Інструкція з експлуатації

SECUREDOC v 2.0

Версія 1.3

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

Зміст

1. Інформація про програму

SecureDoc v2.0 - це програма для складання і перевірки електронних підписів з можливістю видачі підпису разом із міткою часу.

У програмі SecureDoc v2.0 можна скласти електронний підпис за допомогою сертифікатів, виданих компаніями: EuroCert, CenCert (Enigma), KIR, PWPW та Certum (Asseco).

Формати, у яких можна скласти підпис за допомогою програми SecureDoc: PAdES-BES, PAdES-T, XAdES-BES, XAdES-T з внутрішніми або зовнішніми типами.

Використовуваний набір криптографічних функцій хешування: SHA-256.

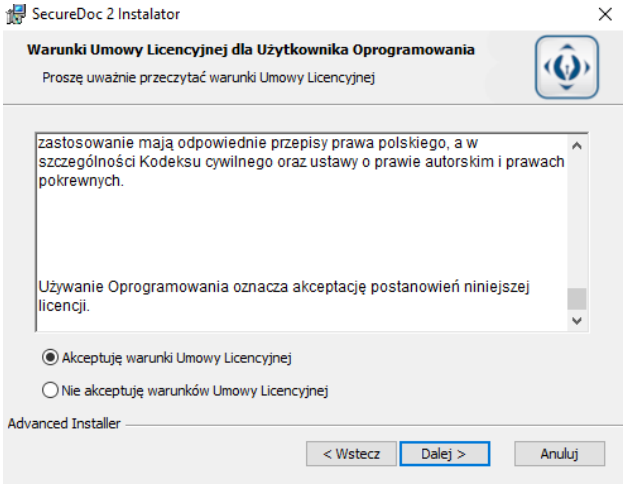
2. Мінімальні системні вимоги

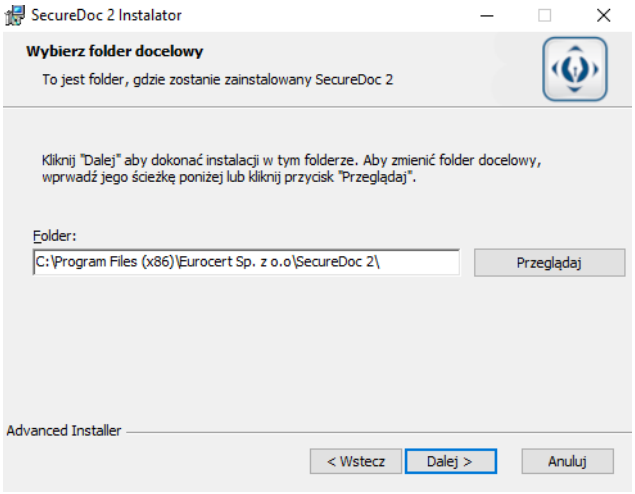
- Операційна система Windows 8 і новіша,
- Програмне забезпечення для управління картою - Charismathics Smart Security Interface,
- Інтернет-з'єднання (необхідне для функцій верифікації).

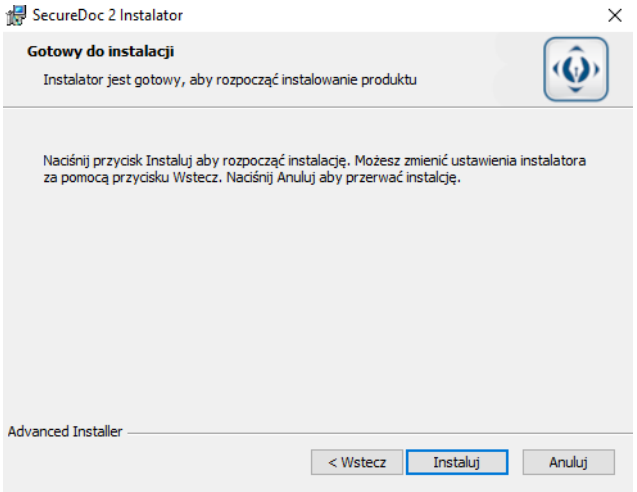
3. Встановлення програми

Для початку встановлення програми перейдіть на сторінку https://eurocert.pl/index.php/oprogramowanie і завантажте "SecureDoc 2 - програму для складання і перевірки кваліфікованого підпису".

Після запуску завантаженого інсталятора слід керуватися діалоговими вікнами, наведеними нижче:







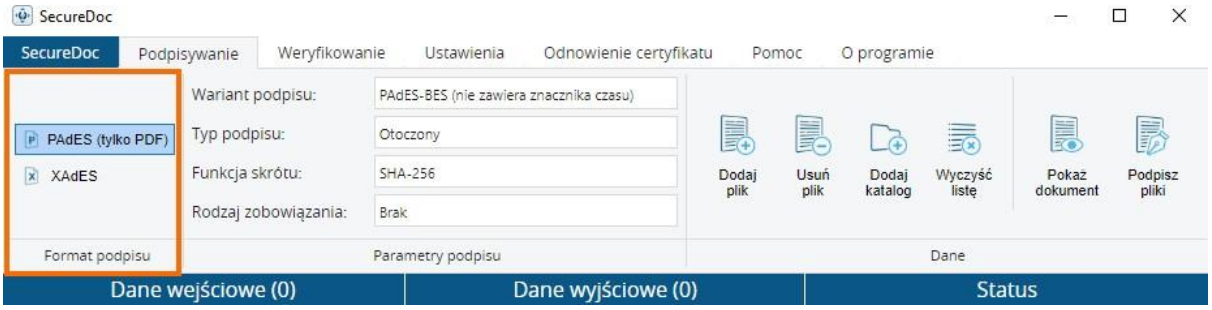
Після завершення цього етапу програма готова до використання.

4. Підписування

Вкладка "Підписування" призначена для створення електронних підписів.

У розділі "Формат підпису" доступні два формати для підписуваних файлів:

PAdES та XAdES

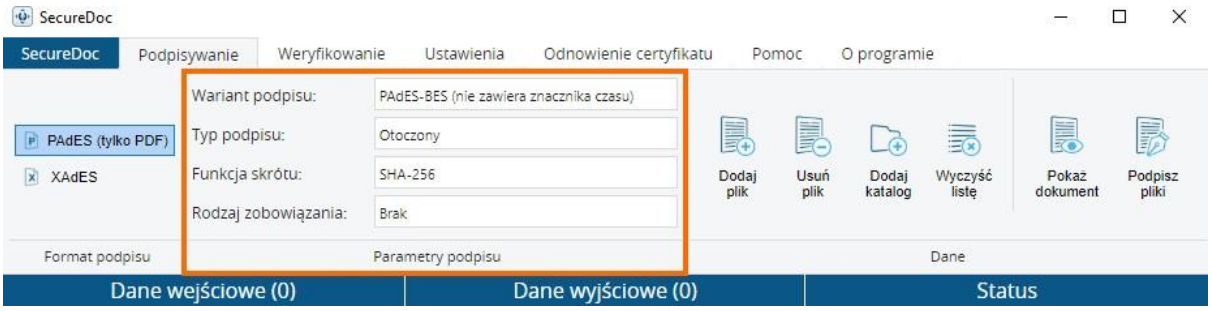


Format PAdES призначений і виключно для файлів PDF і є рекомендованим варіантом для підписування файлів у форматі PDF.

Формат XAdES можна використовувати для підпису всіх форматів файлів (.xml, .docs, .docx, .xmls, .jpeg, .odt і т. д.). Формат XAdES також можна використовувати для створення підпису під документом у форматі PDF. Проте рекомендується використовувати спеціалізований формат PAdES.

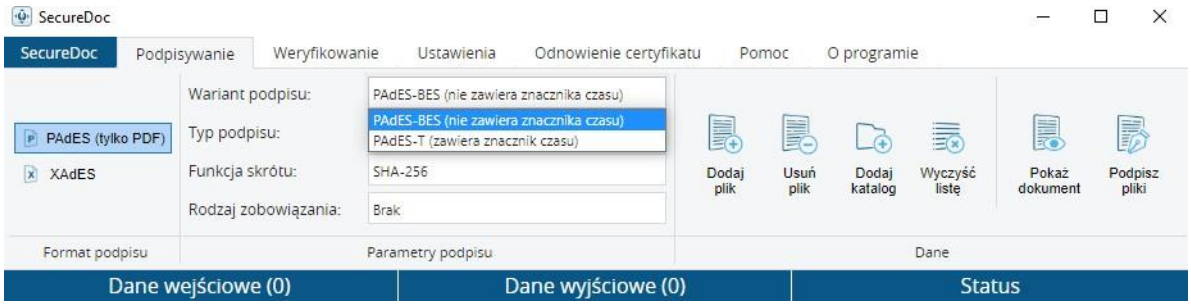
4.1 Розділ „Параметри підпису”

Розділ "Параметри підпису" містить основні налаштування для створення підпису.



4.1.1 Варіант підпису

Залежно від обраного формату підпису доступні наступні варіанти вибору зі списку - PAdES-BES / PAdES-T або XAdES-BES / XAdES-T



Варіант -BES означає, що при підписуванні документа у вибраному форматі він не матиме включеної в нього мітки часу.

З іншого боку, формат -T вказує на те, що підпис буде створено з включеною міткою часу.

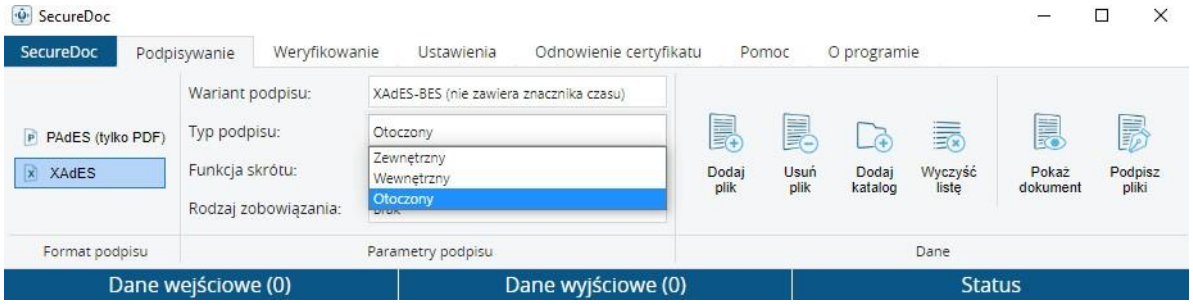
Послуга кваліфікованої мітки часу (яка згадується вище) є додатковою послугою і дозволяє точно визначити дату і час електронних дій в електронному середовищі.

Мітка часу надає можливість підтвердження часу, коли було зроблено електронний підпис, чи визначення, що документ існував у певний час і не був змінений. З погляду чинного законодавства це має значення певної дати.

Використовуючи мітку часу, видану кваліфікованим суб'єктом, ви отримуєте гарантію непідсудності часу підпису документа щодо: судів, установ, компаній, індивідуальних клієнтів і т. д.

Також важливо зазначити, що мітка часу не бере актуальний час з комп'ютера, на якому створено підпис, але звертається до відповідного сервера, щоб отримати інформацію про час.

4.1.2 Тип підпису



4.1.2.1 Зовнішній

При створенні зовнішнього підпису електронний підпис буде створений у окремому файлі та збережений у тому ж каталозі, де знаходиться файл, який підписується.

Зовнішній підпис можна ставити на будь-які файли (будь-якого формату) та розміру.

Слід мати на увазі, що при перевірці підпису потрібно мати оригінальний файл (який містить завартість документа) + файл підпису (який містить підтвердження підпису). Також при відправці зовнішнього підпису необхідно долучити файл, який підписується (оригінальний документ).

Важливо, щоб після створення зовнішнього підпису файл, який підписується, не змінювався жодним чином (не можна змінювати вміст документа АБО назву підписаного документа), оскільки це призведе до порушення цілісності даних і підпис не буде можливо правильно перевірити.

Файл зовнішнього підпису зберігається у форматі XAdES.

4.1.2.2 Внутрішній

Даний тип підпису слід використовувати для будь-яких файлів, які підписуються у форматі XAdES, і в яких ми бажаємо, щоб підпис був включений у файл, який підписується. Іншими словами, файл підпису, підписаний внутрішнім типом, буде містити як текст документа, так і підтвердження підпису (2 в 1).

Важливо пам'ятати, що файл, підписаний внутрішнім типом, буде збережений у форматі XAdES.

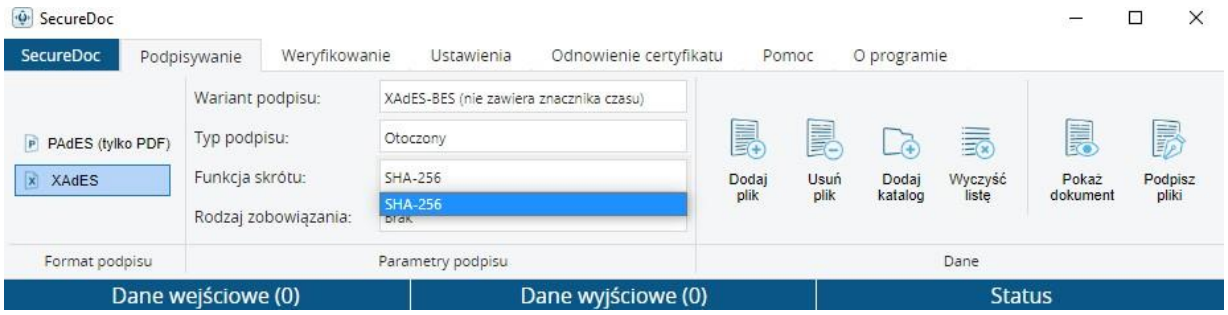
Отже, якщо, наприклад, ми підписуємо файл *document.txt*, то файл, підписаний внутрішнім підписом, буде мати наступний вигляд: *document.txt.XAdES*.

4.1.2.3 Оточений

Даний тип підпису є аналогом внутрішнього і використовується для файлів у форматі XML. Файл підпису буде містити як текст документа, так і підтвердження підпису (2 в 1).

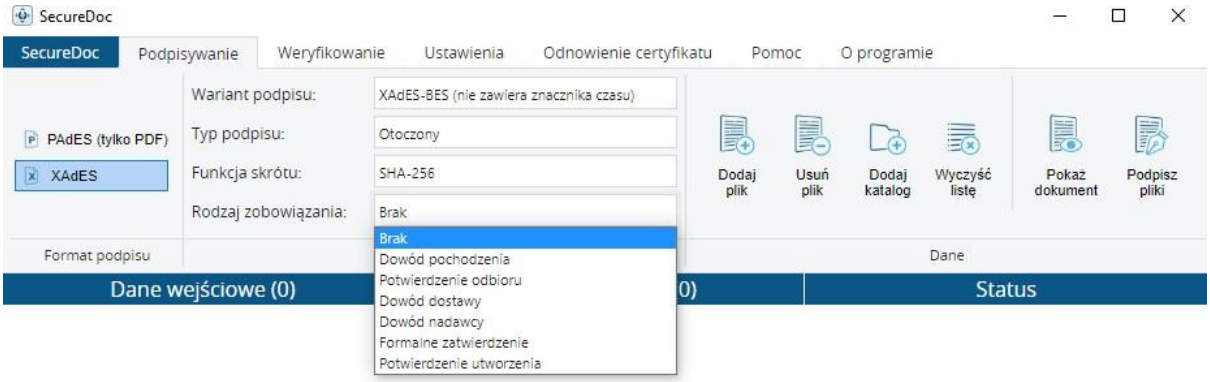
Тобто, якщо ми хочемо підписати файл XML так, щоб він містив підпис + текст документа, слід вибрати тип підпису "оточений". Тип підпису "оточений" використовується виключно для файлів у форматі XML.

4.1.3 Функія Хешування



SHA-256 - це тип криптографічного захисту, більше значення скорочення забезпечує більшу безпеку.

4.1.4 Тип зобов’язання

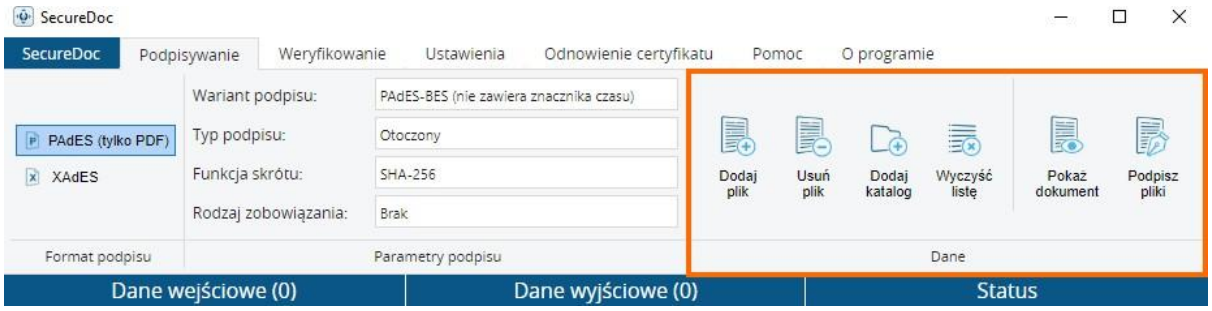


Це поле є вибірковим і містить додаткову інформацію щодо причини / мети створення підпису. Вибір типу зобов'язання не обов'язковий для створення підпису.

До вибору доступні 6 видів зобов'язань:

- Доказ походження
- Підтвердження отримання
- Доказ відправника
- Доказ одержувача
- Формальне підтвердження
- Підтвердження створення

4.2 Розділ „Дане”



Після натискання "Додати файл" відкриється вікно, де ви повинні вибрати файли для підпису.

"Додати каталог" - за допомогою цієї функції ви можете додати всі файли з вибраного каталогу, які відповідають установкам підпису, наприклад, якщо ви вибрали формат підпису PAdES, то з вибраного каталогу будуть взяті всі файли у форматі PDF, а якщо ви вибрали формат XAdES, то будуть взяті всі доступні файли з вибраного каталогу.

Ви також можете видалити файли, які ви вибрали для підпису за допомогою кнопок "Видалити файл" - для видалення окремого файлу (буде видалено вибраний, тобто підсвічений файл), або "Очистити список" - для видалення всього списку вибраних файлів.

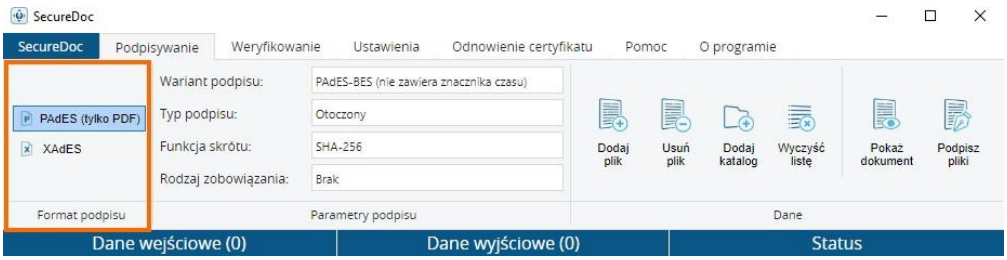
Натискання кнопки "Показати документ" призведе до відображення вмісту вибраного документа в новому вікні.

"Підписати файли" - після натискання цієї кнопки будуть підписані всі файли зі списку вибраних файлів для підпису.

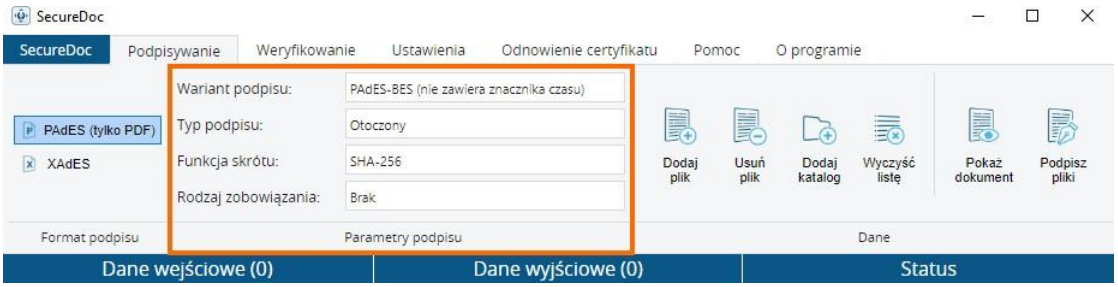
4.3 Процес складання електронного підпису

Слід пам'ятати, що для підпису файлу кваліфікованим підписом потрібно підключити пристрій з криптографічною карткою до комп'ютера.

1. Визначаємо тип підпису, яким ми хочемо підписати документ (поле "Формат підпису").



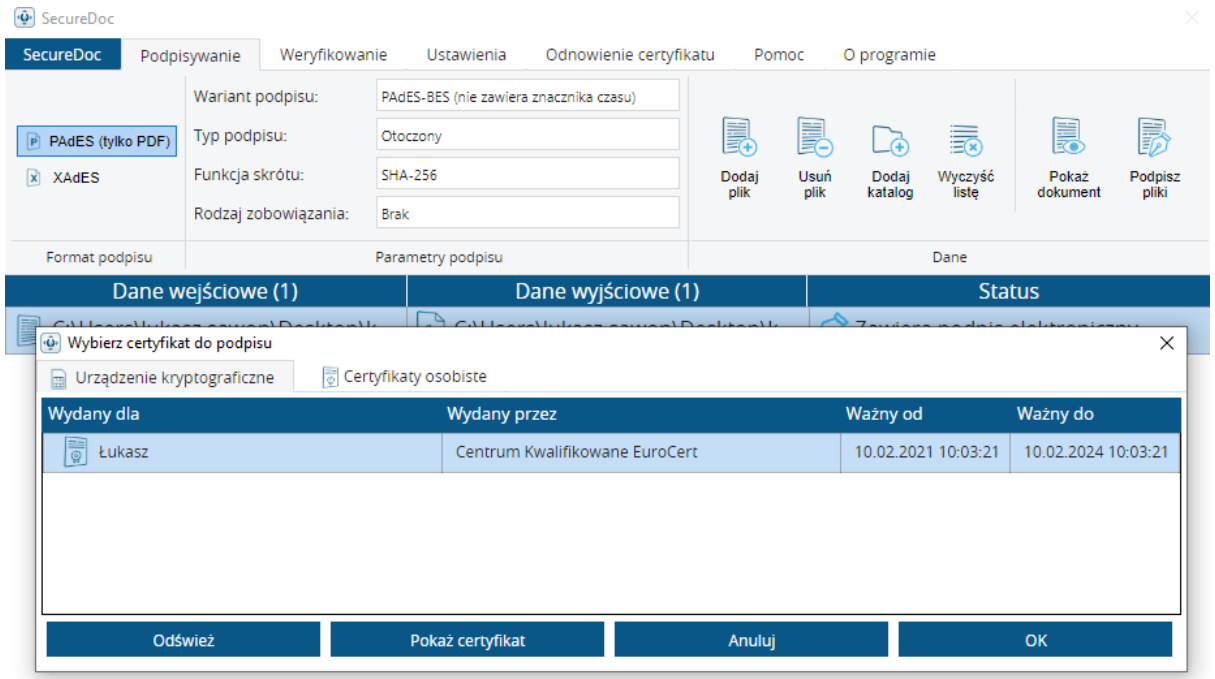
2. Вибираємо бажані параметри підпису в полі "Параметри підпису".



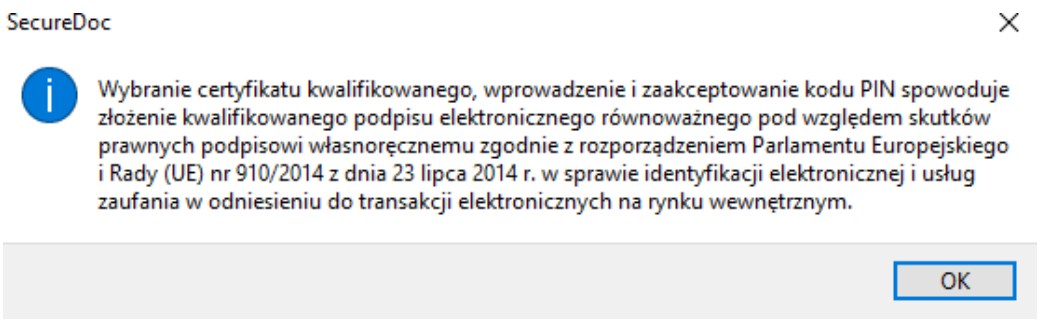
3. Додаємо файли, які ми хочемо підписати
4. Натискаємо "Підписати файли". Зверніть увагу, що всі документи зі списку вибраних для підпису будуть підписані з такими ж налаштуваннями параметрів підпису.
5. Після натиснення "Підписати файли" відкриється вікно вибору сертифікату. Виберіть вкладку "Криптографічний пристрій" і зі списку виберіть сертифікат, яким ви бажаєте підписати вибрані файли, а потім натисніть "OK". На цій вкладці доступні сертифікати, які знаходяться на підключеному пристрої.

   Вкладка "Особисті сертифікати" дозволяє читати сертифікати з сховища системи Windows (включаючи некваліфіковані сертифікати, які не знаходяться на пристрої).

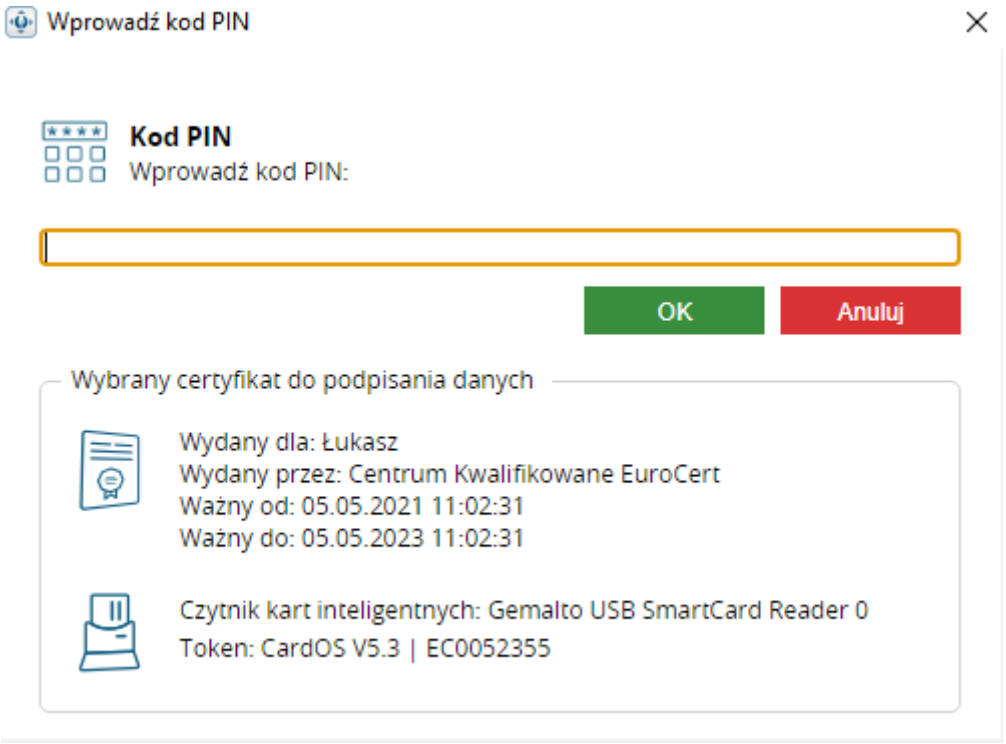
   Рекомендується використовувати вкладку "Криптографічний пристрій", оскільки в цьому випадку програма звертається безпосередньо до сертифікатів на криптографічному пристрої.



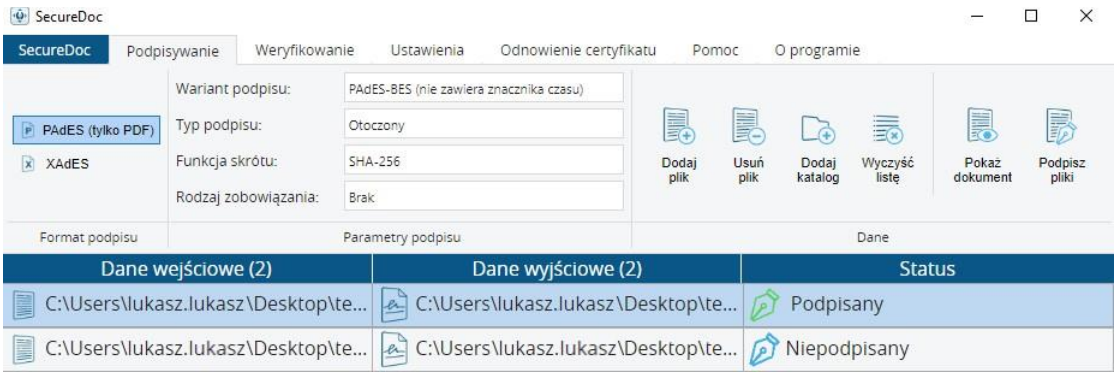
6. Після вибору сертифікату і натиснення "OK" з'явиться інформаційне повідомлення щодо складеного підпису. Після ознайомлення з повідомленням натискаємо "OK".



7. Вводимо ПІН-код і натискаємо "OK". Якщо введений ПІН-код правильний, програма почне процес підпису.

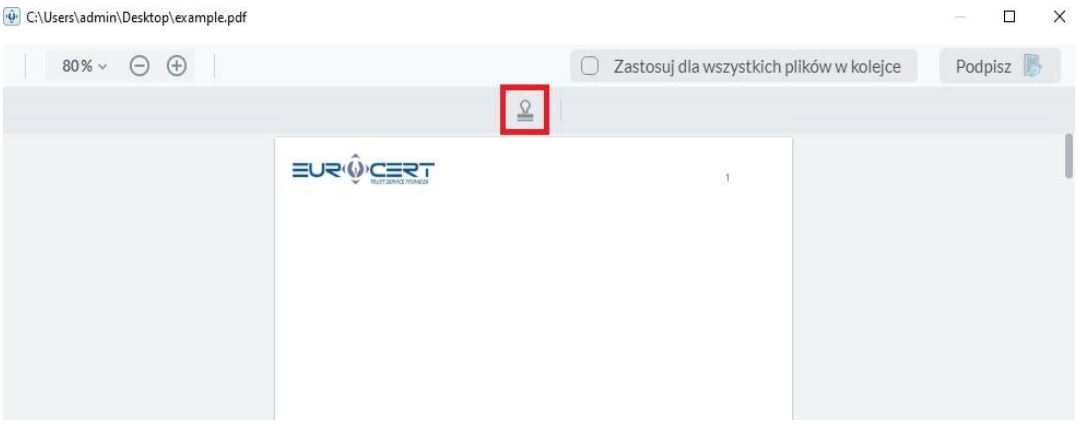


8. Перевіряємо статус підпису. Якщо документ було правильно підписано, то в вікні статусу для підписаних файлів з'явиться статус "Підписаний". Якщо виникла помилка, ви побачите статус "Непідписаний".



4.4 Підписування PDF-файлу з графічним відображенням

Якщо вибрана опція "Виконувати графічний підпис при створенні підпису в форматі PAdES" в розділі "Налаштування" -> "Налаштування підписування" процес підписування включає додаткове вікно з відображеним вмістом PDF-документа, який ми підписуємо. Потрібно натиснути на значок печатки, а потім вказати конкретне місце в документі, натискаючи лівою кнопкою миші.

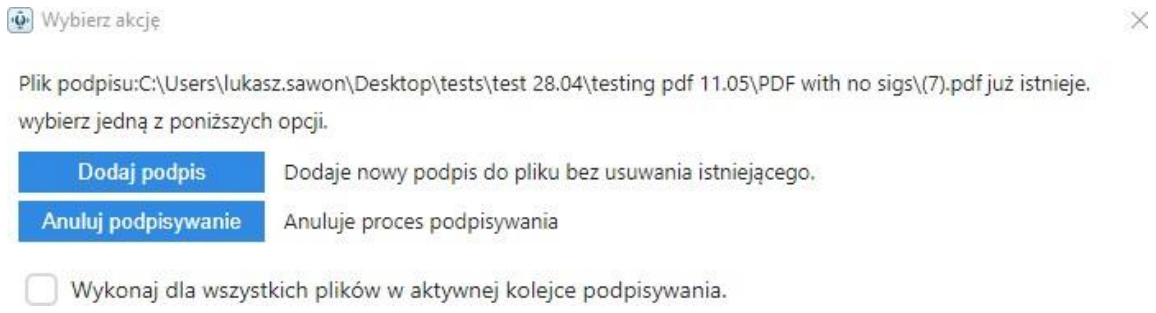


Після натиснення кнопки "Підписати" підпис буде зроблений, і графічне відображення підпису буде додано на позначене місце. У кожному процесі підписування можна додати лише один графічний знак.

При підписанні більшої кількості файлів ви можете розмістити графічний знак на першому файлі, позначивши параметр "Застосувати до всіх файлів у черзі", а потім вибрати "Підписати". Таким чином, кожен документ буде підписано з графічним знаком в тому ж самому місці.

4.5 Додавання наступних підписів до файлу

Для додавання наступного підпису до підписаного файлу, у випадку підпису XAdES ми додаємо файл, який ми підписали, або файл підпису в форматі XAdES і діємо так само, як і при додаванні першого підпису. Під час відображення вікна "Додати підпис" ми вибираємо опцію "Додати підпис".



5. Перевірка

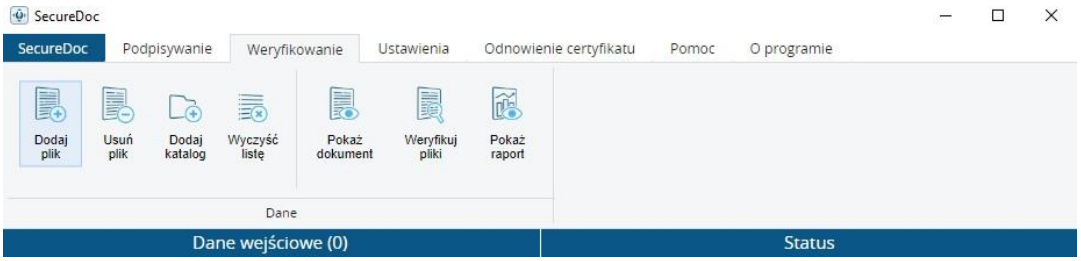
У даній вкладці ми можемо перевірити підписані файли та переглянути звіт для перевірених електронних підписів.

Функціональність кнопок "Додати файл", "Видалити файл", "Додати каталог", "Очистити список" та "Показати документ" ідентична функціональності відповідних кнопок у вкладці "Підписання".

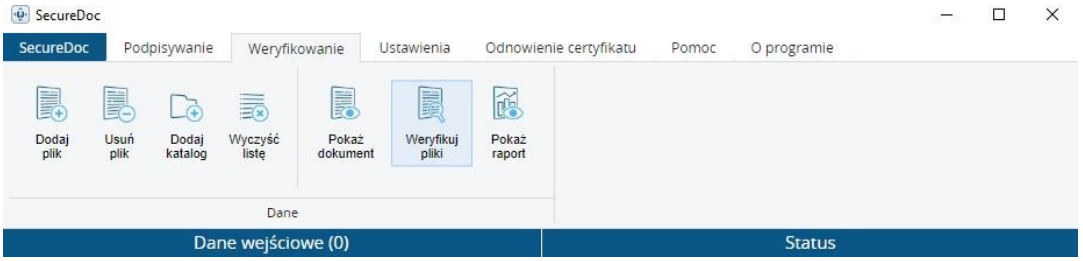
Важливо зауважити, що до списку для перевірки можуть бути одночасно додані файли різного типу підпису. Якщо файл підписаний зовнішнім підписом, слід додати до списку лише файл підпису. Крім того, слід пам'ятати, що як файл підпису, так і підписуваний файл повинні знаходитися в одному і тому ж місці/каталозі. В іншому випадку програма не зможе звертатися до вихідного файлу (зовнішньо підписаного). У разі внутрішнього підпису достатньо вказати підписаний файл.

5.1 Процес перевірки файлів

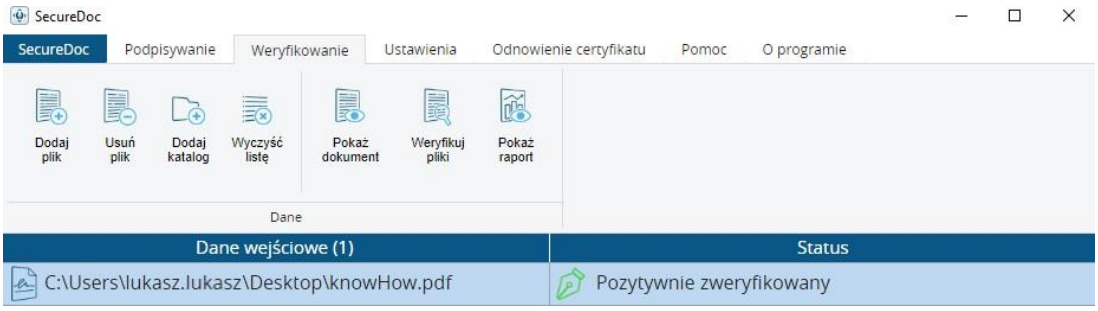
1. Додайте файли, які ви бажаєте перевірити.



2. Клікніть "Перевірити файли" (необхідно мати підключення до Інтернету під час перевірки).



3. Очікуйте повідомлення про результат перевірки.



Залежно від результату перевірки, ви можете отримати статус:
"Успішно перевірено" або "Перевірено негативно"

Для отримання більш докладної інформації про результат перевірки виберіть "Показати звіт"

Ви також можете переглянути підписаний документ, який ви перевіряєте, вибравши "Показати документ"

6. Налаштування:

6.1 Налаштування програми

6.1.1 Загальні налаштування

Мова

Для зміни мови в загальних налаштуваннях, у розділі "Мова" слід вибрати одну з доступних мов із випадаючого списку.

Оновлення

Під час запуску програми SecureDoc 2.0 перевіряє наявність оновлень, і якщо ви використовуєте застарілу версію, програма покаже повідомлення про доступне оновлення. Для встановлення нової версії слід прийняти відображене повідомлення та перейти до встановлення.

Також в цьому розділі наведена інформація про встановлену версію програми.

Проксі

В розділі Проксі є можливість налаштування проксі-сервера, який буде використовуватися програмою SecureDoc. Щоб налаштувати проксі, слід встановити параметр "Увімкнути проксі" і ввести всю необхідну інформацію в доступні поля.

6.1.2 Налаштування підписування

У розділі "Налаштування підписування" можна налаштувати параметри за замовчуванням, які будуть використовуватися при кожному старті програми. Ново визначені налаштування формату підпису застосовуватимуться при наступному запуску програми.

Доступні наступні параметри налаштувань за замовчуванням у програмі SecureDoc v2.0:

- Початковий формат підпису
- Початковий варіант підпису
- Початковий тип підпису
- Початкова функція хешування
- Початковий тип зобов'язання

Додаткові налаштування підпису

У цьому розділі ви маєте можливість налаштувати наступні опції:

„Перезапишіть документ PDF, коли створюється підпис у форматі PAdES" - скасування цієї опції призведе до того, що підписуваний файл PDF після підписання буде збережений в окремому файлі в тій же папці, що і оригінальний файл, з додаванням -sig в кінці назви.

У випадку, коли опція зазначена, підпис буде створений в вихідному файлі і перезапише його, тобто відбудеться редагування підписуваного файлу, замість збереження файлу з підписом в окремому документі.

„Не кодуйте дані XML у Base64" - скасування цієї опції призведе до збереження підписуваного файлу XML у вигляді закодованого в Base64. При встановленій опції підписувані файли XML будуть нормально зберігатися зі стандартним кодуванням UTF-8.

„Перезапишіть файл XML, коли використовуєте тип „Оточений" у форматі підпису XAdES" - якщо підписується файл XML і потрібно, щоб після підписання він зберігався у тому самому форматі - XML, слід **встановити** цю опцію.

Якщо потрібно, щоб файл XML після підписання зберігався у форматі XAdES, цю опцію слід **скасувати**.

„Створити підпис „Оточений" у стандартному варіанті" – Підпис у даній конфігурації блокує додавання подальших підписів до цього ж документа.

6.1.3 Налаштування мітки часу

Для можливості використання міток часу слід налаштувати доступ до сервера міток часу відповідним чином. Ми можемо приступити до цього в момент отримання від EuroCert необхідних конфігураційних даних:

- Адреса сервера міток часу - персоналізоване посилання для доступу до сервера міток часу,
- Ім'я користувача - персоналізований логін,
- Пароль - персоналізований пароль.

Користувач отримує наведені конфігураційні дані в момент придбання додаткової послуги мітки часу.

6.2 Управління смарт-картою

УВАГА! Тричі введення неправильного PIN-коду призводить до його блокування. Для розблокування PIN-коду слід дотримуватися вказівок в секції "Розблокування PIN-коду".

6.2.1 Зміна PIN-коду

Для зміни ПІН-коду слід натиснути "Змінити PIN-код токена", після чого з'явиться наступне вікно:

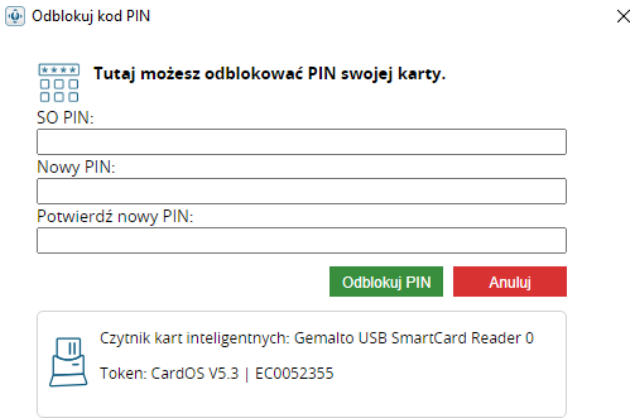
Потім слід ввести "Старий PIN" та двічі вказати "Новий PIN".

Мінімальна довжина PIN-коду - 4 символи, а максимальна - 8 або 10 символів. Новий PIN-код може складатися з будь-яких знаків: цифр, літер (малих, великих), символів та інших знаків.

6.2.2 Розблокування PIN-коду

Тричі введення неправильного PIN-коду під час складання електронного підпису або спроби зміни PIN-коду призводить до його блокування.

Для розблокування PIN-коду слід натиснути "Розблокувати PIN токена", після чого з'явиться наступне вікно:

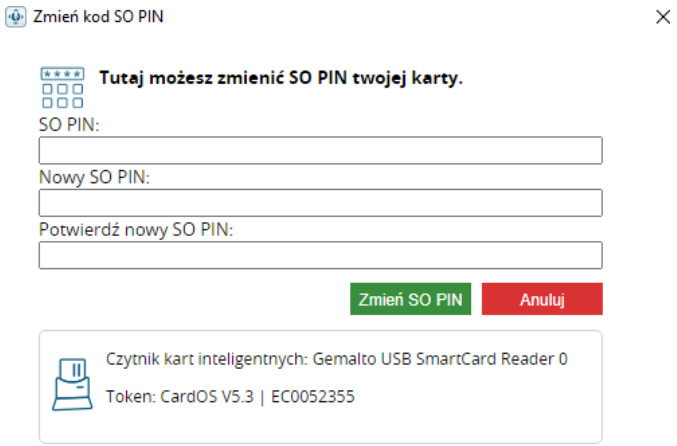


Потім слід ввести "SO PIN" та двічі вказати "Новий PIN”

УВАГА! Якщо тричі ви ввести неправильний код "SO PIN", криптографічна карта буде незворотньо заблокована. У такій ситуації слід придбати новий сертифікат.

6.2.3 Зміна SO PIN-коду

Для зміни коду "SO PIN" слід натиснути "Змінити SO PIN токена", після чого з'явиться наступне вікно:



Потім слід ввести "SO PIN" та двічі вказати "Новий SO PIN"

Новий SO PIN може складатися з будь-яких символів: цифр, літер (малих, великих), символів та інших знаків. Мінімальна довжина SO PINy - 4 символи, а максимальна залежить від моделі криптографічної карти (зазвичай 8 або 10 символів).

УВАГА! Якщо тричі ви введете неправильний SO PIN, криптографічна карта буде незворотньо заблокована. У такій ситуації слід придбати новий сертифікат.

Інша інформація:

Під час зміни PIN / SO PIN може бути підключена тільки одна криптографічна карта до комп'ютера. Підключення більшої кількості карт може призвести до заблокування деяких з них. EuroCert не несе відповідальності за наслідки, пов'язані з невиконанням даної рекомендації.

7. Поновлення сертифікату

Купіть поновлення

Після натиснення цієї кнопки вас перенаправлять на сторінку магазину sklep.eurocert.pl у розділі «Онлайн-оновлення - для існуючих клієнтів EuroCert», де ви можете вибрати бажаний сертифікат.

Оновлення сертифікату

Ми рекомендуємо починати процедуру принаймні за 7 днів до закінчення терміну дії поточного підпису. У випадку, якщо ви почнете процедуру менше ніж за 72 години до закінчення дії сертифікату, ми не гарантуємо успішного завершення процесу поновлення.

Після придбання коду для поновлення, перейдіть на вкладку "Поновлення сертифікату" і натисніть кнопку "Оновлення сертифікату".

З'явиться вікно для введення коду оновлення. Потім заповніть заяву і підпишіть угоду, яку згенерувався поточний кваліфікований підпис.

Варто пам'ятати, що покупка продукту не еквівалентна продовженню терміну дії кваліфікованого підпису. Термін дії підпису буде продовжено лише після завершення процедури, описаної в інструкції.

Після схвалення заявки EuroCert та отримання повідомлення щодо схвалення, вам потрібно буде ввести код оновлення ще раз в програмі SecureDoc, що призведе до активації оновленого сертифікату.

8. Допомога

Ця вкладка містить контактну інформацію до технічної підтримки та можливість завантажити програму AnyDesk для віддалених підключень.

9. Про програму

Вкладка містить ліцензію.