

Інструкція підписання документів через ЦЗО

ПРИКЛАД ПІДПИСАННЯ ПО ФАЙЛОВОМУ КЛЮЧУ. ВІДМІННІСТЬ ВІД АПАРАТНОГО В КІЛЬКОХ КРОКАХ

Для того, щоб підписати документи за допомогою файлового ключа (апаратного ключа) необхідно перейти на сайт <https://czo.gov.ua/sign> та зробити кілька кроків:

Крок 1. «Підписати файл за Обираємо «за допомогою електронного підпису»

 Довірчі послуги ▾

 Життя ЦЗО ▾

 Документи ▾

 Контакти

Підписати файл за допомогою

Електронного підпису →

Дія.Підпис →

+ Як це працює?

+ Що нового?

+ Формати підписів?

Крок 2. Обираємо файл, та вводимо пароль

Довірічі послуги

Життя ЦЗО

Документи

Контакти

Крок 1 з 4

Зчитайте ключ

ФайловийТокенХмарний

Кваліфікований надавач електронних довірчих послуг

Визначити автоматично

Перетягніть сюди файл ключа
або завантажте його зі свого носія
(зазвичай його назва "Key-6.dat" або *.pfx, *.pk8, *.zs2, *.jks)

Пароль захисту ключа

НазадЗчитати

Що таке файловий носій?

Файловий носій – це спеціальний файл, який містить ваш особистий ключ.

Зазвичай цей файл має назву Key-6 з розширенням *.dat (зустрічаються також розширення *.pfx, *.pk8, *.zs2, *.jks).

Для того, щоб скористатись файловим носієм, вам необхідно:

1. Обрати зі списку свого надавача електронних довірчих послуг – суб'єкта, до якого ви зверталися для отримання електронного підпису.

2. Завантажити із зовнішнього носія чи власного комп'ютера файл з вашим особистим ключем.

3. Вказати пароль доступу до особистого ключа у відповідному полі.

Якщо це апаратний ключ(токен), то вводимо тільки пароль і натискаємо «зчитати»

(ЦЕ ЄДИНА ВІДМІННІСТЬ У ПІДПИСАННІ ФАЙЛОВИМ ТА АПАРАТНИМ КЛЮЧЕМ)

Крок 1 із 3

Файловий ключ

Апаратний ключ

☐ файлова система (каталоги користувача)

Оновити

Пароль

|



Зчитати ключ

Крок 3. Перевіряємо дані ключа

В цьому кроці можемо ознайомитись з інформацією про підписанта. Після перевірки даних ключа натискаємо клавішу «Далі»

Довірчі послуги

Життя ЦЗО

Документи

Контакти

Крок 2 з 4

Перевірте дані

Клієнт ЮР-особа 12 (тестовий сертифікат)

Організація
Клієнт ЮР-особа 12 (тестовий сертифікат)
Посада
(тестовий сертифікат)
РНОКПП ЄДРПОУ
999999999 999999999

Сертифікати

ЕЦП (ДСТУ 4145)
EU-4454624186E4B187040000007C2802006F10600.cer

Протоколи розподілу ключів (ДСТУ 4145)
EU-4454624186E4B187040000007C28020070110600.cer

Назад

Далі

Що таке сертифікат?

Сертифікат є засобом підтвердження приналежності відкритого (публічного) ключа його власникові.

Сертифікат видається кваліфікованим надавачем електронних довірчих послуг та використовується для перевірки, що відкритий ключ належить саме тому власнику, чиї дані зазначено в ньому.

Файл сертифікату має розширення ".cer", зазвичай зазначені файли можливо відкрити вбудованими засобами операційної системи.

Файл сертифікату містить ідентифікаційні дані, які однозначно визначають кваліфікованого надавача та користувача електронних довірчих послуг, строк дії сертифікату тощо.

Крок 4. Підписання

Не звертаємо увагу на рекомендацію, та натискаємо «Ні, обрати інший формат»

Довірчі послуги

Життя ЦЗО

Документи

Контакти

Крок 3 з 4

Підписати та зберегти

Рекомендуємо підписувати документи у форматі ASIC-E.

Це уніфікований формат електронного документообігу, який гарантує, що ваші документи прийматимуть всі держоргани.

Так, підписати в форматі ASIC-E

Ні, обрати інший формат

Що таке ASIC?

ASIC – структурований контейнер, що дозволяє зберігати набір файлових об'єктів з пов'язаними е-підписами та/або е-позначками часу, що відповідає специфікації ZIP.

ASIC-S дозволяє зберігати один файловий об'єкт з пов'язаним е-підписом та в подальшому додавати нові. Також дає можливість додавати файли для захисту е-позначок часу.

ASIC-E дозволяє зберігати один або кілька файлових об'єктів з пов'язаними е-підписами та в подальшому додавати файлові об'єкти, файли е-підпису та е-позначки часу.

Потім обираємо формат **CAdES**. Дані та підпис зберігаються в **CMS файлі (*.p7s)**. додаємо файл який буде підписуватись, та натискаємо клавішу «Підписати»

Підписати та зберегти

Виберіть, в якому форматі підписати документ

☐ XAdES. Дані та підпис зберігаються в XML файлі (*.xml)

☐ PAdES. Дані та підпис зберігаються в PDF файлі (*.pdf)

☒ CAdES. Дані та підпис зберігаються в CMS файлі (*.p7s)

NEW! ☐ ASIC. Дані та підпис зберігаються в архіві

☐ ASIC-E. Дані та підпис зберігаються в архіві (розширений формат)

☐ ASIC-S. Дані та підпис зберігаються в архіві (простий формат)

Алгоритм підпису
DSTU 4145

Тип підпису
Підпис та дані в одному файлі (enveloped)

Формат підпису
CAdES-X Long – Довгостроковий з повними даними ЦСК для перевірки

Файл(и) для підпису:

- Заява повернення коштів для Фізичних осіб.doc

Змінити

Підписати Назад

Який формат обрати

- Що таке XAdES?
- Що таке PAdES?
- Що таке CAdES?
- Що таке ASIC?
- Що таке ASIC-E?
- Що таке ASIC-S?

Крок 5. Збереження файлу

Коли документ підписано, обираємо «**Файл з підписом**» та завантажуюмо на комп'ютер. Також можна переглянути файл без підпису.

👍 Документ підписано

⬇ Завантажити все архівом

📎 Файл з підписом
Заява повернення коштів для Фізичних осіб.doc.p7s
64.5 KB

⬇

📎 Файл(и) без підпису
Заява повернення коштів для Фізичних осіб.doc
32.5 KB

⬇

📎 Протокол створення та перевірки кваліфікованого електронного підпису від 08.12.2021
Заява повернення коштів для Фізичних осіб.Validation_Report.pdf
55.7 KB

⬇

Підписувачі

- Підписувач
- Клієнт ЮР-особа 12 (тестовий сертифікат)
- П.І.Б.
- Клієнт ЮР-особа 12 (тестовий сертифікат)
- РН ОКПП
- 9999999999
- Потрапляє до (отримувача)

Який формат обрати

- Що таке XAdES?
- Що таке PAdES?
- Що таке CAdES?
- Що таке ASIC?
- Що таке ASIC-E?
- Що таке ASIC-S?

Зверніть увагу, що Вам необхідно завантажити в пропозицію два документи – файл з підписом, типу ***.p7s** та файл без підпису.

Заява_на_участь.pdf
21.12.2021 10:17
Підпис
Заява_на_участь.pdf.p7s

Заява на участь