امضای الکترونیکی پیشرفته (AES): برگه انطباق

سطح امضا، نگهداری شواهد و میزبانی

به‌روزرسانی: 12 اکتبر 2026

سطح امضا

امضای الکترونیکی پیشرفته به‌معنای ماده ۲۶ مقررات (EU) شماره 910/2014 (eIDAS). این امضا بر چهار الزام زیر استوار است.

1. به‌طور یکتا به امضاکننده مرتبط است: یک جفت‌کلید شخصی در مرورگر امضاکننده ساخته می‌شود و گواهی ویژه همان امضا صادر می‌شود.
2. شناسایی امضاکننده: پیوند امضای شخصی از طریق ایمیل و سپس یک کد یک‌بارمصرف از طریق پیامک به تلفن همراه او. دو کانال جداگانه.
3. تحت کنترل انحصاری امضاکننده: کلید خصوصی قابل صدور نیست و هرگز مرورگر او را ترک نمی‌کند.
4. هر تغییر بعدی قابل تشخیص است: محتوای سند با یک چکیده امضاشده SHA-256 و مهر زمانی RFC 3161 مهروموم می‌شود.

شواهد ارائه‌شده

هر سند امضاشده با یک گواهی اثبات همراه است: رویدادهای دارای مهر زمانی (بازکردن، دریافت کد، امضا)، نشانی IP، شماره گواهی و اثر انگشت سند.

نگهداری

اسناد امضاشده و ردپای ممیزی به‌مدت ۱۰ سال نگهداری می‌شوند، صرف‌نظر از طرح انتخابی.

تنها داده‌هایی که با کلید آزمایشی (محیط آزمایشی) ساخته شده‌اند پس از ۳۰ روز حذف می‌شوند.

میزبانی و حفاظت از داده‌ها

برنامه، پایگاه داده و ذخیره‌سازی اسناد روی زیرساخت اختصاصی ما در اتحادیه اروپا اجرا می‌شوند (میزبان IONOS). رمزنگاری TLS 1.3 در انتقال و AES-256 در حالت ذخیره. قرارداد پردازش داده (DPA) مطابق GDPR را می‌توان به‌صورت آنلاین از حساب مشتری امضا کرد.

خوب است بدانید

امضای تأییدشده (QES) به‌ازای هر امضا از طریق یک ارائه‌دهنده خدمات اعتماد تأییدشده همکار عرضه می‌شود؛ این برگه فقط سطح پیشرفته را توضیح می‌دهد.

گواهینامه ISO 27001: ممیزی صدور گواهی در جریان است و گواهی هنوز دریافت نشده است.