezpieczeństwa transmisji danych oraz wymiany wiadomości e-mail. Wiadomości są podpisywane cyfrowo i szyfrowane, co pozwala odbiorcy zweryfikować integralność wiadomości oraz wiarygodność nadawcy — oba te elementy stanowią kluczowe kroki w ochronie przed atakami phishingowymi, złośliwym oprogramowaniem i innymi cyberzagrożeniami.

1. Certyfikat należy pobrać ze strony: <https://www.actalis.com>
 - a. W pierwszym kroku zarejestruj się na stronie.
 - b. Podczas rejestracji zaznacz opcję **No agree** przy wszystkich zgodach marketingowych.
 - c. Na podany przez Ciebie adres e-mail otrzymasz kod weryfikacyjny – użyj go, aby zakończyć proces rejestracji.
 - d. Po zalogowaniu się przejdź na stronę: <https://www.actalis.com/s-mime-certificates>
 - e. Jeden certyfikat na okres 1 roku jest bezpłatny. Aby kontynuować, należy wybrać opcję **PROCEED**



**Mailbox
Validated**

Certify your emails for free

Free / First year*
Renews at €6.00 + VAT / year

Quantity**

— 1 +

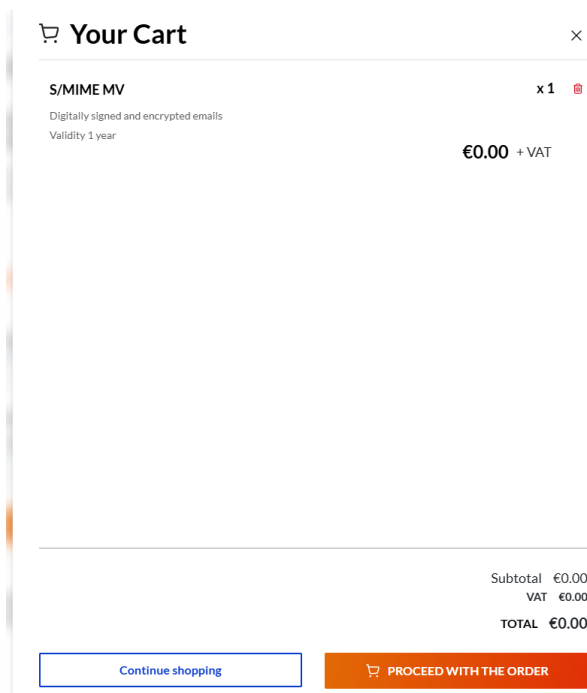
Duration***

Stay longer, save more.

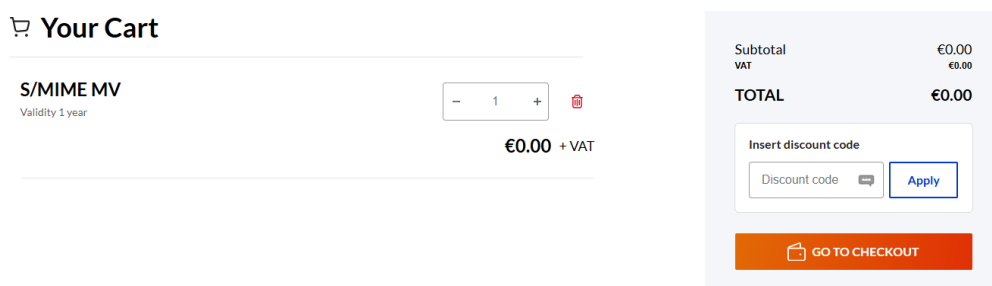
— 1 year +

PROCEED

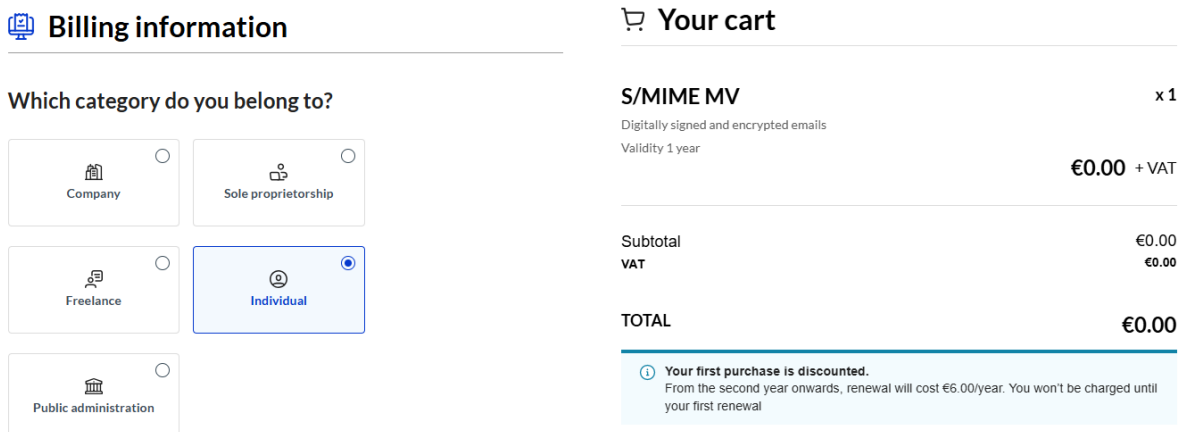
- f. Na tym etapie w koszyku znajduje się jeden certyfikat S/MIME MV o ważności 1 roku, który jest bezpłatny (0,00 €). Aby przejść dalej, należy kliknąć **PROCEED WITH THE ORDER**.



- g. Aby kontynuować proces zamówienia, kliknij przycisk **GO TO CHECKOUT**.



- h. Na tym etapie należy w sekcji Billing information wybrać kategorię **Individual** (Osoba prywatna). Poniżej musisz jeszcze podać podstawowe dane.



- i. Zaznaczyć oba pola zgody potwierdzające zapoznanie się i akceptację warunków („Conditions of supply...”), a następnie zatwierdzić transakcję.

Personal Information

Billing information

Payment

Your cart

S/MIME MV

Digitally signed and encrypted emails

Validity 1 year

€0.00 + VAT

Subtotal

VAT

TOTAL

€0.00

€0.00

€0.00

No payment method required.

Acceptance of terms and conditions

By selecting "Confirm and pay" I confirm that I have read the [Pre-contractual disclosure](#).

I confirm that I have read and expressly accept the [Conditions of supply for SSL Server Code Signing online and S/MIME certificates](#)

I confirm that I have read and expressly accept the clauses of the [Conditions of supply for SSL Server Code Signing online and S/MIME certificates](#)

Your first purchase is discounted.

From the second year onwards, renewal will cost €6.00/year. You won't be charged until your first renewal

- j. Kliknij **Activate** from your account, aby przejść do aktywacji certyfikatu i dokończyć jego konfigurację.

You have completed your purchase

We have emailed a summary email to: cyber_zsz@prz.edu.pl.

1x S/MIME MV (Validity: 1 year)

€0.00

Total without VAT

€0.00

VAT Total

€0.00

Total with VAT

€0.00

What to do next:

Review your order

Manage and track it from your account under Order history and invoices.

Order number:

Payment method:

Order placed by:

Email address

ACDAAGOKO

Michał test

cyber_zsz@prz.edu.pl

Activate your certificate

We've sent you a summary of your order by email. Log in to your account to complete configuration and activation.

Activate from your account

- k. W kolejnym kroku ekran powinien wyglądać jak poniżej – kliknij **Activate now**, aby rozpocząć aktywację certyfikatu.

Michał test

cyber_zsz@prz.edu.pl

Logout

Your certificates:

All (1)

Activation (1)

Certificate type

S/MIME Mailbox Validated

Sort by

Expiry Date (Newest First)

S/MIME - Mailbox Validated

Not yet activated

Update status

Validity 1 year

Certificate status

Start your certificate activation here

Activate now

Order n. ACDAAGOKO of 18/10/2025

Activation

To be verified

Active

Expiring

Expired

- l. Na tym etapie należy w polu **Email** wpisać adres, dla którego chcesz uzyskać certyfikat <- Twój uczelniany mail. Następnie kliknij przycisk **Verify**, aby wysłać prośbę o weryfikację adresu e-mail — na wskazany adres zostanie wysłany kod weryfikacyjny potrzebny do dalszej aktywacji certyfikatu.

Customer area

Michał test
cyber_zsz@prz.edu.pl
Logout

ACTIVATION PROCESS
S/MIME - Mailbox Validation
Validity 1 year



Request certificate

Which email do you want to request verification for?

Enter the email address you want to verify.

Email

cyber_zsz@prz.edu.pl

Verify

- m. Na tym etapie należy zapoznać się z warunkami korzystania z usługi - kliknij przycisk **Start verification**, aby rozpocząć proces weryfikacji adresu e-mail przez urząd certyfikacji.

Customer area

Michał test
cyber_zsz@prz.edu.pl
Logout

ACTIVATION PROCESS
S/MIME - Mailbox Validation
Validity 1 year



Request certificate

Terms and Conditions

Review your information and submit it to the Certification Authority for verification.

Email: cyber_zsz@prz.edu.pl

Terms and conditions

By continuing you accept the contract's Terms and Conditions.

[Terms and conditions for SSL Server Code Signing online and S/MIME certificates](#)

[Approval of clauses in the SSL Server Code Signing online and S/MIME certificate terms and conditions](#)

[Data Protection Policy](#)

Go back

Start verification

- n. Twoje żądanie wydania certyfikatu zostało pomyślnie przesłane do urzędu certyfikacji (Certification Authority). Aby zakończyć ten etap, kliknij **Back to Account**.

Customer area

Michał test
cyber_zsz@prz.edu.pl
Logout

ACTIVATION PROCESS
S/MIME - Mailbox Validation



Your certificate request has been submitted

We've forwarded your certificate details to the Certification Authority. You'll be notified as soon as the verification is completed.

A summary email has been sent to:

You'll receive a **confirmation email** once all necessary checks have been completed.

Email: cyber_zsz@prz.edu.pl

Back to Account

- o. Weryfikacja może potrwać kilka minut. Po zakończeniu weryfikacji otrzymasz wiadomość potwierdzającą (confirmation email) zawierającą dalsze instrukcje dotyczące aktywacji certyfikatu.

Michał test
cyber_zsz@prz.edu.pl
[Logout](#)

Your certificates:

All (1)

To be verified (1)

Certificate type

All

Sort by

Expiry Date (Newest First)

S/MIME - Mailbox Validated

To be verified

[Refresh verification status](#)

Validity 1 year

Certificate status

We are completing the necessary checks. We'll update you on the outcome and the next steps.

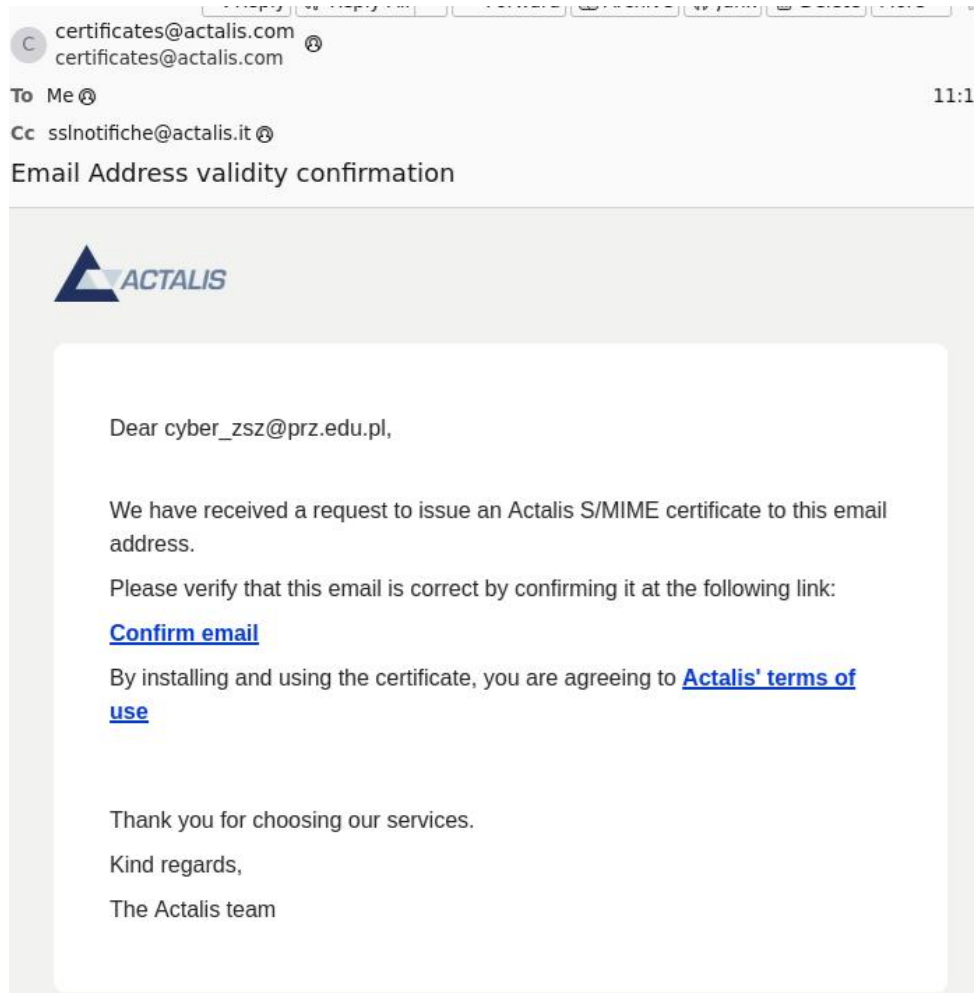
[What do I have to do now?](#)

Linked email: cyber_zsz@prz.edu.pl
Order n. ACDAAGOKO of 18/10/2025

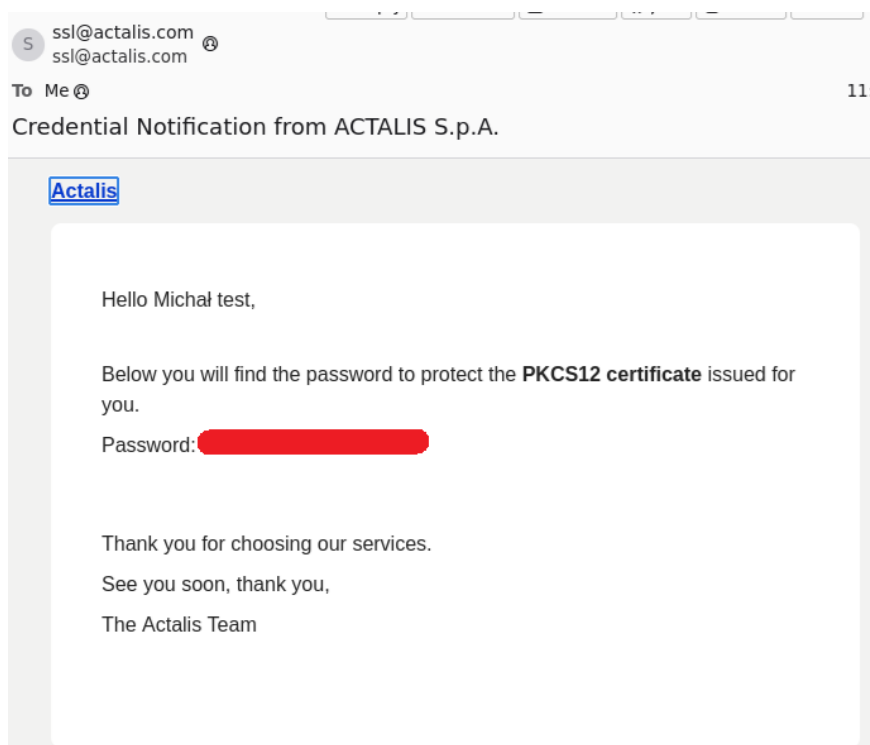
Activation To be verified Active Expiring Expired

[Delete certificate](#)

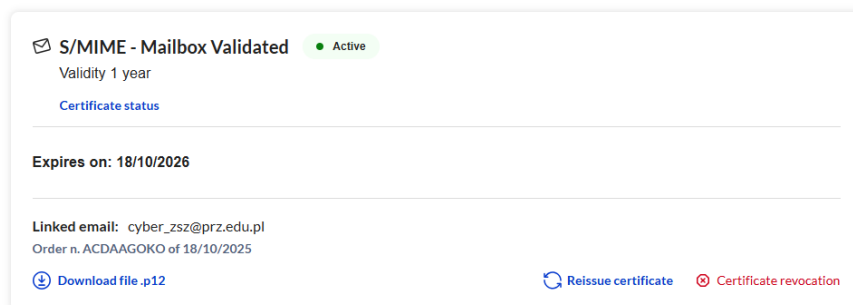
- p. W międzyczasie przejdź do swojej skrzynki pocztowej i potwierdź adres e-mail, klikając przycisk **Confirm email** w otrzymanej wiadomości.



- q. Po zakończeniu weryfikacji otrzymasz od Actalis nową wiadomość e-mail zawierającą hasło do pliku certyfikatu PKCS12, który został dla Ciebie wygenerowany. Hasło to będzie potrzebne podczas instalacji lub importu certyfikatu (np. w programie pocztowym lub przeglądarce).

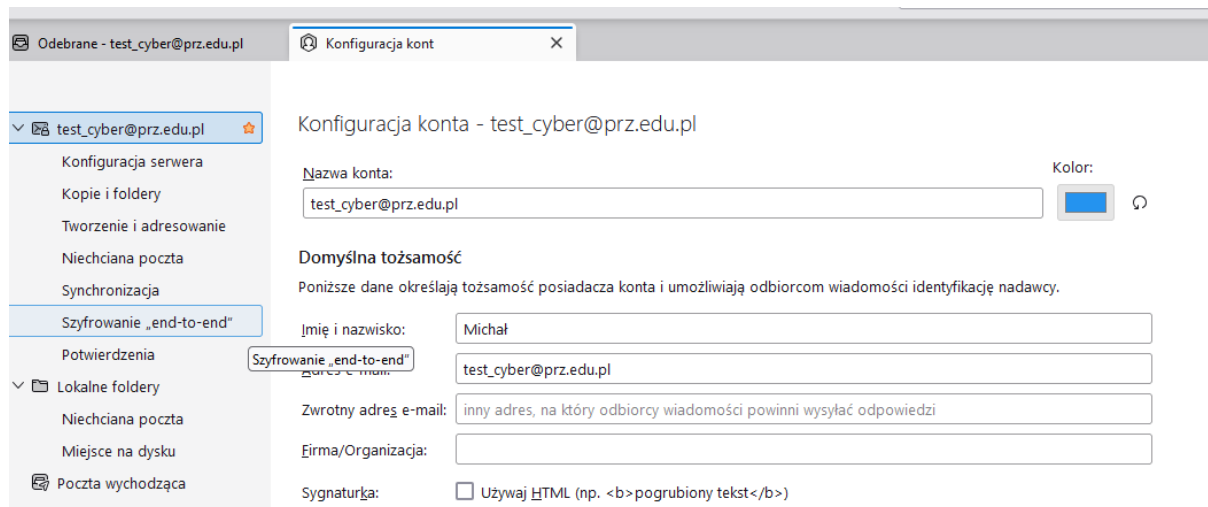


- r. Na tym etapie certyfikat S/MIME – Mailbox Validated został już aktywny i przypisany do Twojego adresu e-mail. Aby go pobrać, kliknij [Download file .p12](#).



2. Konfiguracja programu pocztowego.

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



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

S/MIME

Certyfikat osobisty do podpisywania cyfrowego:

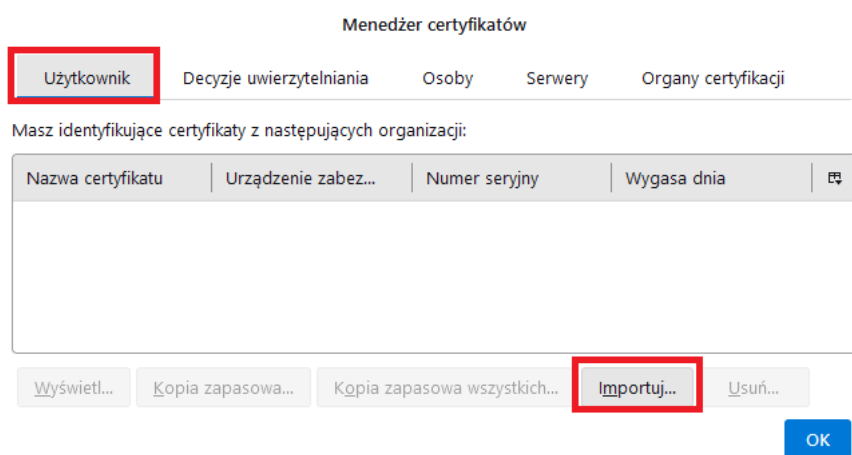
 Wybierz... Wyczyść

Certyfikat osobisty do szyfrowania:

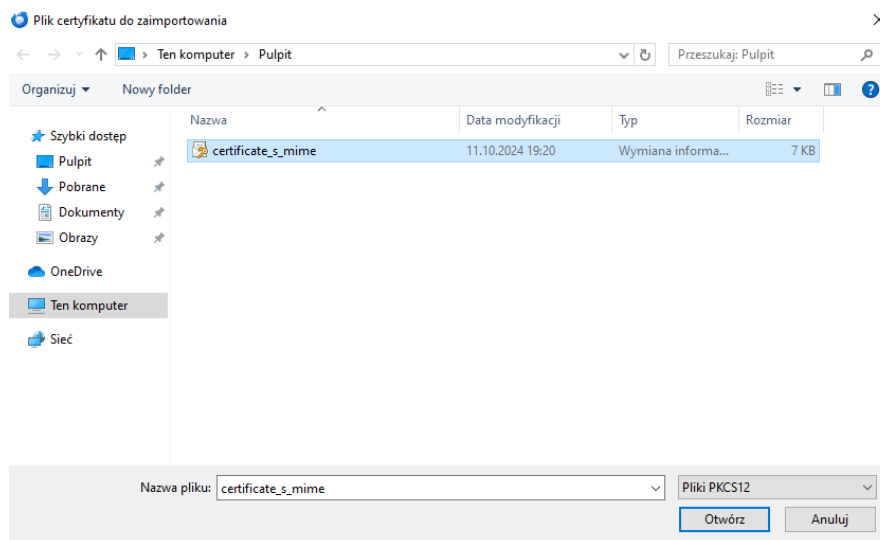
 Wybierz... Wyczyść

Zarządzaj certyfikatami S/MIME Urządzenia zabezpieczające S/MIME

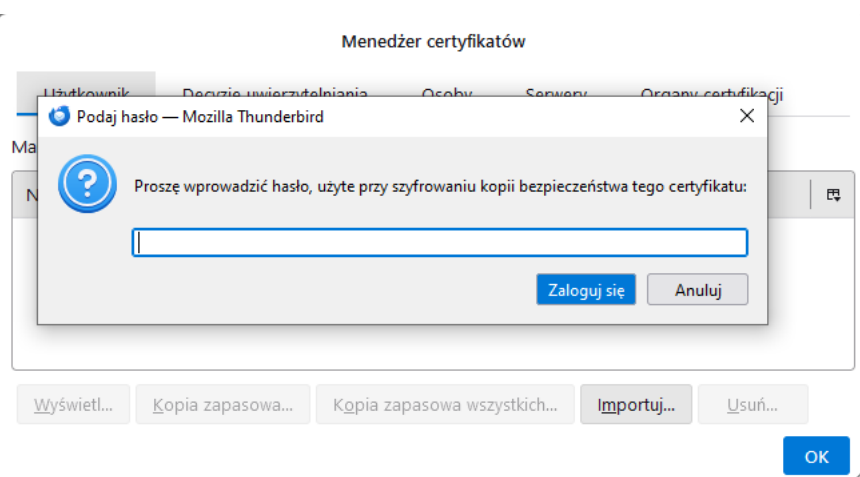
- c. Wybierz zakładkę Użytkownik, a następnie Importuj....



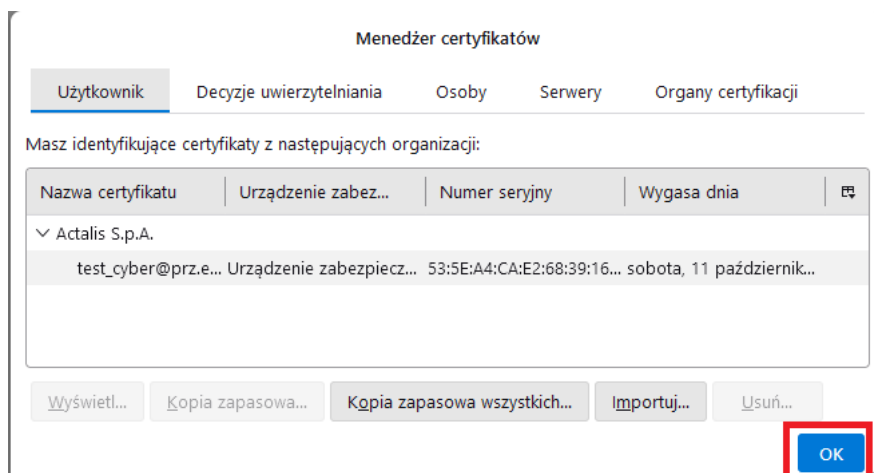
- d. Znajdź swój certyfikat S/MIME w formacie PKCS #12 (.p12), a następnie kliknij przycisk Otwórz, aby zaimportować go do programu.



- e. W kolejnym kroku podaj hasło, które otrzymałeś wcześniej w wiadomości e-mail od Actalis.



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



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

S/MIME

Certyfikat osobisty do podpisywania cyfrowego:

Wybierz...

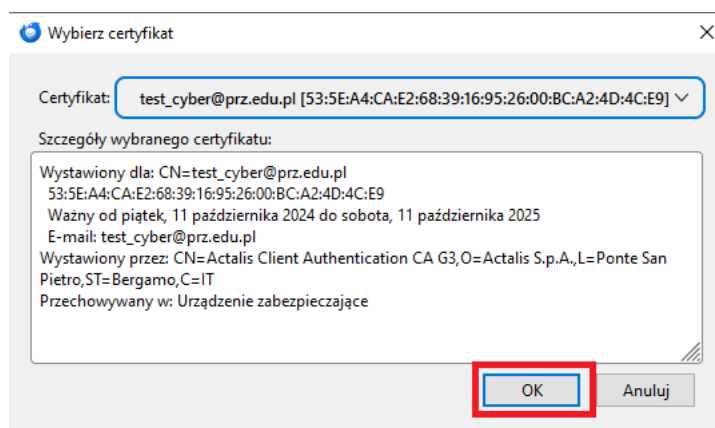
Wyczyść

Certyfikat osobisty do szyfrowania:

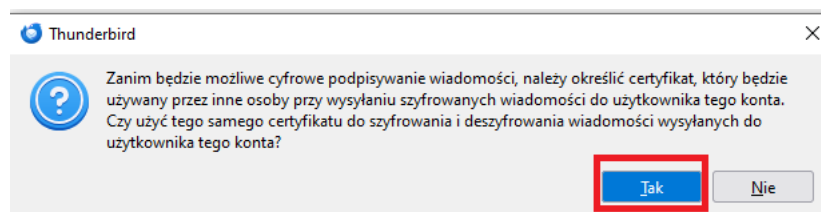
Wybierz...

Wyczyść

- h. Kliknij przycisk **OK**.



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



- 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]

Wybierz...

Wyczyść

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]

Wybierz...

Wyczyść

Zarządzaj certyfikatami S/MIME

Urządzenia zabezpieczające S/MIME

Aby uzyskać nowy osobisty certyfikat S/MIME, wygeneruj żądanie podpisania certyfikatu (CSR) i prześlij je do organu certyfikacji (CA).

[Więcej informacji](#)

Wygeneruj i zapisz plik CSR jako...

Domyślne ustawienia wysyłania wiadomości

☒ Wyłącz szyfrowanie nowych wiadomości

☐ Włącz szyfrowanie nowych wiadomości

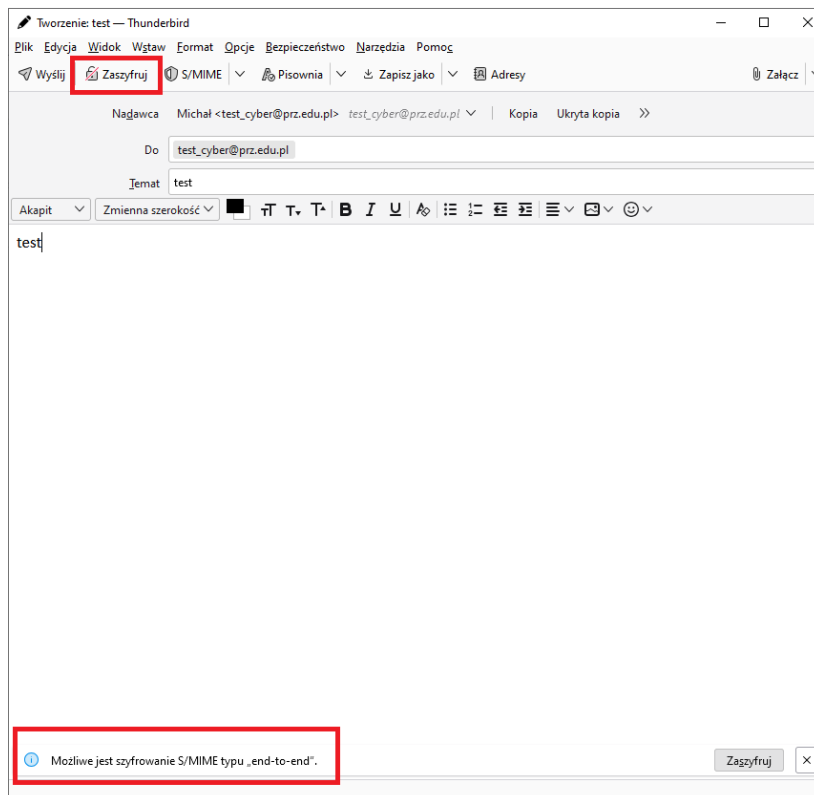
Będzie można wyłączać szyfrowanie dla poszczególnych wiadomości.

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

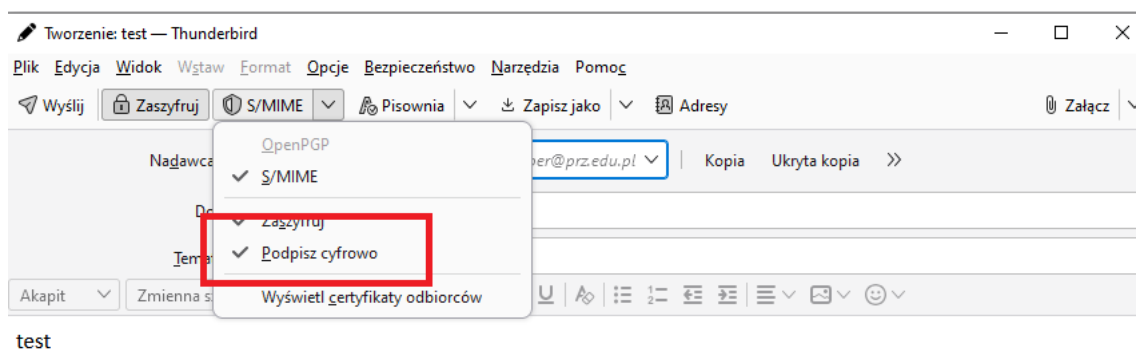
III. Zadanie do wykonania

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

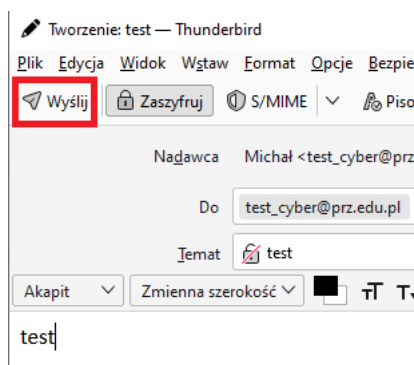
1. Kliknij przycisk + Nowa wiadomość.
2. Wygeneruj przykładową treść wiadomości, wypełnij pole Temat, a następnie wpisz adres e-mail odbiorcy – w tym wypadku wyślij meil do samego siebie. Po dodaniu adresu kontaktu, Thunderbird powiadomi Cię, czy szyfrowanie jest możliwe. Kliknij przycisk *Zaszyfruj*,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



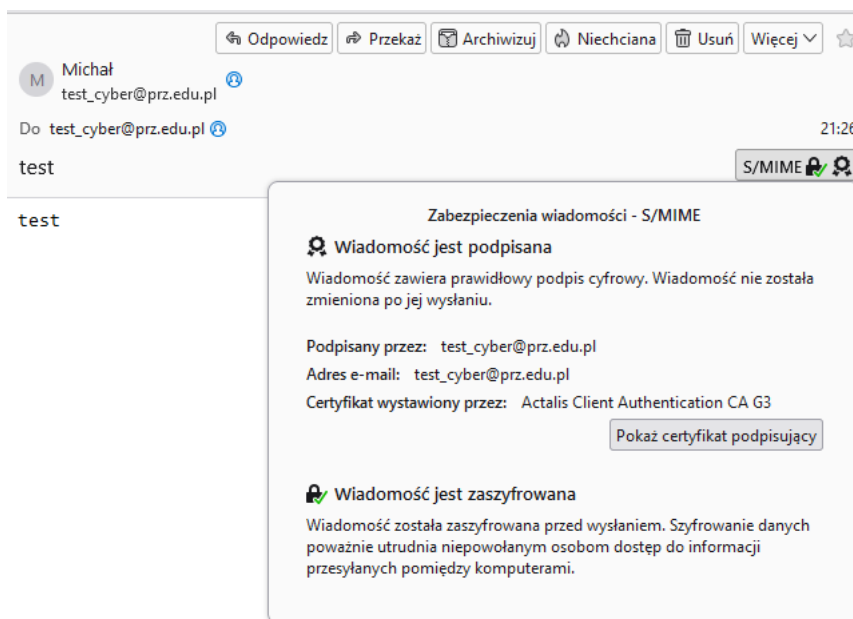
3. Oprócz szyfrowania podpisz cyfrowo swoją wiadomość e-mail, klikając zakładkę S/MIME i zaznaczając opcję Podpisz cyfrowo.



4. 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 OK, aby potwierdzić.



5. Jeśli odbiorca będzie również korzystać 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 **cyber_zsz@prz.edu.pl**

UWAGA: Aby możliwe było szyfrowanie wiadomości e-mail, obie strony muszą posiadać swoje klucze publiczne. W przeciwnym razie pojawi się komunikat z opcją wysłania wiadomości w formie tylko niezaszyfrowanej.

Wymiana tych kluczy odbywa się na jeden z dwóch sposobów:

1. Automatyczna wymiana przez podpisane wiadomości:

- Użytkownik A wysyła do użytkownika B wiadomość podpisaną cyfrowo.
- W podpisie automatycznie zawarty jest certyfikat z kluczem publicznym A.
- Użytkownik B, odbierając wiadomość, importuje klucz publiczny A do swojego programu pocztowego.
- Następnie B wysyła również podpisaną wiadomość – w ten sposób A otrzymuje klucz publiczny B.
- Od tego momentu obie strony mogą wymieniać zaszyfrowane i podpisane wiadomości.

2. Ręczna wymiana kluczy publicznych:

- Użytkownik udostępnia swój certyfikat publiczny (.cer / .crt) np. poprzez stronę internetową lub wiadomość e-mail.
- Druga strona importuje ten certyfikat do swojego programu pocztowego.
- Dzięki temu może natychmiast wysłać zaszyfrowaną i podpisaną wiadomość bez wcześniejszej wymiany podpisanych maili.

W skrócie:

- Podpisana wiadomość = przekazanie klucza publicznego.
- Zasyfrowana wiadomość = wymaga posiadania klucza publicznego odbiorcy.
- Klucz prywatny = zawsze pozostaje tylko u właściciela i nigdy nie jest udostępniany.

Do zadania wybierzemy opcję nr 2. 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 pobrany ze strony prowadzącego klucz publiczny *.crt.

Po zakończeniu tych kroków, szyfrowanie wiadomości do cyber_zsz@prz.edu.pl powinno być możliwe.