

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

FINNCA INS Instrukcja dla subskrybentów

© 2018 FINN Sp. z o.o. Wszelkie prawa zastrzeżone

Historia zmian dokumentu:

Wersja	Data publikacji	ata 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. Wstep	1
2. Żądanie nowego certyfikatu użytkownika w systemie Windows	1
3. Żądanie nowego certyfikatu komputera w systemie Windows	1
4. Podpisywanie dokumentów w pakiecie OpenOffice	3
5. Podpisywanie dokumentów w pakiecie Microsoft Office	3
6. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Mozilla Thunderbird	4
7. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Microsoft Outlook	5
8. Instrukcja użycia certyfikatu do podpisywania wiadomości w programie Mail w systemie Apple OS X	Х6

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).







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**.

🖹 FINNCA INS1 Instrukcja wnioskowania o certyfikaty w Windows v2016.03.10.odt - OpenOffice Writer					gnatury cyfrowe			×
<u>P</u> lik	<u>E</u> dytuj <u>W</u> idok W <u>s</u> taw <u>F</u> ormat T <u>a</u>	abel	a <u>N</u> arzędzia <u>O</u> kno Po <u>m</u> oc	Zawartość dokumentu została podpisana przez:				
	Nowy	$\left \cdot \right $	崎 🐝 🐘 🛍 • 🏈 🖆 • 🖓 • 🖓 • 🕹 🖽 • 2	ſ	Podpisał	Cyfrowe ID wydane przez	Data	
2	Otwórz Ctrl+C Poprzednie dokumenty	•	Roman ∨ 10 ∨ G K P ≡ Ξ Ξ		e	FINN Enterprise CA	05.04.2016 11:53:4	1
1	Kreatory	•	· · · 1 · · · X · · · 1 · · · 2 · · · 3 · · · 4 · ·					
1	Zamknij							
	Zapisz Ctrl+S	s						
	Zapisz jako Ctrl+Shift+S	s						
	Zapisz <u>w</u> szystko							
Z	Załad <u>u</u> j ponownie							
	Wersje	_		l				
<u>\$</u>	Eksportuj				Sygnatury w tym dokum	encie są poprawne		
	Eksportuj Jako PDF Wyś <u>l</u> ij	•		[Zobacz certyfikat	Podpisz dokument	<u>U</u> suń	
6	<u>W</u> łaściwości			L				
	Podpisy cyfrowe			ſ	-			
	Szablony	•			Pomoc		Zamknij	
Ilu	stracja 1: Podpisyw	va	nie dokumentu w OpenOffice	Ilı	ustracja 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.

¢	
Informacje	Informacje
Nowy	Chroń dokumont
Otwórz	Określ, jakie typy zmian inne osoby mogą wprowadzać w bieżącym dokumencie.
Zapisz	dokument ~
Zapisz jako	<u>Oznacz jako wersję ostateczną</u> Powiadom czytelników, że ta wersja dokumentu jest ostateczna i formatu jon jako tylko do odczytu
Save as Adobe PDF	Szyfruj przy użyciu hasła zawiera on następujące Zawiera on następujące Chroń ten dokument hasłem
Drukuj	Ogranicz edytowanie
Udostępny	
Eksportuj	Ogranicz dostęp Udziel dostępu innym użytkownikom, jednocześnie odbierając
Zamknij	Im mozitwość edytówania, kopiowania i drukowania. Dodaj podpis cyfrowy Zapewnij integralność dokumentu przez dodanie
Konto	niewidocznego podpisu cyfrowego
Opcje	
Ilustracja	1: Podpisywanie dokumentu w Microsoft
Office.	1 2

		Ро	dpisywanie			?	x
6 <u>Zo</u>	<u>bacz dodatko</u>	we informacje o po	dpisywanym doł	umencie			
Masz zai treści do	miar dodać po kumentu.	dpis cyfrowy do teg	go dokumentu. 1	en podpis nie b	ędzie wid	oczny	w
<u>T</u> yp zobo	owiązania:						
Dokum	ent zatwierdzo	ony przez					¥
<u>C</u> el podj	pisywania teg	o dokumentu:					
Aby do	ołączyć inform	acje o osobie podp	isującej, kliknij p	rzycisk Szczegółj	. <u>S</u> zcz	egóły.	
Podpis	sywanie jako:	Przemysław Sztoci	ı		70	ień	
Wysta	wiony przez:	FINN Enterprise C	A		<u>-</u>		
				<u>P</u> odpisz	:	Anulu	ij
		<u>)</u>		1.1	,		

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.





FINNCA INS - Instrukcja dla subskrybentów (6)

х

r<u>c</u>zyść

<u>(</u>czyść

S Menedżer certyfikatów – 🗆 🗙	Konfiguracja kont
Uzytkownik Osoby Serwery Organy certyfikacji Pozostałe	Konfiguracja ser Kopie i foldery Abuvent f. i advisor for a formation formation formation formation for the series of the ser
Nazwa certyfikaty, które identyfikają następujące organy certyfikacji: III. Nazwa certyfikatu Urządzenie zabezpieczające III. Google Internet Authority Urządzenie zabezpieczające III. 4 Equifax Secure Inc. III. III.	Tworzenie Certyfikat podpisu osobistego oraz certyfikat zsyfrujący. Niechciana poczta Podpis cyfrowy Miejsce na dysku Certyfikat do cyfrowego podpisywania wysyłanych wiadomości Potwierdzenia Wyczyść
Equifax Secure Global eBusiness CA-1 Builtin Object Token Equifax Secure eBusiness CA-1 Builtin Object Token #FINN Sp. z o.o.	Zabezpieczenia a admin@finn.pl Konfiguracja ser Szyfrowanie wiadomości
FINN Root CA Urządzenie zabezpieczające FINN Enterprise CA Urządzenie zabezpieczające 4 Generalitat Valenciana Root CA Generalitat Valenciana Boot CA Generalitat Valenciana Builtin Ohiert Token Wyświetl Edytuj ustawienia zaufania	Kopie i foldery Certyfikat do szyfrowania i deszyfrowania otrzymanych wiadomości: Tworzenie Wybigrz Niechciana poczta Domyślne ustawienia szyfrowania podczas wysyłania wiadomości: Synchronizacja Niechciana poczta wysyłania wiadomości: Potwierdzenia Mumznań (i otrzywaj szyfrowania)
ок Ilustracja 3: Thunderbird - menedżer certyfikatów	Zabezpieczenia <i>Ilustracja 4: Thunderbird - konfiguracja konta</i>

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.
- W oknie Zmienianie ustawień zabezpieczeń sprawdzamy czy w polu Certyfikat podpisujący jest nasz 4. certyfikat. Możemy go zmienić wybierając sąsiadujące pole Wybierz.
- Zatwierdzamy kolejno zmiany klikając OK. Nasza wiadomość podczas wysyłania zostanie podpisana. 5.

		Bez tytułu - Wiadomość (HTML)	Właściwości	×
$\left(\leftarrow \right)$			Ustawienia Zabezpieczenia	
\smile			Ważność Normalny 🗸 🧛 Zmień ustawienia zabezpieczeń dla tej wiadomości.	
Informacje	Bez tv	rtuku	Charakter Normalny V Ustawienia zabezpieczeń	
· · · · ·	DCZ ty	cara	🗌 Nie autoarchiwizuj tego elementu	
Zapisz		Ogranicz uprawnienia do tego elementu	Opcje głosowania i śledzenia	
Zanicz jako		Umożliwia skonfigurowanie ograniczeń dla tego elementu. Możesz na przykład	Użyj przycisków głosowania	~
Zapisz Jako	Ustaw	ograniczyć adresatom możliwość przesyłania wiadomości e-mail dalej do innych	Żądaj potwierdzenia dostarczenia dla tej wiadomości Żądaj potwierdzenia przeczytania dla tej wiadomości	
Zapisz	uprawnienia *	osób.	Opcje dostarczania	
załączniki			Ŏ □ Odpowiedzi trafiają do Książka adreso	owa
Drukuj	<u><u></u></u>	Przenies element do innego folderu	Nie dostarczaj przed Brak V 00:00 V	
	Przenieś do	Umoziwia przeniesienie lub skopiowanie tego elementu do innego tolderu. Bieżacy folder – Skrzynka nadawcza	Dezaktualizuje się po Brak 🗸 00:00 🗸	
Zamknij	folderu *	- breggy rolder. Skrzylika nadaweza	Zapisz kopię wysłanej wiadomości	
			Kontakty	
Konto pakietu	P.	Właściwości	Kategorie 🔻 Brak	
Office	Ē_•	Umożliwia ustawianie i wyświetlanie zaawansowanych opcji i właściwości tego		
	Właściwości	 Rozmiar: Jeszcze nie zapisane 	Zamk	knij
Opcje		· ·	Ilustracia 2: Właściwości wiadomości	
Ilustracia	a 1: Zakład	ka Plik		
Właściwości	zabezpieczeń	×	Zmienianie ustawień zabezpieczeń	×
Szyfruj treš	ść i załączniki wiad	domości	Preferencie ustawienia zabezpieczeń	
Dodaj pod	lpis cyfrowy do wi	adomości	Nazwa ustawień zabezpieczeń:	
🗌 Wyślij	j wiadomość jako	podpisaną zwykłym <u>t</u> ekstem	<niestandardowe dla="" ustawienie="" wiadomości="" zabezpieczeń=""></niestandardowe>	
Z <u>a</u> żąd	laj potwierdzenia	S/MIME dla tej wiadomości		
Ustawienia za	bezpieczeń —		Format kryptograficzny: S/MIME	\sim
<u>U</u> stawienie	zabezpieczeń:		Certyfikaty i algorytmy	
< Automaty	/cznie>	✓ Z <u>m</u> ień ustawienia	Certyfikat podpisujacy:	z
Etykieta za	abezpieczeń			
Mod	lu <u>ł</u> zasad:	<Żadne> V Kon <u>f</u> iguruj	Algorytm mieszania: SHA1 🗸	
<u>K</u> lasy	yfikacja:	\sim	Certyfikat szyfrowania: Wybier.	z
<u>O</u> znaczeni	e prywatności:		Algorytm szyfrowania: AFS (256-bit)	
			✓] Wysły te certyfikaty z podpisanymi wiadomościami	
	L		OK Anulu	uj
			Instracia 1: Zmioniania ostaviań zabeznicezań	
		OK Anuluj	nusiracja 4. Zmienianie osiawien 200e2pieczen	
Ilustracia	a 3: Właści	wości 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.

⊖ ⊖ ⊖ ∭ Kliknij, aby zablokować pęk kluczy	login.		Dostęp do pęku k	luczy	çk kluczy	login.	Dostęp do pęku kluczy	
Pęki kluczy Pęki	Jerzy Wiśniewski Wydany przez: FINN Enterprise CA Wydasz, pitek J. Morraz 0217 06:01:44 Czas standardowy pacyficzny © Ten certyfikat jest ważny				lówne	Centification Wydany przez: FINN E Wygasa: piątek, 10 m © Ten certyfikat jest v	Lokacja lub adres email:	
	Nazwa FINN Enterprise CA FINN Root CA FINN Root CA Servey Nowa prefet Kopiuj "Jerzy Usuń "Jerzy	Rodzaj certyfikat certyfikat rencja tożsamości zy Wiśniewski" v Wiśniewski"	Wygasa 10 cze 2020, 08:20:28 10 cze 2030, 16:34:26 10 mar 2017, 06:01:44 28 maj 2019, 01:18:54	Pek klut login login login login		Nazwa INN Enterprise CA FINN Root CA Image: Time Annual mail.finn.pl	Certyfikat: 🕞 Jerg 📆 Jerg 🤹 👌 Wybierz preferowany certyfikat dla lokacji lub adresu pokazanego ponizej. Anuluj Dodaj	
Kategoria Wszystkie rzeczy Hasła Bezpieczne notatki Moje certyfikaty Klucze	Eksportuj "J Informacje Przetestuj "J	erzy Wiśniewski"						
[,] ⊂ertyfikaty Ilustracja 1: Apli	kacja Pęk klu	czy			Ilus	tracja 2: Okno Ż	ądaj certyfikatów	



9. Żądanie certyfikatu dla serwera Linux

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

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 refreshinterval 48 url <u>http://ca.finn.pl/finn-root-ca/finn-root-ca.crl</u> set security pki ca-profile finn-ent-ca ca-identity finn-ent-ca enrollment url <u>http://ca.finn.pl/mscep</u> 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 <u>http://ca.finn.pl/finn-ent-ca/finn-ent-ca.crl</u>

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=lodzfront.finn.pl,OU=Infrastruktura,O=FINN Sp. z o.o.,C=PL" email "psztoch@finn.pl" filename lodzfront.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 Wervfikacja:

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