FINN Sp. z o.o.
NIP 8321912565
REGON 731586439
KRS 0000023991 Kapitał zakł. 1 400 000 PLN
Sąd Rej. Łódź-Śródmieście XX Wydział KRS

Adres kontaktowy – Oddział w Łodzi
93-490 Łódź, ul. Pabianicka 159/161
tel. (42) 206 66 00, (42) 684 98 91
fax (42) 684 98 92
sekretariat@finn.pl, http://www.finn.com.pl

FINNCA INS
Instrukcja dla subskrybentów

Historia zmian dokumentu:

Wersja	*Data publikacji*	*Data obowiązywania*	*Opis*
v1.0	19.02.2018	20.03.2018	Uruchomienie centrum certyfikacji FINN CA. Pierwsza wersja dokumentu zatwierdzona przez zarząd.

Spis treści

1. Wstęp

Niniejszy dokument to zbiór instrukcji i procedur postępowania dla najczęściej wykonywanych czynności przez Subskrybentów.

Inne informacje dotyczące Centrum Certyfikacji FINN CA są publikowane na stronie internetowej, dostępnej pod adresem **`http://ca.finn.pl`**.

2. Żądanie nowego certyfikatu użytkownika w systemie Windows

Procedura obejmuje wygenerowaniem żądania do FINN Enterprise CA, automatyczne wygenerowanie certyfikatu przez FINN Enterprise CA oraz jego samoczynne umieszczenie w magazynie użytkownika.

1. Otwórz Menedżera certyfikatów, klikając przycisk **Start**, wpisując w polu Wyszukaj polecenie *certmgr.msc*, a następnie naciskając klawisz **ENTER**. Jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.
2. Kliknij folder **Osobisty**.
3. W menu **Akcja** wskaż polecenie **Wszystkie zadania**, a następnie kliknij polecenie **Żądaj nowego certyfikatu**.
4. Okno informacyjne **Zanim rozpoczniesz.** Kontynuuj operację upewniając się, że komputer jest podłączony do sieci. Kliknij **Dalej**.
5. Okno **Wybierz zasady rejestracji certyfikatu**. Pozostawiamy wartości domyślne i klikamy **Dalej**.
6. Okno **Żądaj certyfikatów**. Wybieramy **FINN CA User**. Kliknij **Zarejestruj**.
7. Okno **Wyniki instalacji certyfikatów**. Po prawidłowym wygenerowaniu certyfikatu powinniśmy zobaczyć przy żądanym certyfikacie opis **STAN: Powodzenie**. Kliknij **Zakończ**.

3. Żądanie nowego certyfikatu komputera w systemie Windows

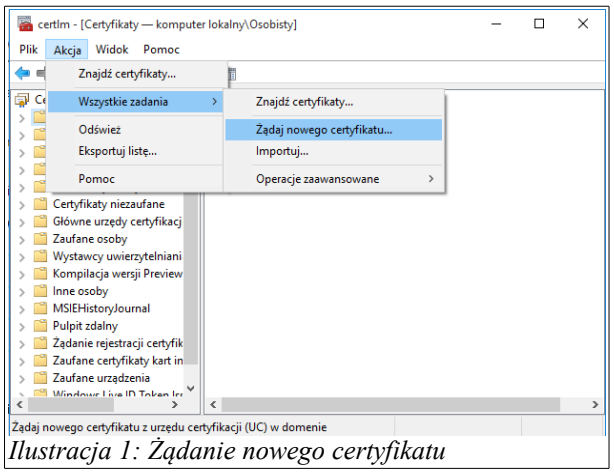
Procedura obejmuje wygenerowaniem żądania do FINN Enterprise CA, automatyczne wygenerowanie certyfikatu przez FINN Enterprise CA oraz jego samoczynne umieszczenie w magazynie komputera.

1. Otwórz Menedżera certyfikatów, klikając przycisk **Start**, wpisując w polu Wyszukaj polecenie *certlm.msc*, a następnie naciskając klawisz **ENTER**. Jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.

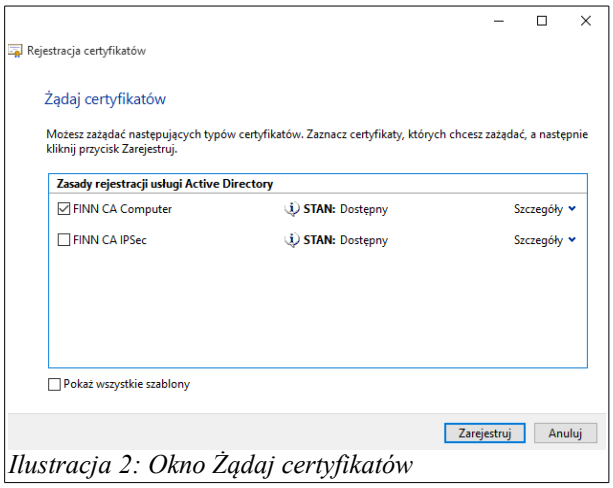
   Uwaga! W systemie Windows 7 powyższe polecenie nie działa. Aby uzyskać okno magazynu certyfikatów komputera musimy skorzystać z *Microsoft Management Console (MMC)*. Wpisz w polu Wyszukaj polecenie

mmc, a następnie naciśnij klawisz **ENTER**. W menu **Plik** wybierz **Dodaj/Usuń przystawkę**. Z dostępnych przystawek wybierz **Certyfikaty,** kliknij **Dodaj**. W oknie **Przystawka certyfikatów** wybierz **Konto komputera**, kliknij **Dalej**. W oknie **Wybieranie komputera** wybierz **Komputer lokalny,** kliknij **Zakończ**, a następnie w oknie **Dodawanie lub usuwanie przystawek** kliknij **OK.** Dalej kliknij w pole **Certyfikaty (Komputer lokalny)**

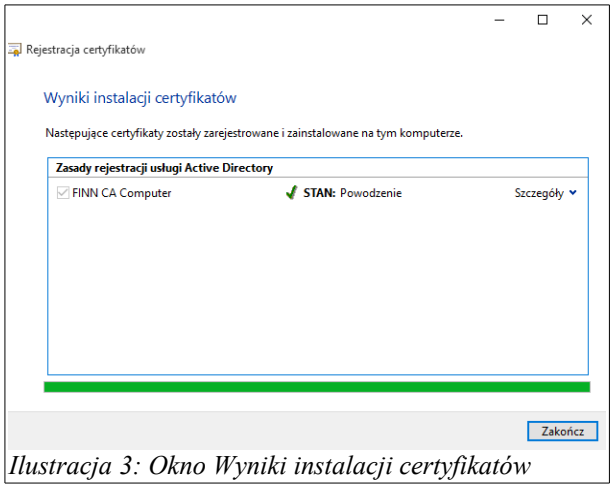
2. Kliknij folder **Osobisty**.
3. W menu **Akcja** wskaż polecenie **Wszystkie zadania**, a następnie kliknij polecenie **Żądaj nowego certyfikatu** (Ilustracja 1: Żądanie nowego certyfikatu).
4. Okno informacyjne **Zanim rozpoczniesz.** Kontynuuj operację upewniając się, że komputer jest podłączony do sieci. Kliknij **Dalej**.
5. Okno **Wybierz zasady rejestracji certyfikatu**. Pozostawiamy wartości domyślne i klikamy **Dalej**.
6. Okno **Żądaj certyfikatów**. Wybieramy **FINN CA Computer**. Kliknij **Zarejestruj** (Ilustracja 2: Okno Żądaj certyfikatów).
7. Okno **Wyniki instalacji certyfikatów**. Po prawidłowym wygenerowaniu certyfikatu powinniśmy zobaczyć przy żądanym certyfikacie opis **STAN: Powodzenie**. Kliknij **Zakończ** (Ilustracja 3: Okno Wyniki instalacji certyfikatów).



Ilustracja 1: Żądanie nowego certyfikatu



Ilustracja 2: Okno Żądaj certyfikatów

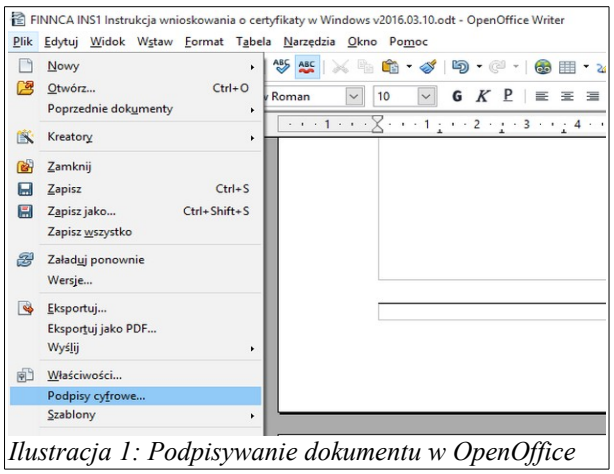


Ilustracja 3: Okno Wyniki instalacji certyfikatów

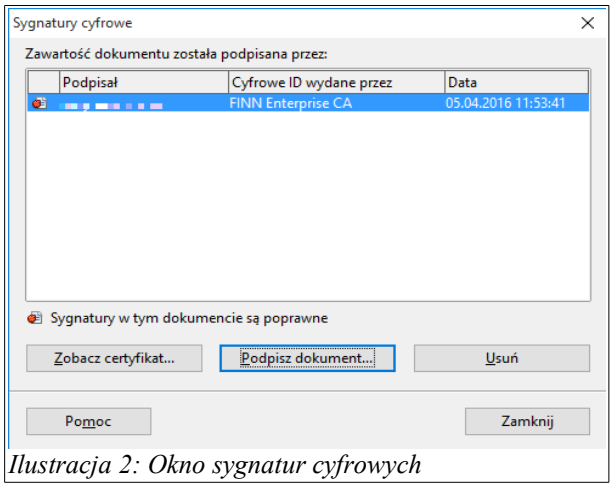
4. Podpisywanie dokumentów w pakiecie OpenOffice

Aby podpisać dokument w dowolnej aplikacji pakietu OpenOffice wykonujemy następujące kroki:

1. Z menu wybieramy **Plik**, a następnie **Podpisy cyfrowe**.
2. W oknie **Sygnatury cyfrowe** wybieramy **Podpisz dokument**. Następnie wybieramy nasz certyfikat i klikamy **OK**.



Ilustracja 1: Podpisywanie dokumentu w OpenOffice



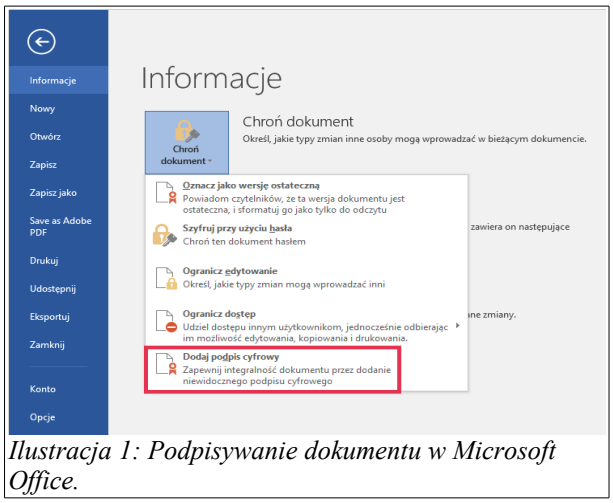
Ilustracja 2: Okno sygnatur cyfrowych

5. Podpisywanie dokumentów w pakiecie Microsoft Office

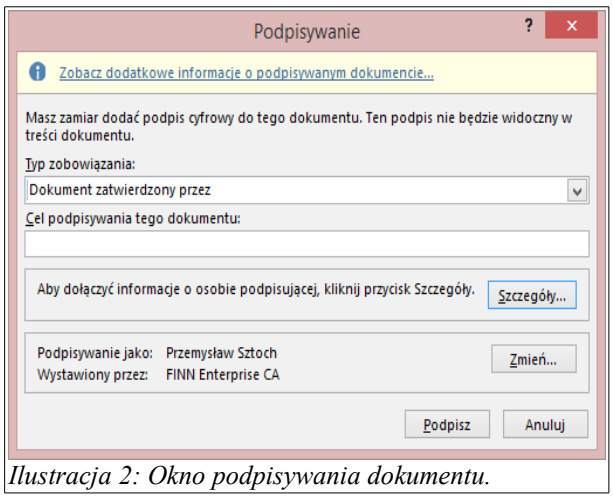
Aby podpisać dokument w dowolnej aplikacji pakietu Microsoft Word wykonujemy następujące kroki:

1. W edytowanym dokumencie z menu aplikacji wybieramy **Plik**.
2. Klikamy na pole **Chroń dokument**, a następnie **Dodaj podpis cyfrowy**.
3. W oknie **Podpisywanie** wybieramy *Tryb zobowiązania* oraz opcjonalnie możemy wpisać *Cel podpisywania dokumentu*. Do podpisu jest użyty domyślny certyfikat wyświetlony w dolnej części okna. Aby zmienić certyfikat klikamy **Zmień...**
4. Aby podpisać dokument klikamy **Podpisz**.

Inne aplikacje pakietu Office (np. Excel) mają bardzo podobne mechanizmy.



Ilustracja 1: Podpisywanie dokumentu w Microsoft Office.

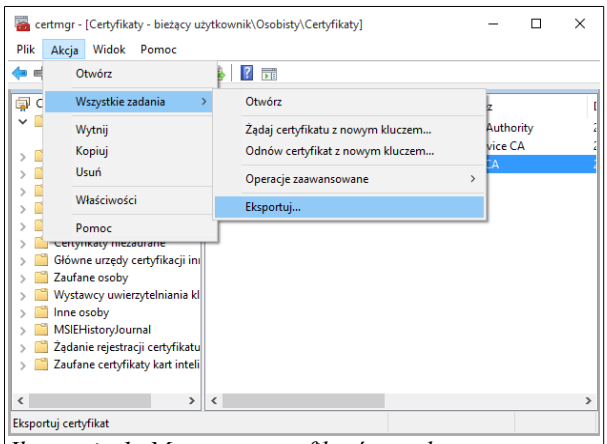


Ilustracja 2: Okno podpisywania dokumentu.

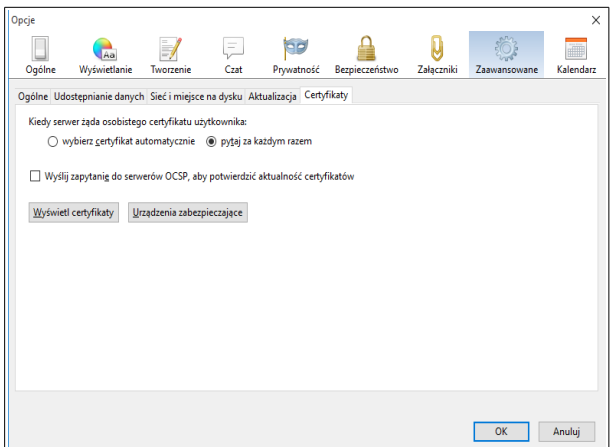
6. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Mozilla Thunderbird

Program Mozilla Thunderbird nie używa certyfikatów systemowych. Aby użyć certyfikatu należy wyeksportować go z magazynu systemowego a następnie zainstalować w aplikacji Mozilla Thunderbird. W tym celu wykonujemy następujące kroki:

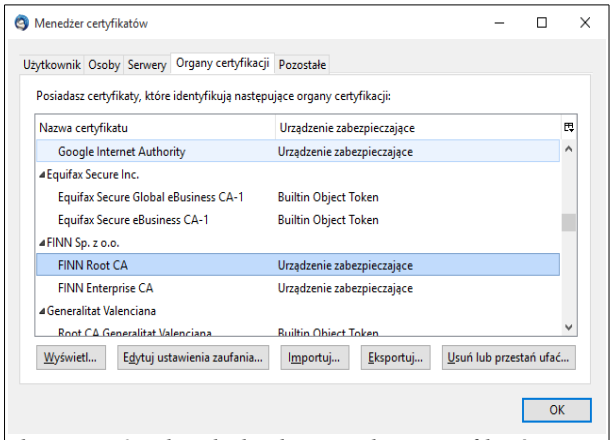
1. Otwórz Menedżera certyfikatów, klikając przycisk **Start**, wpisując w polu Wyszukaj polecenie *certmgr.msc*, a następnie naciskając klawisz **ENTER**. Jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.
2. Kliknij folder **Osobisty**, a następnie **Certyfikaty**. Wybieramy nasz imienny certyfikat.
3. W menu **Akcja** wskaż polecenie **Wszystkie zadania**, a następnie kliknij polecenie **Eksportuj...**
4. W oknie *Kreator eksportu certyfikatów* **Eksportowanie klucza prywatnego** zaznaczmy *„Tak, eksportuj klucz prywatny”*. Klikamy **Dalej**.
5. *W oknie Kreator eksportu certyfikatów* **Format pliku eksportu** w sekcji **Wymiana informacji osobistych - PKCS #12** zaznaczamy tylko *„Jeśli to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacyjnej”*. Klikamy **Dalej**.
6. *W oknie Kreator eksportu certyfikatów* **Zabezpieczenia** tworzymy hasło zabezpieczające certyfikatu. Klikamy **Dalej**.
7. *W oknie Kreator eksportu certyfikatów* **Eksport pliku** wpisujemy nazwę i ścieżkę zapisu naszego certyfikatu. Klikamy **Dalej**.
8. Finalizujemy eksport klikając **Zakończ**.
9. W programie Mozilla Thunderbird w menu aplikacji klikamy **Narzędzia**, a następnie **Opcje**.
10. W oknie **Opcje** wybieramy zakładkę **Zaawansowane**, poniżej klikamy zakładkę **Certyfikaty**. Klikamy pole **Wyświetl certyfikaty**.
11. W oknie **Menedżer certyfikatów** wybieramy zakładkę **Osoby**. Klikamy pole **Importuj**. Wybieramy certyfikat zapisany w ścieżce z *punktu 7*. Wpisujemy hasło utworzone w *punkcie 6*.
12. W oknie **Menedżer certyfikatów** przechodzimy na zakładkę Organy certyfikacji. Odnajdujemy certyfikat **FINN Root CA**. Klikamy pole **Edytuj ustawienia zaufania**. Wybieramy wszystkie sposoby użycia. Klikamy **OK**.
13. W oknie **Menedżer certyfikatów** klikamy **OK**. Zamykamy okno **Opcje** klikając **OK**.
14. Klikamy **Narzędzia**, a następnie **Konfiguracja kont**. Klikamy pole **Zabezpieczenia** w sekcji naszego konta pocztowego. Aby umożliwić podpisywanie i szyfrowanie wiadomości w polach **Podpis cyfrowy** i **Szyfrowanie wiadomości** wybieramy pole **Wybierz** i klikamy nasz zaimportowany certyfikat. Klikamy **OK**.
15. Aby podpisać edytowaną wiadomość klikamy pole **Zabezpieczenia** i wybieramy opcję **Podpisz cyfrowo tę wiadomość.**



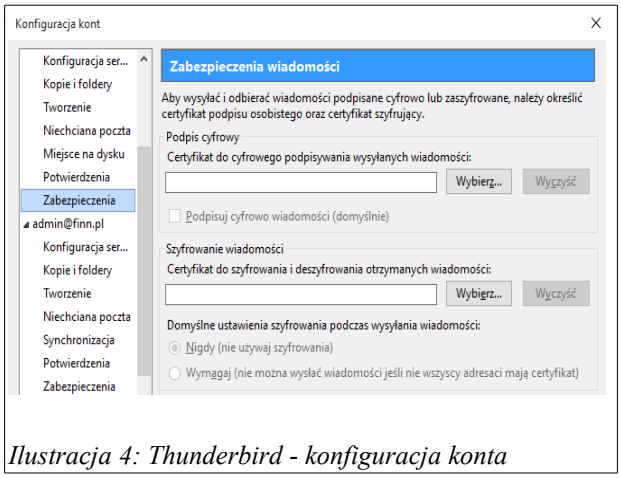
Ilustracja 1: Magazyn certyfikatów - eksport



Ilustracja 2: Thunderbird – wyświetl certyfikaty



Ilustracja 3: Thunderbird - menedżer certyfikatów

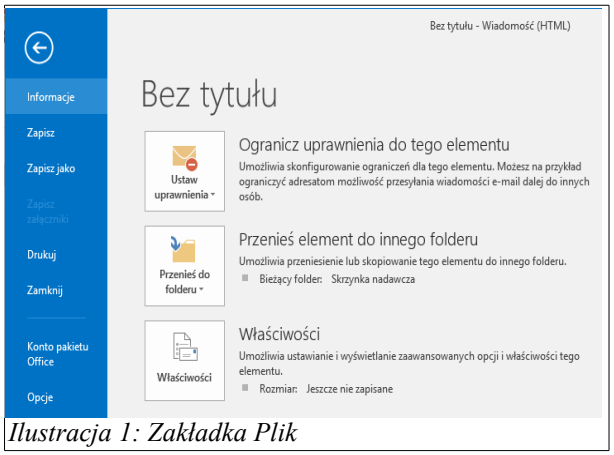


Ilustracja 4: Thunderbird - konfiguracja konta

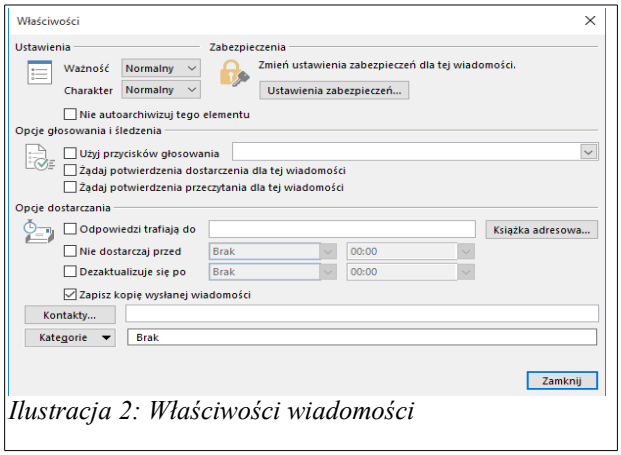
7. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Microsoft Outlook

Microsoft Outlook podczas podpisywania korzysta z certyfikatów z magazynu systemowego. Aby podpisać dokument w tej aplikacji należy wykonać następujące kroki:

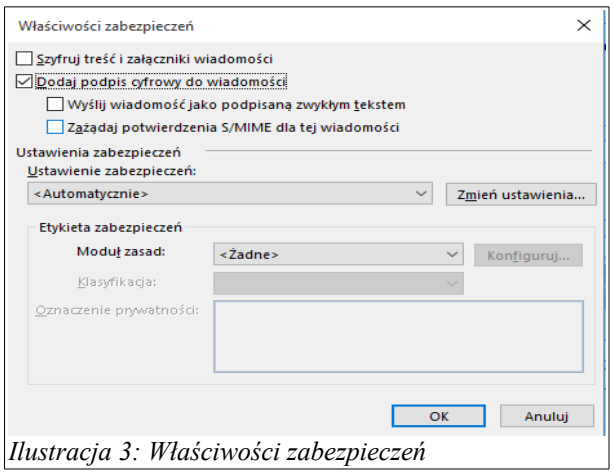
1. Podczas edycji wiadomości wybieramy z menu pozycję **Plik**, a następnie pole **Właściwości**.
2. W oknie **Właściwości** klikamy **Ustawienia zabezpieczeń**.
3. W oknie Właściwości zabezpieczeń zaznaczmy **Dodaj podpis cyfrowy** do wiadomości. Klikamy następnie pole **Zmień ustawienia**.
4. W oknie **Zmienianie ustawień zabezpieczeń** sprawdzamy czy w polu *Certyfikat podpisujący* jest nasz certyfikat. Możemy go zmienić wybierając sąsiadujące pole **Wybierz**.
5. Zatwierdzamy kolejno zmiany klikając **OK**. Nasza wiadomość podczas wysyłania zostanie podpisana.



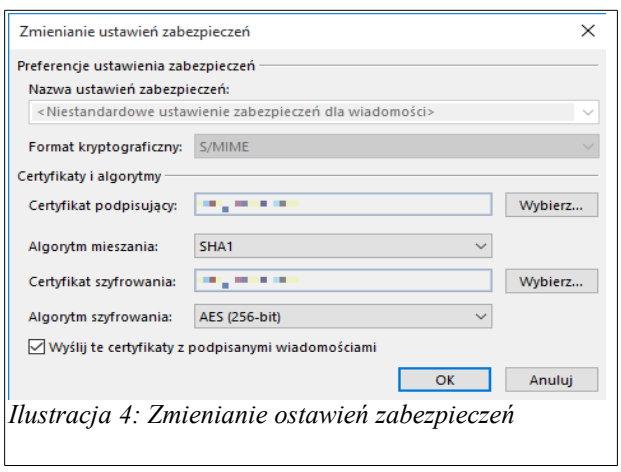
Ilustracja 1: Zakładka Plik



Ilustracja 2: Właściwości wiadomości



Ilustracja 3: Właściwości zabezpieczeń

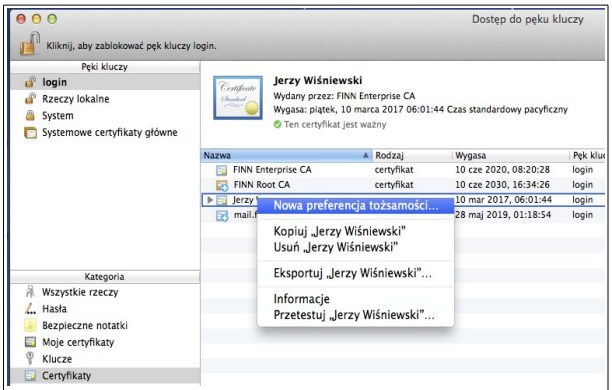


Ilustracja 4: Zmienianie ostawień zabezpieczeń

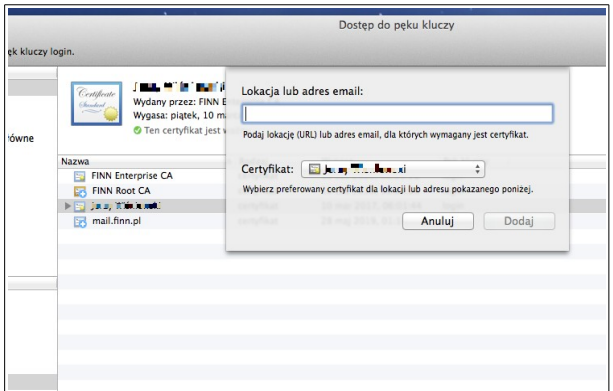
8. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Mail w systemie Apple OS X

Aby użyć certyfikatu w systemie OS X najpierw musimy go wyeksportować do pliku *.pfx lub *.p12 (procedura eksportu certyfikatu została opisana w rozdziale 6.) i wgrać do komputera. Dalej wykonujmy następujące kroki:

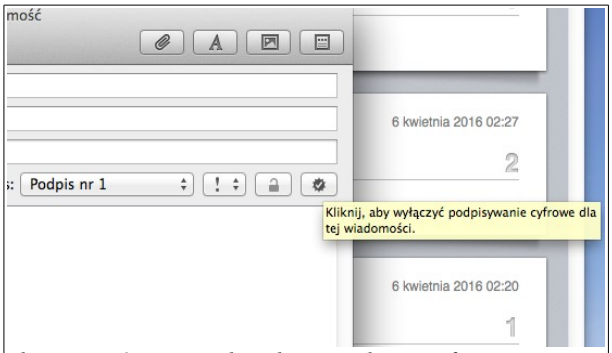
1. Klikamy na *pliku certyfikatu* - akcja ta uruchomi aplikację **Pęk kluczy**. Podajemy **hasło** zabezpieczające certyfikat.
2. Po podaniu **prawidłowego hasła** certyfikat zostanie automatycznie wprowadzony do systemu.
3. Klikamy prawym klawiszem na certyfikacie wybierając polecenie **Nowa preferencja tożsamości**.
4. W pole **Lokacja lub adres email** wpisujemy nasz adres poczty elektronicznej. Klikamy **Dodaj**.
5. Na oknie tworzenia wiadomości pojawi nam się **Przycisk wyboru podpisu cyfrowego**.



Ilustracja 1: Aplikacja Pęk kluczy



Ilustracja 2: Okno Żądaj certyfikatów



Ilustracja 2: Przycisk wyboru podpisu cyfrowego

9. Żądanie certyfikatu dla serwera Linux

Przykład wygenerowania żądania certyfikatu dla serwera WWW o nazwie `nazwa.domena.pl` w systemie Linux CentOS 6:

```
# cd /etc/pki/tls/private
# umask 077
# openssl genrsa -out nazwa.domena.pl.key 2048
Generating RSA private key, 2048 bit long modulus
.............................................+++
.............+++
e is 65537 (0x10001)
# openssl req -utf8 -subj "/CN=nazwa.domena.pl/O=Podmiot/L=Łódź/ST=łódzkie/C=PL" -new -key
nazwa.domena.pl.key -out nazwa.domena.pl.csr
```

Następnie wysyłamy żądanie do operacyjnego urzędu certyfikacji.

Możemy to zrobić poprzez przeglądarkę internetową: `https://ent-ca.corp.finn.pl/certsrv/` i podstronę *Request a certificate / Submit a certificate request...* – przeklejamy wtedy zawartość pliku CSR do formularza

i wybieramy **odpowiedni** szablon *FINN CA Web Server*. Po akceptacji żądania przez operatora CA wystawiony certyfikat można pobrać z podstrony *View the status of a pending certificate request*.

Metoda alternatywna to wykorzystanie linii komend Windows. Plik z żądaniem musi być dostępny lokalnie.

```
certreq -submit -attrib "CertificateTemplate: FINNCA_WebServer" nazwa.domena.pl.csr
```

Polecenie wyświetli przydzielony identyfikator żądania, np. `RequestId: "64"`. Możemy go wykorzystać do wygodnego pobrania certyfikatu na dysk lokalny:

```
certreq -retrieve 64 nazwa.domena.pl.crt
```

Tak wygenerowany certyfikat umieszczamy na serwerze – prawdopodobnie w katalogu `/etc/pki/tls/certs`.

Jeżeli na serwerze używamy SELinux'a to konieczne może być użycie `restorecon -rv /etc/pki/tls`.

9.1. Żadanie certyfikatu dla urządzenia sieciowego z systemem JunOS

```
set security pki ca-profile finn-root-ca ca-identity finn-root-ca revocation-check crl refresh-interval 48 url http://ca.finn.pl/finn-root-ca/finn-root-ca.crl
set security pki ca-profile finn-ent-ca ca-identity finn-ent-ca enrollment url http://ca.finn.pl/mscep
set security pki ca-profile finn-ent-ca revocation-check use-crl
set security pki ca-profile finn-ent-ca revocation-check ocsp url http://ca.finn.pl/ocsp
set security pki ca-profile finn-ent-ca revocation-check ocsp connection-failure fallback-crl
set security pki ca-profile finn-ent-ca revocation-check crl refresh-interval 24 url http://ca.finn.pl/finn-ent-ca/finn-ent-ca.crl

file copy http://ca.finn.pl/finn-root-ca/finn-root-ca.crt finn-root-ca.crt
request security pki ca-certificate load ca-profile finn-root-ca filename finn-root-ca.crt
request security pki ca-certificate enroll ca-profile finn-ent-ca

request security pki generate-key-pair size 2048 certificate-id finn-ipsec
```

Żądanie certyfikatu przy pomocy usługi SCEP (NDES):

Pobieramy tzw. hasło wezwania ze strony `https://ent-ca.corp.finn.pl/certsrv/mscep_admin/`.

```
request security pki local-certificate enroll ca-profile finn-ent-ca certificate-id finn-ipsec challenge-password 7F9F180328B8CC5B domain-name v0-front.finn.pl subject "CN=v0-front0,SN=BM0813AA0140,OU=VPN,O=FINN Sp. z o.o.,L=Lodz,ST=lodzkie,C=PL"
```

Ręczne generowanie żadania i wgranie certyfikatu:

```
request security pki generate-certificate-request certificate-id lodz-front subject "CN=lodz-front.finn.pl,OU=Infrastruktura,O=FINN Sp. z o.o.,C=PL" email "psztoch@finn.pl" filename lodz-front.csr
file copy http://domena.pl/nazwapliku.crt lodz-front.crt
request security pki local-certificate load certificate-id lodz-front filename lodz-front.crt
```

Weryfikacja:

Sprawdzamy czy mamy zaczytane certyfikaty urzędów certyfikacji:

```
show security pki ca-certificate detail
```

Sprawdzamy czy pobrały się listy CRL:

```
show security pki crl detail
```

Weryfikujemy certyfikaty urzędów certyfikacji:

```
request security pki ca-certificate verify ca-profile finn-root-ca
request security pki ca-certificate verify ca-profile finn-ent-ca
```

Weryfikujemy certyfikat routera:

```
request security pki local-certificate verify certificate-id finn-ipsec
```