

system obsługi banku Novum Bank Enterprise NOE

# Internet Banking - generacja certyfikatu i obsługa karty Vasco Digipass KEY101

Instrukcja Użytkownika

Wersja 1.0

## I. Obsługa certyfikatu dla pracownika firmy – karta KEY101

## 1. Przygotowanie karty do wydania klientowi

#### Klient banku powinien otrzymać:

- kartę kryptograficzną Vasco Digipass KEY101
- oprogramowanie SafeSign



Programy dostępne są na FTP:/support/install/IB podpis cyfrowy/vasco KEY101 i muszą być udostępnione klientowi wraz z kartą kryptograficzną.

2. Karta już jest sformatowana.



Uwaga! – Powtórne formatowanie zmienia predefiniowany PIN użytkownika i administratora.

#### Klient banku musi u siebie w komputerze:

- zainstalować dostarczone oprogramowanie (SafeSign)

- zmienić **PIN** karty, predefiniowany PIN użytkownika to 1111, jeśli pozostanie bez zmian to aplikacja podpisu może nie działać prawidłowo. Zmieniony **PIN** ma być znany tylko osobie podpisującej nim przelewy.

3. ETAP I - Generacja wniosku o certyfikację dla kart Vasco Digipass KEY101

#### Etap I powinien wykonać właściciel/pracownik firmy (klient banku – osoba używająca karty)

- 1. Zainstaluj program zarządzający kartami elektronicznymi **SafeSign** (są to sterowniki urządzenia + zarządzanie PIN-ami i certyfikatami na karcie).
- 2. Uruchom certmgr.msc. W programie należy wybrać w kolejności:
  - Certyfikaty > Bieżący użytkownik -> Osobisty -> Certyfikaty
  - Zakładka Akcja > Wszystkie zadania -> Operacje zaawansowane -> Utwórz żądanie niestandardowe -> Dalej
  - należy wybrać: Kontynuuj bez zasad rejestracji

	_		Х
🔄 Rejestracja certyfikatów			
Wybierz zasady rejestracji certyfikatu			
Zasady rejestracji certyfikatu umożliwiają rejestrację certyfikatu na podstawie wstępn szablonów certyfikatów. Zasady rejestracji certyfikatu mogą już być skonfigurowane	ie zdefini dla użytk	owanych ownika.	
Ustawienia konfigurowane przez administratora			
Zasady rejestracji usługi Active Directory			<b>~</b>
Ustawienia konfigurowane przez użytkownika		Dodaj no	we
Ządanie niestandardowe			
Kontynuuj bez zasad rejestracji			
	<u>D</u> alej	Anu	luj

- W opcji Szablon należy wskazać: (Brak szablonu) Starszy klucz,

- W opcji Format zadania: format zaznaczony domyślnie

Potwierdzamy przyciskiem: Dalej

			_		×
🔄 Rejestracja certyfikatów					
Żądanie niestano	lardowe				
Z poniższej listy wybi	erz opcję i skonfiguruj opcje certyfikatu z	zgodnie z wymagania	ami.		
Szablon:	(Brak szablonu) Starszy klucz			~	
	Pomiń rozszerzenia domyślne				_
Format żądania:	PKCS #10				
	○ Wywołanie CMC				
Uwaga: archiwizowa niestandardowego ż	nie klucza nie jest dostępne w przypadku adania certyfikatu, nawet jeśli ta opcia b	u certyfikatów utworz edzie określona w cer	zonych na po rtvfikacie.	dstawie	
	,				
			Dalej	Anu	ıluj

- W opcji Szczegóły:

Właściwości certyfikatu –> Zakładka Podmiot

					_		×
🔄 Rejestracja certyfikatów							
Informacje o certyfi	kacie						
Kliknij przycisk Dalej, aby dostosować żądanie certy	używać opcji fikatu, a nast	już wybranych d ępnie kliknij przyd	la tego szablonu lı cisk Dalej.	ıb kliknij p	orzycisk Sz	czegóły, a	by
🗹 Żądanie niestandard	owe	🤃 STAI	N: Dostępny		9	Szczegóły	^
Następujące opcje o Użycie klucza: Zasady aplikacji:	pisują sposół	b użycia i okres w	ażności stosowany	/ do certyf	ikatów te <u>c</u>	go typu:	
Okres wazności (	(dni):				Wła	aściwości	
					Dalej	Anı	ıluj

W oknie Właściwości certyfikatu należy uzupełnić dane **Nazwa podmiotu** wybieramy: Jednostka organizacyjna, Nazwa pospolita, Kraj, Organizacja, i wpisujemy **Wartość** – nazwę – >zatwierdzamy Dodaj->Zastosuj

Właściw	ości certyfi	ikatu				×
Ogólne	Podmiot	Rozszerzenia	Klucz prywatny			
Podmi wystaw alterna	otem certy viony. Moż tywnych, k	fikatu jest uży esz wprowadz ttórych można	tkownik lub komp ić informacje o tyj a będzie używać w	outer, dla pach naz certyfika	i którego certyfikat w podmiotu i war acie.	został tości nazw
Podmi Użytko	ot certyfika wnik lub k	atu omputer, <mark>kt</mark> ór	y odebrał certyfika	at		
Nazwa	podmiotu	:			CN-1#2	
Jedno	ostka orgar	nizacyjna 🗸	Dodaj >		O=vt3 C=pl	
Warto	ść:		< Usuń		OU=jot3	
Nazwa	alternatyw	/na:	-			
Typ: Nazw	a katalogu	~				
Warto	ść:		Dodaj >			
			< Usuń			
				ОК	Anuluj	Zastosuj

W opcji Szczegóły:

Właściwości certyfikatu -> Zakładka Rozszerzenia -> Użycie klucza -> należy wybrać jn:

Właściwości certyfikatu		Х
Ogólne Podmiot Rozszerzenia Klucz prywatny Poniżej przedstawiono rozszerzenia certyfikatów dla tego typu certyfikatów.		^
Użycie klucza Rozszerzenie użycia klucza opisuje przeznaczenie certyfikatu.	^	
Dostępne opcje:     Wybrane opcje:       Podpisywanie listy CRL     Szyfrowanie danych       Tylko odszyfrowywanie     Dodaj >       Uzgadnianie klucza     Dodaj >       Vodpisywanie certyfikatu klu     < Usuń		
<ul> <li>Vstaw te użycia klucza jako krytyczne</li> </ul>	>	
Rozszerzone użycie klucza (zasady aplikacji)	*	
Podstawowe warunki ograniczające	*	¥
OK Anuluj	Zastos	uj

W opcji Szczegóły:

Właściwości certyfikatu -> Klucz prywatny -> Dostawca usług kryptograficznych -> należy

odznaczyć opcję domyślną

Microsoft Strong Cryptographic Provider (Podpis)

a <u>zaznaczyć opcję</u>

SafeSign Standard Cryptographic Service Provider (Podpis)

Właściwości certyfikatu	×
Ogólne Podmiot Rozszerzenia Klucz prywatny	
Dostawca usług kryptograficznych	^
Dostawca CSP to program generujący parę kluczy publiczny i prywatny, które są używane w wielu procesach związanych z certyfikatami.	
Wybierz dostawcę usług kryptograficznych (CSP):	
Microsoft Enhanced Cryptographic Provider v1.0 (Podpis)	^
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider (Podpis)	
Microsoft Enhanced RSA and AES Cryptographic Provider (Podpis)	
Microsoft RSA SChannel Cryptographic Provider (Szyfrowanie)	
SafeSign Standard Cryptographic Service Provider (Podpis)	
SafeSign Standard RSA and AES Cryptographic Service Provider (Podpis)	~
Pokaż wszystkich dostawców CSP	
Opcje klucza	*
Typ klucza	~
OK Anuluj Zast	tosuj

Należy potwierdzić Zastosuj, OK, Dalej. Pojawi się okno wpisania PINU: domyślnie to 1111

Enter PIN	
To log in to "test vasco"	
Enter PIN:	
➤ Minimum PIN length ✓ Maximum PIN length	1 4 bytes h 15 bytes
ОК	Cancel

- otrzymuję plik żądania xxx.req. W pliku zmieniamy rozszerzenie na \*.p10. Zapisujemy.

Tak utworzony plik z rozszerzeniem \*.p10 (wniosek o certyfikację) należy dostarczyć do Banku, gdzie zostanie wygenerowany certyfikat w systemie NOE.

## 4. ETAP II - Generacja certyfikatu w systemie Novum Bank

W module INTERNET BANKING – administracja należy otworzy okno szczegółowych danych pracownika (tego, dla którego generowany jest certyfikat): USTAWIENIA... nazwisko imię (Id = ...), (FIRMY  $\rightarrow$  EDYTUJ  $\rightarrow$  EDYCJA OSOBY)

Kowalska Eliza Ident: 10222512	(ID = 799)					×
Król sp. z o.o. (ID	= 27690)			Zwykły użyt	kownik	~
Certyfikat nr: 633		Ważny do:	2022-08-16	Założo	ny: 2016-03-	17
🗌 Blokada od dnia:			I	Idane logowan:	ie: 2019-08-	19 14:36:10
			Nieu	idane logowan:	ie: 2019-06-	10 09:04:11
Wułacz nowiadomier	ia o naruszeniu	CSP	Błędne p	próby logowan:	ia: 🚺	
nyrqor ponradonrei	iu o nurusceniu	001				
Wlight Konto Sub	vonto likk	ad Onic konta				
3259 27 813 181	S S S S S S S S S S S S S S S S S S S	RACHUNKT B	IEŻACE PRZED	SIFRIORSTV IN	DYWIDHAI NYCH	
3259 27 016 101	0	RACHUNKI B	IEŻACE PODMI	OTÓW NIEFINAN	SOWYCH	
3259 27016 101	-9 0	Rachunki V	AT dla 27016	-101		
						~
Produkt: dla firm	44 8747 101	18 0000 3259	2000 0010	Limit poj.	oper. 999,99	9,999,999.00
Nazwa klienta: DMC Nazwa kliencka: Rach	spółka z o.o.			Limit dzien	ny	
Nazwa bankowa: RACH	JNKI BIEŻĄCE PRZ	2EDSIĘBIORSTW		Limit miesi	ęczny	
INDYWIDUALNYCH 27013	-101			Limit w skl	epie	700.00
Certyfikaty Hasło	Poczta		Limity	Rachunek	Uprawnienia	Domyślne
Listy haseł Formular	ze Historia		Przelewy	Statystyka	Ustawienia	Esc zamknij

W wyświetlonym powyżej oknie wybieramy przycisk **Certyfikaty**, a w następnym oknie LISTA CERTYFIKATÓW KLIENTA wybieramy przycisk **Dopisz**.

Ustawienia Kowalska Eliza	×
Długość klucza:	1,024
Hasło do klucza banku:	
Ważny miesięcy: 36	Do dnia: 2022-08-21
Opis, numer seryjny karty key101	:
Wczytaj request, generuj	certyfikat Esc anuluj

W oknie Ustawienia...(IMIĘ I NAZWISKO), przykład powyżej, wprowadzić należy ustawienia dla tej osoby (wpisujemy hasło do klucza banku, okres ważności klucza – domyślnie 36 miesięcy, podajemy opis - zalecany nr seryjny karty), następnie klikamy Wczytaj request, generuj certyfikat i kojarzymy go z odpowiednim plikiem z żądaniem certyfikatu - \*.p10. Potwierdzamy dane certyfikatu. Plik z certyfikatem zabezpieczającym o nazwie z wniosku o certyfikację i rozszerzeniu crt powstanie w tym samym katalogu, co plik \*.p10.

Certyfikat pracownika zostanie dopisany do listy jego certyfikatów, widoczny w oknie ustawień pracownika pod przyciskiem **Certyfikaty**.

			Inform	iacja (l	Press HELP t	o view stack tr	ace)	>	×	
					ertyfikat zos :\Users\kasia	tał zapisany do t\Desktop\cert	pliku yfikat key101\ce	rtyfikat101.crt		
						[	ОК	Pomoc	]	
Lista c	ertyfil	katów k	lienta							×
	ID	cert.	Ważny	do	Wydany	Opis			Status	~
		633	2022-	08-16	2019-08-1	6 key 101			ok	
<u> </u>										
-										
Cert	tufi	kat h	anku 1	[D = <sup>1</sup>	100 ważnu	w okresie 21	315-07-16 - 2	025-07-16		
0	-yr 1	inde e			in nachy	" om este e				
0										$\sim$
										×.
Dop	isz	Edu	JCIA	Usu	ń Użui:	innei firmu	Import	F2 zapi	sz Esc an	ului

5. ETAP III - Zapis certyfikatu na kartę

W celu zapisania certyfikatu ma kartę należy uruchomić ponownie program SafeSign Token Managment Utility i zaimportować certyfikat

#### Digital IDs -> Import Certificate...

👒 Token Management Utility	_	Ф	Х
Digital IDs Token Integration Tasks Help			
Reader or Token Name	Token	Status	
KEY101	operat	tional	
<			>

🔿 Token Management Utility	- 🗆 X
Digital IDs Token Integration Tasks Help	
Show Registered Digital IDs	Token Status
Import Digital ID	operational
Import Certificate	
Exit	
٤	

W momencie importu certyfikatu należy wskazać miejsce, z którego zostanie pobrany certyfikat oraz wpisać hasło certyfikatu

Import Digital ID		×
Digital ID file:		2
✓ Import CA certificate Set the label of the II Label on token:	s ) on the token to a non default-val	ue
Digital ID password:		
	OK Can	icel

Proces poprawnego importu certyfikatu zakończy się komunikatem jn:

Information	>	×
1	The certificate has been imported successfully!	
	ОК	

Tak wygenerowany certyfikat gotowy jest do podpisu przelewów przez pracownika firmy.

Po uruchomieniu certmgr.msc w folderze **Osobisty -> Certyfikaty** wygenerowany certyfikat powinien pojawić się na liście:

🙀 Certyfikat	×
Ogólne Szczegóły Ścieżka certyfikacji	
Informacje o certyfikacie	_
System Windows nie ma wystarczających informacji, aby zweryfikować ten certyfikat.	
Wystawiony dla: vasco test	
Wystawiony przez: Bank Spoldzielczy w Naszej Miejscowosci	
Ważny od 17.05.2019 do 17.05.2022	
P Masz klucz prywatny, który odpowiada temu certyfikatowi.	
Oświadczenie wystawcy	
ОК	

# Spis treści

l. 1.	Obsługa certyfikatu dla pracownika firmy – karta KEY101 Przygotowanie karty do wydania klientowi	. 1
2.	Karta już jest sformatowana	. 1
3.	ETAP I - Generacja wniosku o certyfikację dla kart Vasco Digipass KEY101	. 1
4.	ETAP II - Generacja certyfikatu w systemie Novum Bank	. 6
5.	ETAP III - Zapis certyfikatu na kartę	. 7