

Jednostka organizacyjna:
Dział Informatyzacji

**„Instrukcja podpisywania dokumentów
certyfikatem kwalifikowanym za pomocą
aplikacji Sigillum Sign.”**



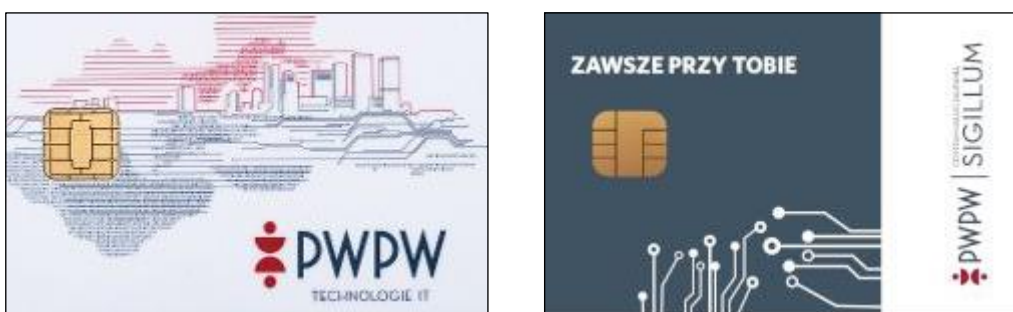
Spis treści:

1	Podpisywanie za pomocą formatu PAdES.....	3
2	Podpisywanie za pomocą formatu XAdES.....	10
3	Dodawanie kolejnego podpisu.....	11
4	Weryfikacja podpisanego pliku.....	12

1 Podpisywanie za pomocą formatu PAdES.

UWAGA! Certyfikat Kwalifikowany musi znajdować się w czytniku kart podczas wykonywania wszystkich czynności.

1. Format **PAdES** jest przeznaczony do podpisywania plików w formacie **PDF**.
2. Przed rozpoczęciem podpisywania użytkownik powinien sprawdzić jaki ma typ karty. Jest to ważne dla dalszego procesu podpisywania. (Rys.1.)

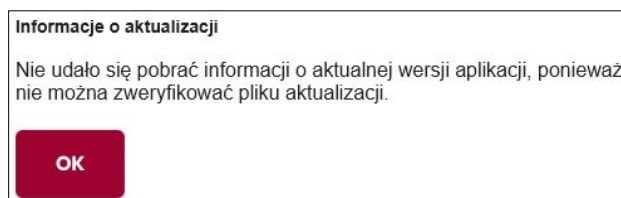


Karta CARBON

Karta DARK

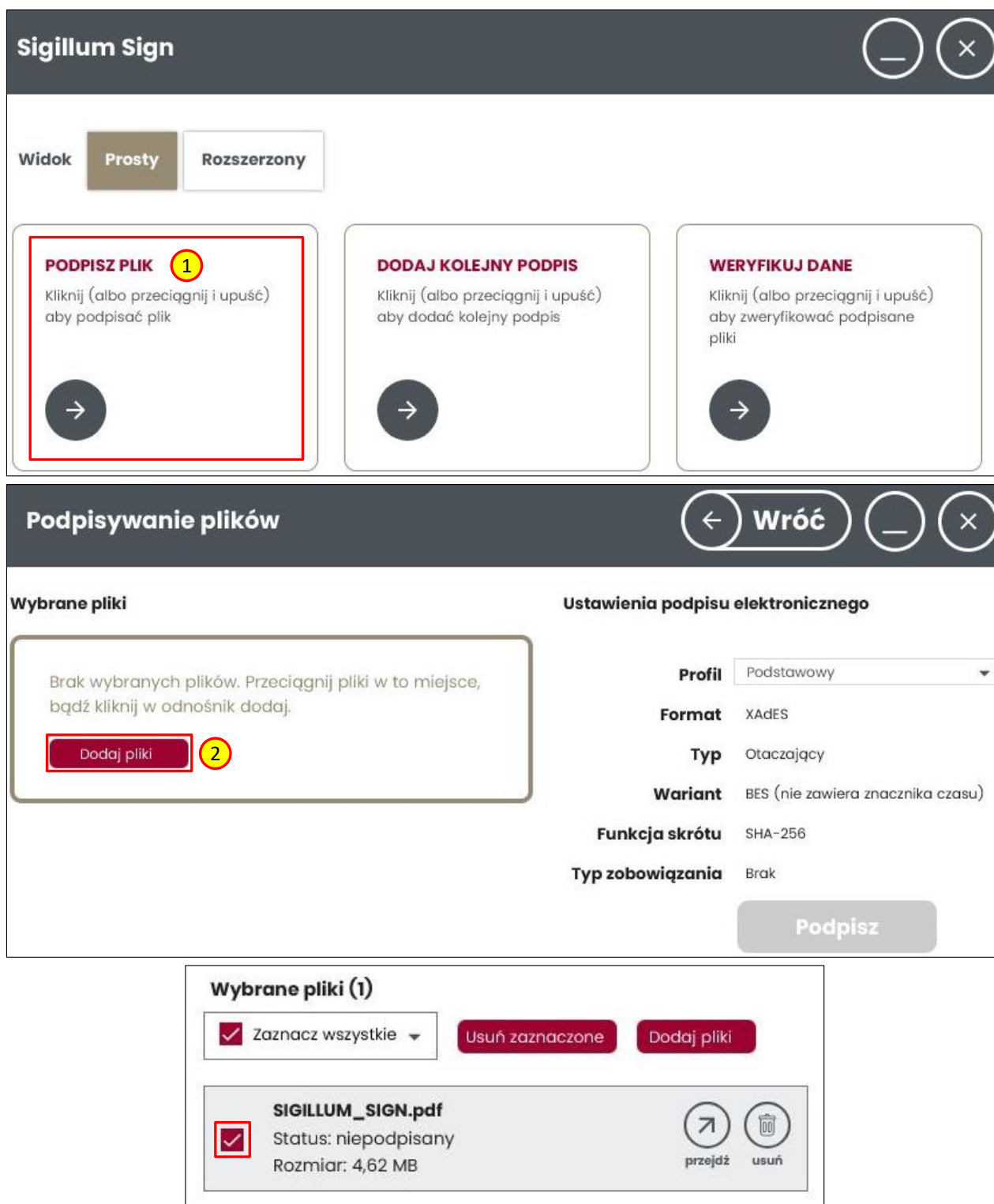
Rys.1. Wygląd poszczególnych typów kart.

3. **UWAGA!** Podczas uruchamiania aplikacji może pojawić się komunikat z błędem aktualizacji. Jest to błąd niezależny od użytkownika i nie ma on wpływu na działanie programu.(Rys.2.)



Rys.2. Komunikat błędu aplikacji.

4. Po uruchomieniu aplikacji należy wybrać opcję „Podpisz plik”(1). Pojawi się okno gdzie, za pomocą przycisku „Dodaj pliki”(2), można dodać dokument do podpisania. Można też przeciągnąć ikonę dokumentu na pole po lewej stronie aplikacji. UWAGA! Plik musi być zaznaczony aby można było wykonać operację podpisania(3). (Rys.3.)

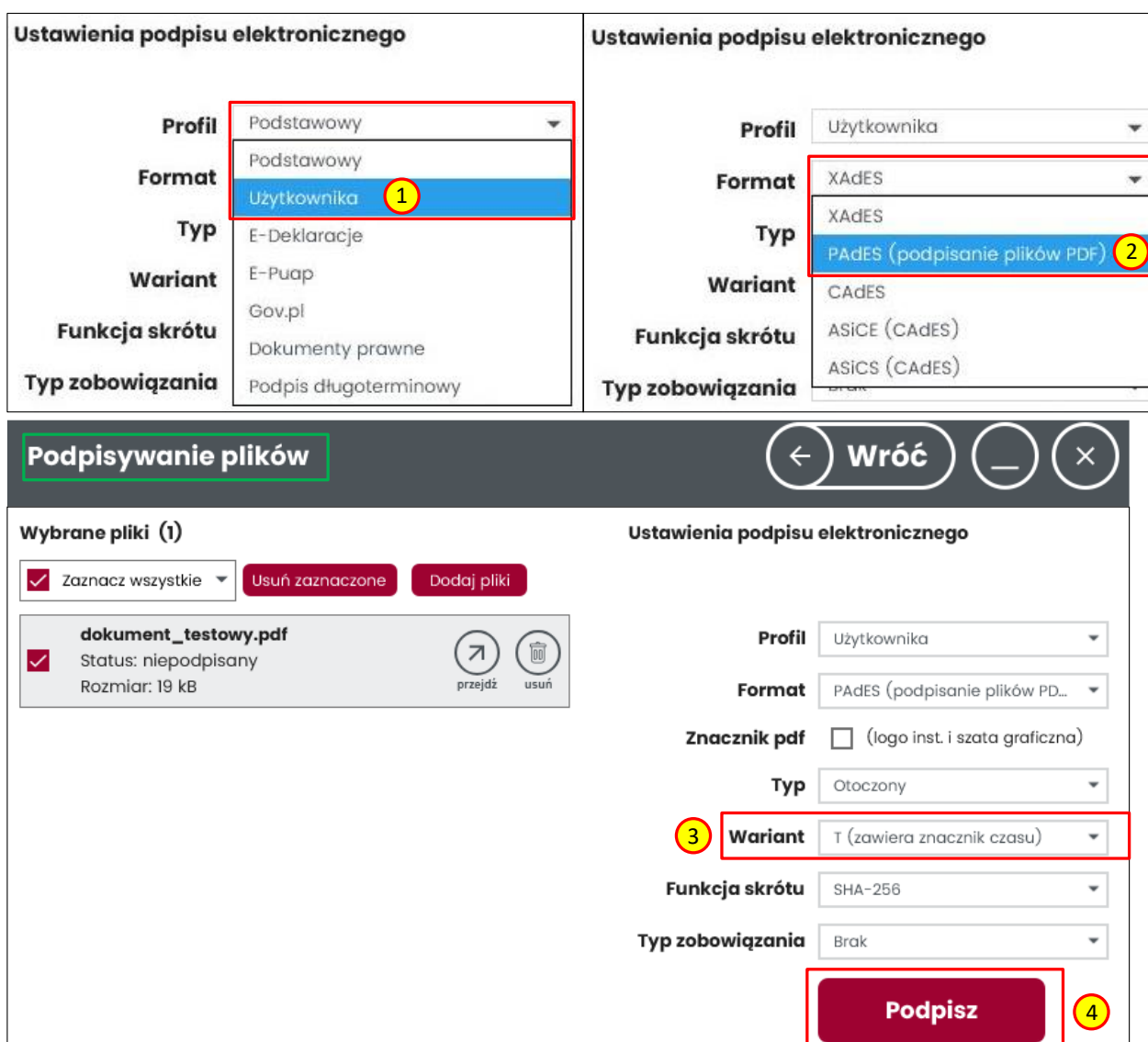


Rys.3. Wybór pliku do podpisania.

5. Po prawej stronie okna można wybrać predefiniowany profil podpisywania(1) (podstawowy, użytkownika, e-deklaracje, e-puap i inne). Należy użyć profilu „Użytkownika”. W polu „Format” należy wybrać „PAdES (podpisanie plików PDF)”(2).

UWAGA!!! W celu umożliwienia weryfikacji podpisu po upływie jego ważności dobrze jest użyć znacznika czasu do podpisu. W celu jego użycia należy, w polu „Wariant” wybrać opcję „T (zawiera znacznik czasu)” (3). Po wybraniu tego wariantu system poprosi i pin dwukrotnie (raz dla podpisu dokumentem, raz dla znacznika czasu)

Po naciśnięciu przycisku „Podpisz”(4) program przejdzie do kolejnego okna. (Rys.4.)



Ustawienia podpisu elektronicznego

Profil	Podstawowy
Format	Podstawowy
Typ	E-Deklaracje
Wariant	E-Puap
Funkcja skrótu	Gov.pl
Typ zobowiązania	Dokumenty prawne

Ustawienia podpisu elektronicznego

Profil	Użytkownika
Format	XAdES
Typ	XAdES
Wariant	PAdES (podpisanie plików PDF)
Funkcja skrótu	CAAdES
Typ zobowiązania	ASiCE (CAAdES)

Podpisywanie plików

Wybrane pliki (1)

Zaznacz wszystkie

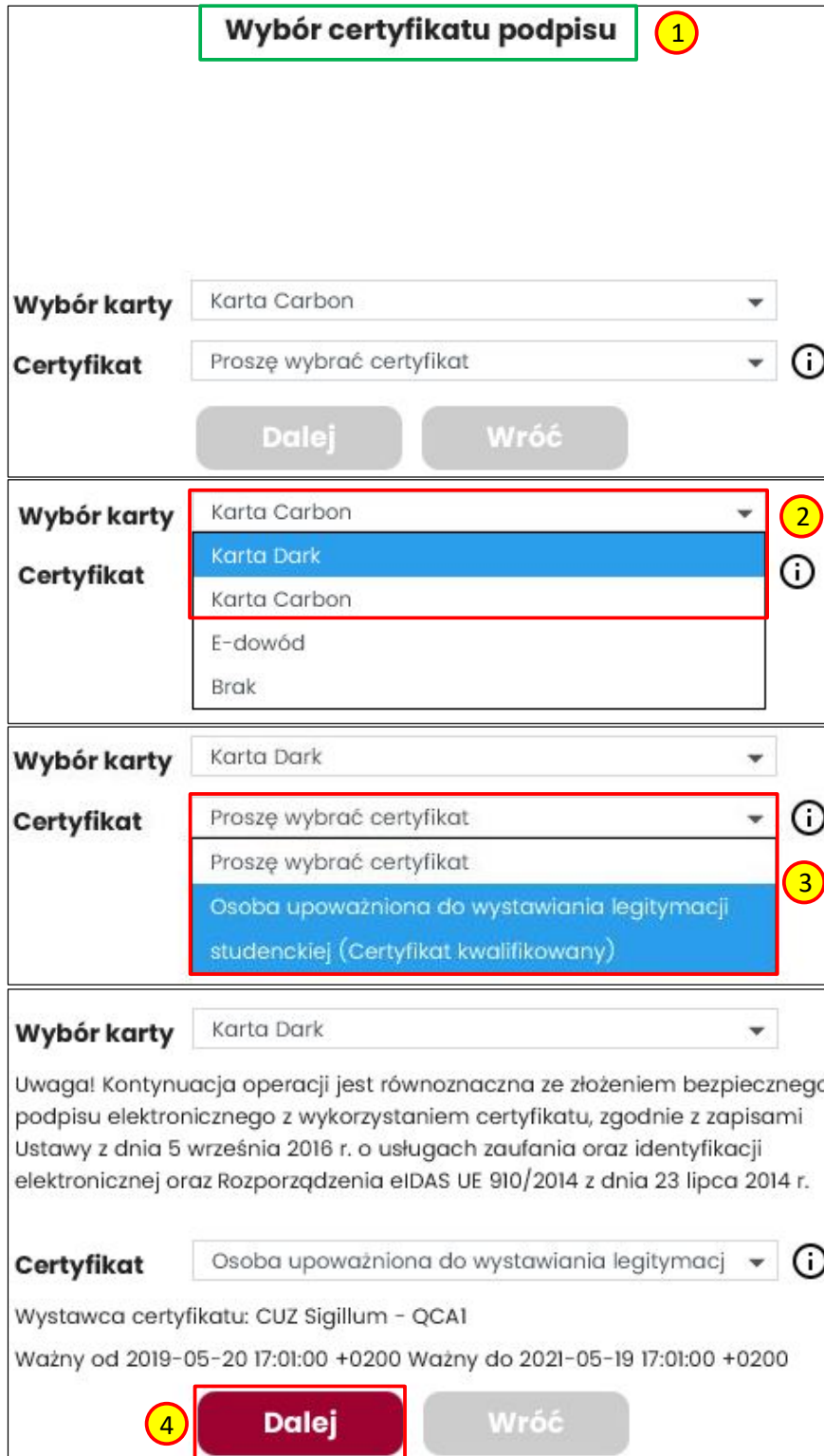
<input checked="" type="checkbox"/>	dokument_testowy.pdf	<input type="button" value="przejdź"/>	<input type="button" value="usuń"/>
	Status: niepodpisany		
	Rozmiar: 19 kB		

Ustawienia podpisu elektronicznego

Profil	Użytkownika
Format	PAdES (podpisanie plików PD...
Znacznik pdf	<input type="checkbox"/> (logo inst. i szata graficzna)
Typ	Otoczony
Wariant	T (zawiera znacznik czasu)
Funkcja skrótu	SHA-256
Typ zobowiązania	Brak

Rys.4. Wybór właściwego formatu podpisu.

6. W oknie „Wybór certyfikatu podpisu” (1), należy wybrać rodzaj karty z jakiej korzystamy (2). Wybór jest zależny od typu karty jakiego używa użytkownik. Po wybraniu odpowiedniej karty aplikacja odczyta zawarty na niej certyfikat. Będzie on widoczny w rozwijanym menu „Certyfikat” (3). Klikając na niego potwierdzamy i przechodzimy do okna końcowego gdzie wybór trzeba zatwierdzić przyciskiem „Dalej” (4). (Rys.5.)



Wybór certyfikatu podpisu 1

Wybór karty: Karta Carbon

Certyfikat: Proszę wybrać certyfikat ⓘ

Dalej Wróć

Wybór karty: Karta Carbon 2

Certyfikat: Karta Dark ⓘ

Karta Carbon

E-dowód

Brak

Wybór karty: Karta Dark

Certyfikat: Proszę wybrać certyfikat ⓘ

Proszę wybrać certyfikat 3

Osoba upoważniona do wystawiania legitymacji studenckiej (Certyfikat kwalifikowany)

Wybór karty: Karta Dark

Uwaga! Kontynuacja operacji jest równoznaczna ze złożeniem bezpiecznego podpisu elektronicznego z wykorzystaniem certyfikatu, zgodnie z zapisami Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej oraz Rozporządzenia eIDAS UE 910/2014 z dnia 23 lipca 2014 r.

Certyfikat: Osoba upoważniona do wystawiania legitymacj ⓘ

Wystawca certyfikatu: CUZ Sigillum - QCAI

Ważny od 2019-05-20 17:01:00 +0200 Ważny do 2021-05-19 17:01:00 +0200

4 Dalej Wróć

Rys.5. Wybór typu karty oraz certyfikatu.

7. Potwierdzenie wywoła okno wprowadzenia PIN-u karty(1). Po potwierdzeniu pojawi się okno szczegółowych informacji na temat składanego podpisu, operację kończymy przyciskiem „Dalej”(2). Plik zostanie zapisany automatycznie w katalogu źródłowym podpisywanego pliku. Na koniec pojawi się informacja o powodzeniu bądź niepowodzeniu podpisania dokumentu(3). Proces kończymy wciskając przycisk „OK”. Podpisana kopia pliku zawierająca „BES” w nazwie pliku pojawi się w katalogu źródłowym(4). (Rys.6.)

Wprowadź PIN do klucza prywatnego dla wybranego certyfikatu 1

PIN:

Potwierdź
Anuluj

Parametry wykorzystywane do podpisu:

Rodzaj operacji Nowy podpis

Format PAdES (podpisanie plików PDF)

Wariant BES (nie zawiera znacznika czasu)

Typ Otoczony

Funkcja skrótu SHA-256

Typ zobowiązania Brak

Wystawca certyfikatu CUZ Sigillum - QCA1

Numer seryjny [REDACTED]

Podmiot certyfikatu [REDACTED]

Położenie certyfikatu czytnik kart

2
Dalej
Wróć

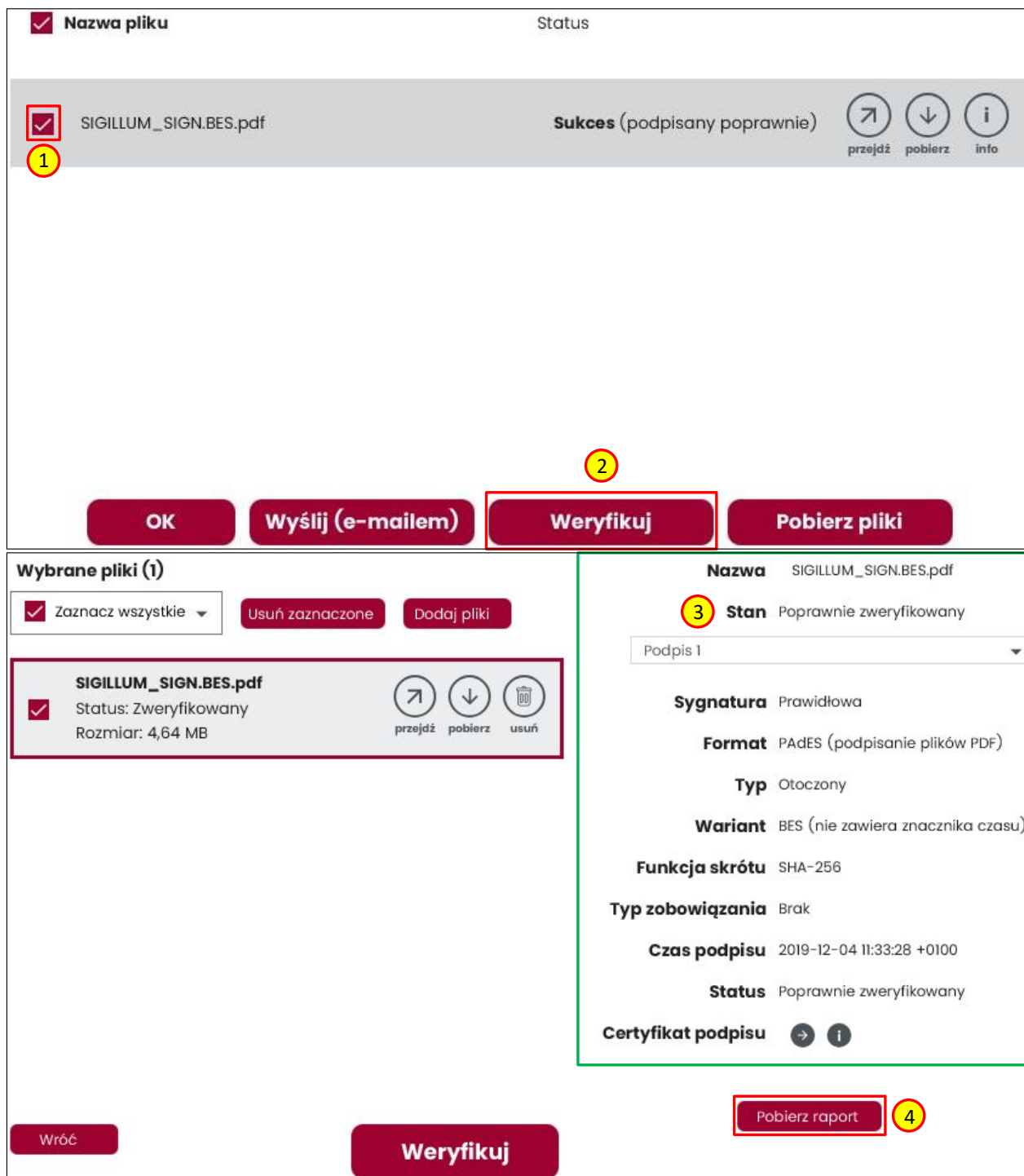
Przetworzone pliki (1)

<input type="checkbox"/> Nazwa pliku	Status	
<input type="checkbox"/> SIGILLUM_SIGN.BES.pdf	3 Sukces (podpisany poprawnie)	<input type="button" value="↶"/> <input type="button" value="↷"/> <input type="button" value="i"/> <small>przejdź pobierz info</small>

<input type="checkbox"/> SIGILLUM_SIGN.BES.pdf	4	04.12.2019 11:...	Adobe Acrobat ...	4 750 KB
<input type="checkbox"/> SIGILLUM_SIGN.pdf		12.12.2018 09:...	Adobe Acrobat ...	4 730 KB

Rys.6. Kończenie procesu podpisu dokumentu.

8. Na tym etapie można wygenerować raport weryfikacji podpisu. W tym celu należy zaznaczyć dokument(1) i wcisnąć przycisk „Weryfikuj”(2). Pojawi się okno z wynikiem weryfikacji podpisu(3). Dodatkowo można pobrać raport klikając przycisk „Pobierz raport”(4). (Rys.7.)



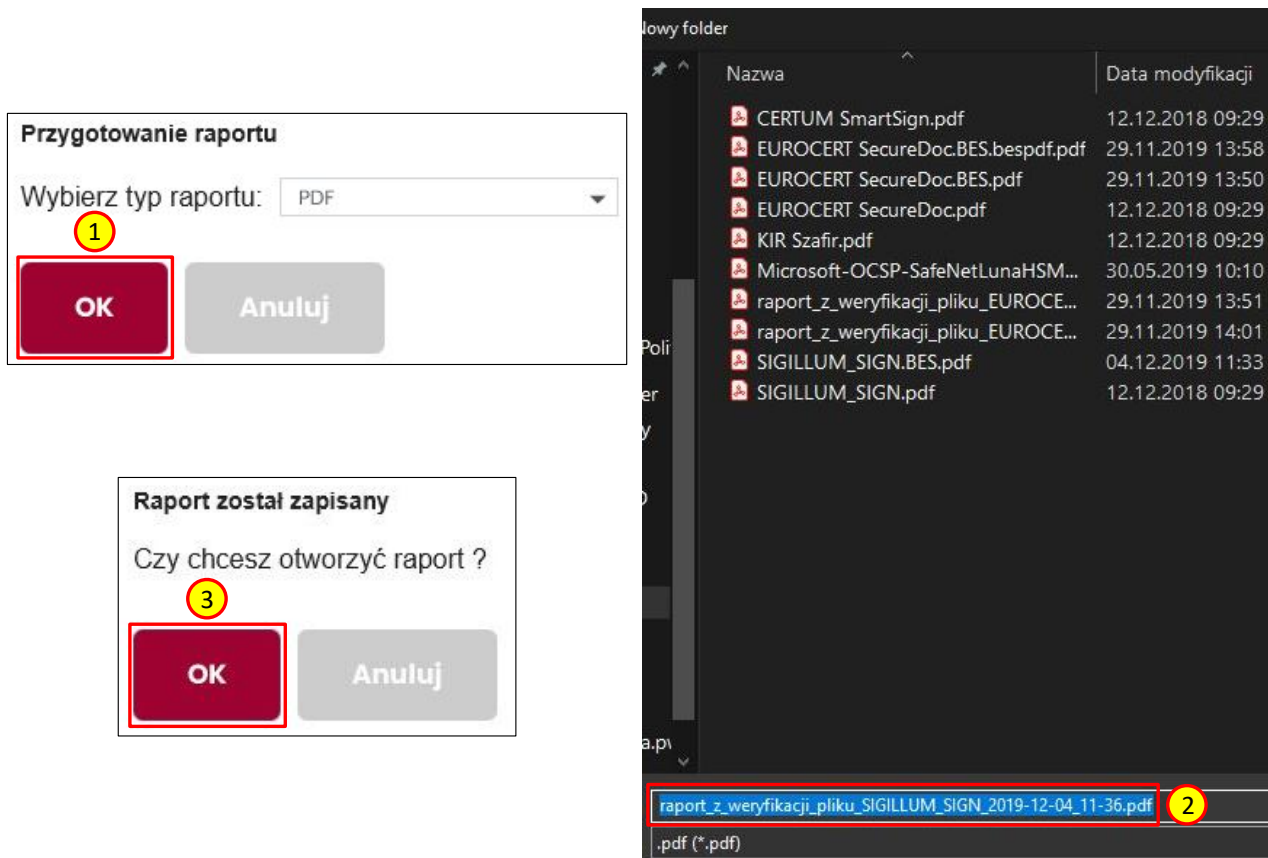
The screenshot displays a software interface for document verification. At the top, there is a table with columns for 'Nazwa pliku' and 'Status'. A file named 'SIGILLUM_SIGN.BES.pdf' is listed with a status of 'Sukces (podpisany poprawnie)'. A red box labeled '1' highlights the file name, and a red box labeled '2' highlights the 'Weryfikuj' button below the table.

Below the table, there is a section titled 'Wybrane pliki (1)'. It contains a list of selected files, including 'SIGILLUM_SIGN.BES.pdf' with a status of 'Zweryfikowany' and a size of '4,64 MB'. A red box labeled '3' highlights the 'Weryfikuj' button in this section.

To the right of the file list is a detailed verification status window. It shows the file name 'SIGILLUM_SIGN.BES.pdf' and a status of 'Poprawnie zweryfikowany'. Below this, various technical details are listed: 'Sygnatura: Prawidłowa', 'Format: PAdES (podpisanie plików PDF)', 'Typ: Otoczony', 'Wariant: BES (nie zawiera znacznika czasu)', 'Funkcja skrótu: SHA-256', 'Typ zobowiązania: Brak', 'Czas podpisu: 2019-12-04 11:33:28 +0100', and 'Status: Poprawnie zweryfikowany'. A red box labeled '4' highlights the 'Pobierz raport' button at the bottom right of the interface.

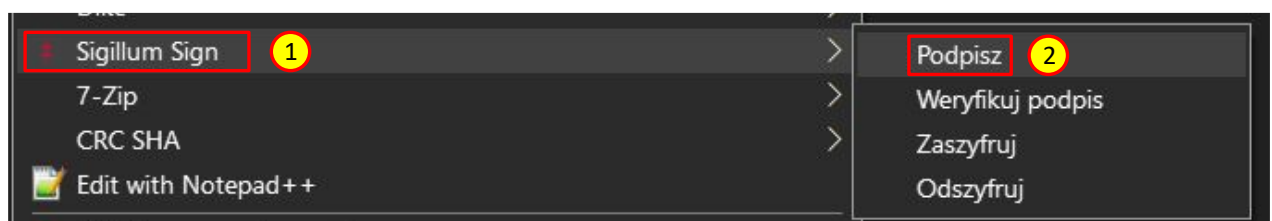
Rys.7. Weryfikacja złożonego podpisu.

9. Program zapyta nas o typ raportu i, po potwierdzeniu(1) zapisze go w miejscu pliku źródłowego(2). Po tej operacji pojawi się pytanie o otwarcie raportu. Po wciśnięciu „OK”(3) dokument otworzy się automatycznie. Nie ma potrzeby zapisywać raportu ponownie, jest on już zapisany na dysku. (Rys.8.)



Rys.8. Generowanie raportu z weryfikacji podpisu.

10. Opcjonalnie dokumenty można podpisać lub zweryfikować korzystając z menu kontekstowego. Na ikonie z plikiem należy kliknąć prawym przyciskiem myszy, następnie wybrać „Sigillum Sign”(1) i „Podpisz”(2). Uruchomi to program i otworzy okno widoczne na Rys.2. (Rys.9.)



Rys.9. Podpisywanie za pomocą menu kontekstowego.

11. **UWAGA!** Możliwe jest wielokrotne składanie podpisów elektronicznych na dokumentach podpisywanych programem Sigillum Sign. Dodawanie kolejnego podpisu jest opisane w części 3. instrukcji.

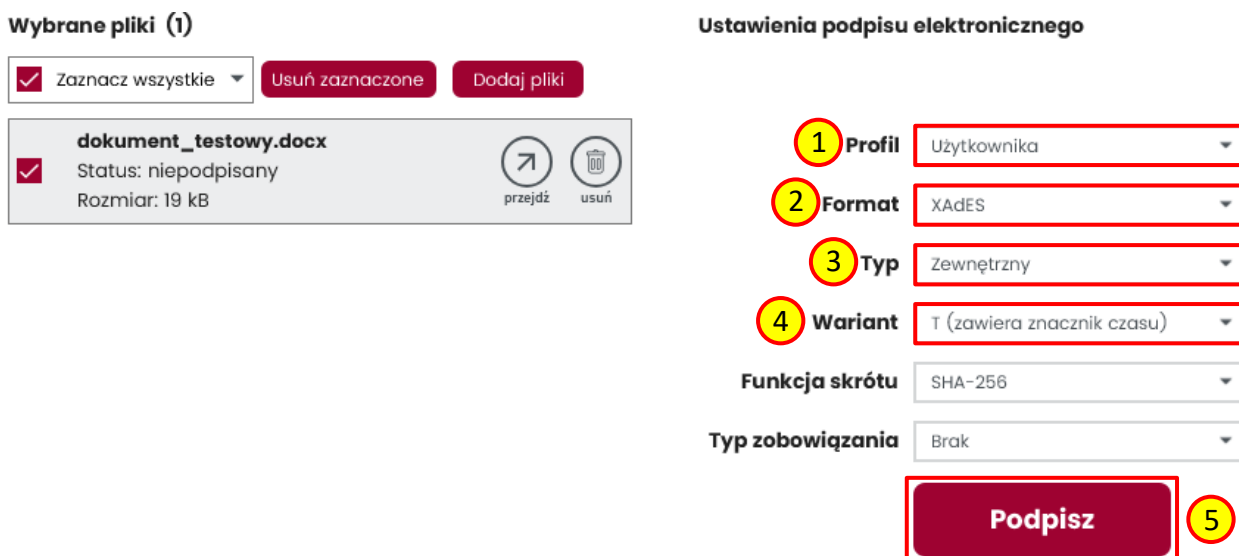
2 Podpisywanie za pomocą formatu XAdES.

UWAGA! Certyfikat Kwalifikowany musi znajdować się w czytniku kart podczas wykonywania wszystkich czynności.

1. Format **XAdES** jest przeznaczony do podpisywania każdego rodzaju plików.
2. **UWAGA!!!** Większość działań jest analogiczna jak przy podpisie za pomocą formatu PAdES, w tej części instrukcji zostaną pokazane tylko różnice.
3. Po uruchomieniu aplikacji postępujemy tak samo jak w punkcie 3 części dotyczącej formatu PAdES.
4. Po prawej okna stronie należy użyć profilu „**Użytkownika**”(1). W polu „Format” należy wybrać „**XAdES**”(2) a w polu „Typ” wybieramy „**Zewnętrzny**”(3).



UWAGA! Analogicznie jak w przypadku formatu PAdES dobrze jest wybrać Wariant podpisu „T” (zawiera znacznik czasu), umożliwi to poprawną weryfikację podpisu po upływie terminu ważności (4). Po wybraniu tego wariantu system poprosi i pin dwukrotnie (raz dla podpisu dokumentem, raz dla znacznika czasu)

Po naciśnięciu przycisku „Podpisz”(5) program przejdzie do kolejnego okna. (Rys.1.)



Rys.1. Podpisywanie za pomocą formatu XAdES.

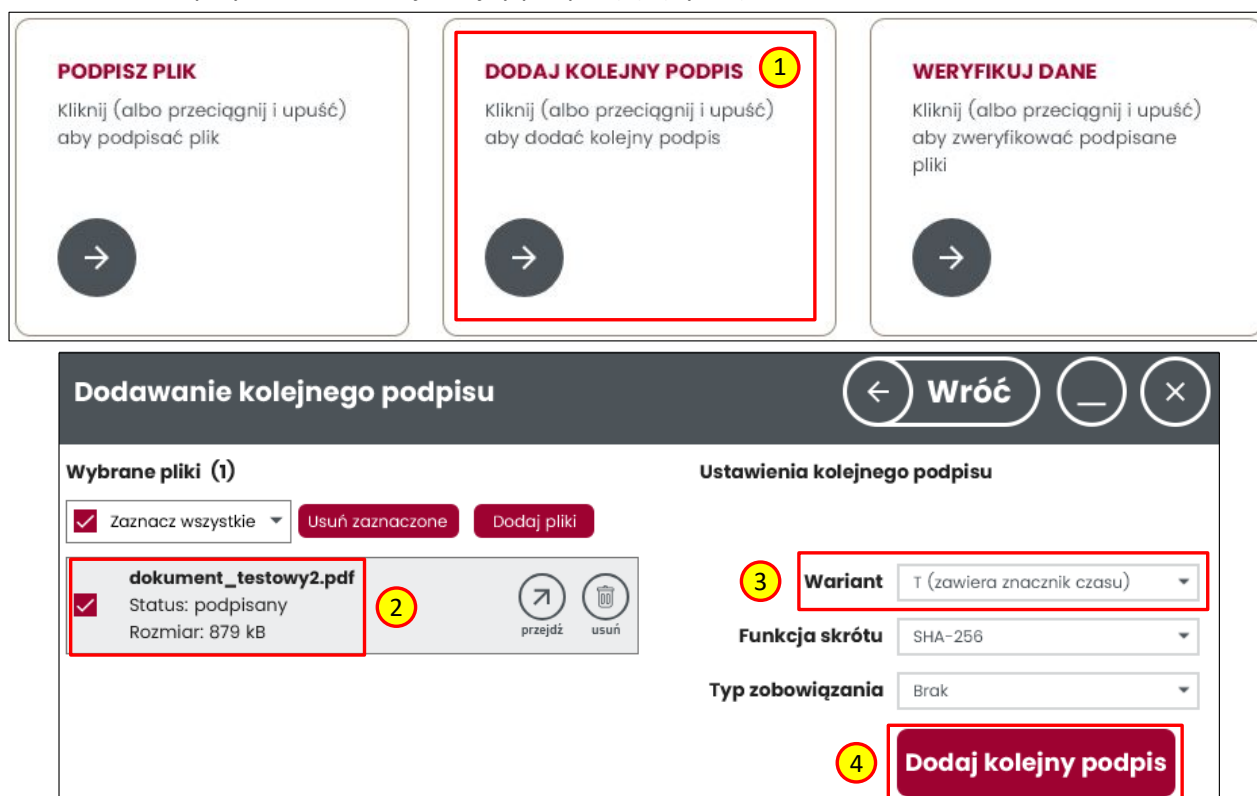
5. Dalej postępujemy tak samo jak w punktach od 5 do 7 części dotyczącej formatu PAdES.
6. W przypadku formatu XAdES nie powstanie podpisana kopia pliku źródłowego tylko nowy plik zawierający wyłącznie podpis. Plik będzie posiadał rozszerzenie „.xades”(1) i będzie automatycznie zapisany w katalogu źródłowym podpisywanego pliku.(Rys.2.)

 SIGILLUM_SIGN.BES.docx.xades 1	04.12.2019 11:...	Weryfikuj przy ...	6 KB
 SIGILLUM_SIGN.docx	02.09.2019 11:...	Dokument pro...	53 KB

Rys.2. Plik podpisu z rozszerzeniem „.xades”.

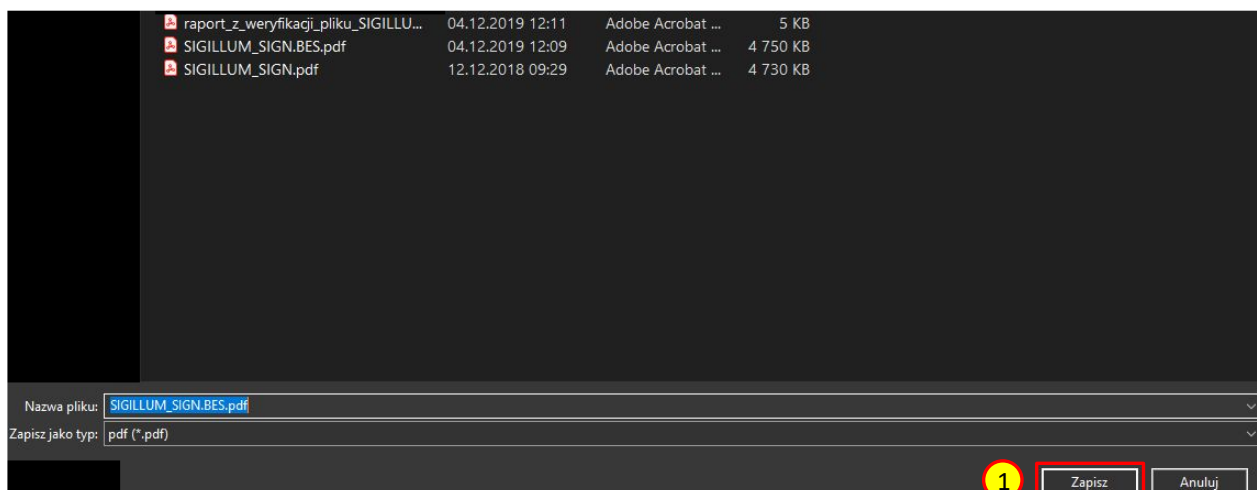
3 Dodawanie kolejnego podpisu.

1. W przypadku kiedy podpisujemy plik już podpisany należy użyć opcji „Dodaj kolejny podpis”(1). Następnie dodajemy plik analogicznie jak w części dotyczącej podpisu PAdES. W tym przypadku nie ma możliwości wyboru formatu, zostanie on wybrany automatycznie na podstawie istniejącego już podpisu(2). W polu „Wariant” należy wybrać opcję „T”(3). W celu podpisania wybór należy zatwierdzić przyciskiem „Dodaj kolejny podpis”(4). (Rys.1.)



Rys.1. Dodawanie kolejnego podpisu.

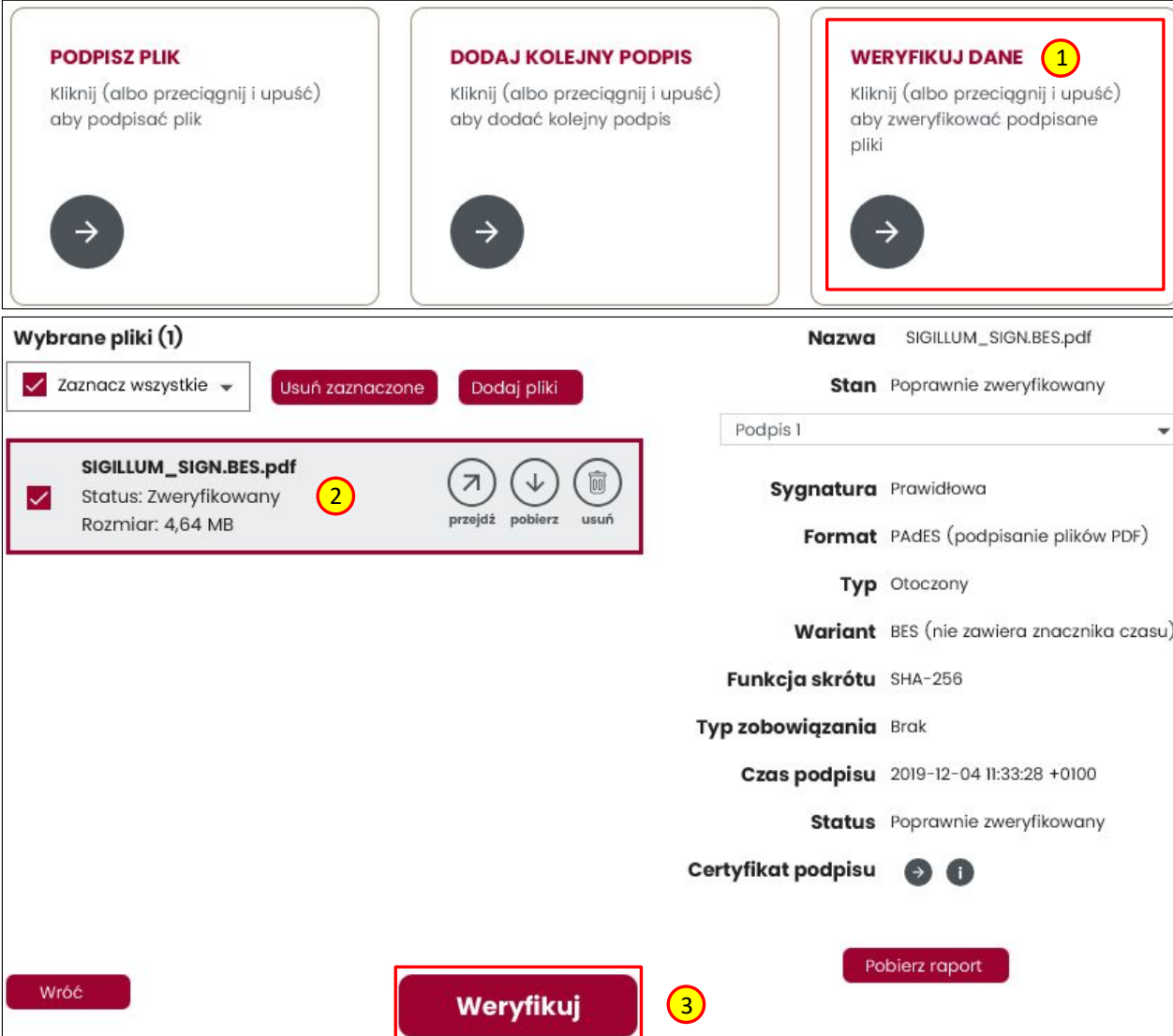
2. Dalsze kroki są analogiczne jak w punktach od 5 do 7 w części dotyczącej formatu PAdES. Jedyną różnicą jest taka że w procesie pojawi się okno „Zapisywanie jako” z wyborem miejsca zapisania lub zmiany nazwy dokumentu. Można bezpiecznie nadpisać istniejący plik, zapisze się kopia zawierająca kolejny podpis(1). (Rys.2.)



Rys.2. Zapisywanie pliku z dodanym kolejnym podpisem.

4 Weryfikacja podpisanego pliku.

1. Aby zweryfikować poprawność podpisu na dokumencie należy wybrać opcję „Weryfikuj dane”(1), a następnie wybrać plik(2) i zatwierdzić przyciskiem „Weryfikuj”(3).(Rys.1.)



PODPISZ PLIK
Kliknij (albo przeciągnij i upuść) aby podpisać plik

DODAJ KOLEJNY PODPIS
Kliknij (albo przeciągnij i upuść) aby dodać kolejny podpis

WERYFIKUJ DANE 1
Kliknij (albo przeciągnij i upuść) aby zweryfikować podpisane pliki

Wybrane pliki (1)

Zaznacz wszystkie

SIGILLUM_SIGN.BES.pdf 2
Status: Zweryfikowany
Rozmiar: 4,64 MB

przejdź pobierz usuń

Nazwa SIGILLUM_SIGN.BES.pdf
Stan Poprawnie zweryfikowany
Podpis 1

Sygnatura Prawidłowa
Format PAdES (podpisanie plików PDF)
Typ Otoczony
Wariant BES (nie zawiera znacznika czasu)
Funkcja skrótu SHA-256
Typ zobowiązania Brak
Czas podpisu 2019-12-04 11:33:28 +0100
Status Poprawnie zweryfikowany
Certyfikat podpisu → ⓘ

3

Rys.3. Weryfikacja podpisanego wcześniej pliku.

2. Dalsze kroki postępowania są analogiczne jak w punktach 8. i 9. części dotyczącej formatu PAdES.
3. W przypadku weryfikowania poprawności podpisów dokumentów podpisanych za pomocą formatu XAdES, należy weryfikować plik podpisu z rozszerzeniem „.xades”. Proces weryfikacji jest taki sam jak opisany powyżej.