**Шановні клієнти!**

Увага! З 07.11.2018 року кваліфікований електронний підпис (КЕП) можна отримати **ЛИШЕ за особистої присутності підписанта.**

Будь ласка, уважно ознайомтеся з переліком необхідних документів, щоб уникнути помилок та необхідності повторного відвідування кваліфікованого постачальника електронних довірчих послуг через неправильно оформлений комплект документів!

Будьте уважні! Приймаються тільки якісні копії всіх документів (чіткі фото та розбірливий текст)

Особа, яка оформлює сертифікати КЕП для юридичної особи, **обов’язково** повинна мати при собі:

* **паспорт громадянина України у формі книжечки або ID-картки** (оригінал для ознайомлення) або інший документ, що його замінює
* **Копії документів про призначення на посаду** кожної особи, на підпис якої отримується сертифікат (наприклад, протокол засідання Загальних зборів, наказ про призначення, витяг з наказу чи протоколу, контракт та інші), має бути засвідчений на кожній сторінці керівником та печаткою, за наявності

Нижченаведені особисті документи засвідчує тільки власник цих документів. Підпис має відповідати зразку підпису в паспорті.

* **Копії паспортів громадян України** або інших документів, що його замінює, 1-2 сторінки (3-6 за наявності відміток) кожної особи, на підпис якої отримується сертифікат
* **Копії довідок про присвоєння ідентифікаційних номерів** або інший документ, який його замінює, наприклад, ID картка на зворотній стороні якої прописаний РНОКПП
* **Заявки на формування кваліфікаційних сертифікатів КЕП** в електронному (у форматі .PCK) та в паперовому вигляді для кожної особи/печатки, на підпис якої отримується сертифікат. Заявки можуть бути сформовані у програмі M.E.Doc або у вебсервісі СОТА. Керівник підписує заявку на свій підпис, бухгалтер підписує свою заявку і т.д.
* **Довіреність** — у випадку, коли співробітник юридичної особи буде отримувати тільки власний кваліфікований сертифікат від імені юридичної особи, без керівника юридичної особи
* **Платіжне доручення**
* **USB-флеш накопичувач** або захищений носій (для кожного сертифікату використовується окремий захищений носій)