

Удосконалений електронний підпис (AES): довідка про відповідність

Рівень підпису, зберігання доказів і хостинг

Оновлено 12 жовтня 2026 р.

Рівень підпису

Удосконалений електронний підпис у значенні статті 26 Регламенту (ЄС) № 910/2014 (eIDAS). Він ґрунтується на чотирьох вимогах нижче.

- 1 Однозначно пов'язаний із підписантом: у браузері підписанта створюється особиста пара ключів і видається сертифікат, що стосується лише цього підпису.
- 2 Ідентифікація підписанта: персональне посилання для підпису електронною поштою, потім одноразовий код у SMS на його мобільний телефон. Два окремі канали.
- 3 Під виключним контролем підписанта: закритий ключ не можна експортувати, і він ніколи не залишає його браузер.
- 4 Будь-яку подальшу зміну можна виявити: вміст документа запечатано підписаним геш-значенням SHA-256 і позначкою часу RFC 3161.

Надані докази

До кожного підписаного документа додається сертифікат доказів: події з позначками часу (відкриття, отриманий код, підпис), IP-адреса, номер сертифіката й відбиток документа.

Зберігання

Підписані документи й журнали аудиту зберігаються 10 років незалежно від обраного тарифу.

Через 30 днів видаляються лише дані, створені з тестовим ключем (пісочниця).

Хостинг і захист даних

Застосунок, база даних і сховище документів працюють на нашій власній інфраструктурі в Європейському Союзі (хостинг-провайдер IONOS). TLS 1.3 під час передавання та AES-256 під час зберігання. Угоду про обробку даних (DPA) за GDPR можна підписати онлайн в особистому кабінеті клієнта.

Варто знати

Кваліфікований підпис (QES) пропонується за кожен підпис через партнерського кваліфікованого надавача довірчих послуг; ця довідка описує лише удосконалений рівень.

Сертифікація ISO 27001: сертифікаційний аудит триває, сертифікат ще не отримано.