deepsign

Your legal electronic signature for every legal standard

With DeepSign you can create three types of electronic signatures recognised by international law: qualified electronic signatures (QES), advanced electronic signatures (AES) and simple electronic signatures (SES).

	Why choose this type?	Security	Use cases
QES Qualified Electronic Signature Highest evidential value	For documents subject to "written-form" requirements under Swiss or EU law. Under Swiss (ZertES) and EU law (eIDAS), the QES is legally equivalent to the handwritten signature.	Identity verified by qualified trust service provider and two-factor identification. Accompanied by a qualified certificate issued by a qualified trust service provider (QTSP) that attests to the signature's authenticity. Proof of document integrity: any modification to the document after signing can be detected.	› Consumer credit contracts › Temporary employment or rental agreements › Assignments of claims › Consumer loan contracts › Bank account applications
AES Advanced Electronic Signature High evidential value	For documents with no statutory form requirement.	Identity verified using official ID document and one-factor identification. Proof of document integrity: any modification to the document after signing can be detected.	› Rental agreements › Purchase agreements › Employment contracts
SES Simple Electronic Signature Low evidential value	For documents with no statutory form requirement.	Low level of proof of identity.	› Quotes for suppliers › Orders and order confirmations › Digital document retention solutions

How do I know which type of signature to use?

The type of electronic signature that you need to use in each case depends on the statutory form requirements for the relevant document, your contractual agreements and your company policy. To find out the appropriate type for your specific situation, please consult with a legal advisor.

Are electronic signatures secure?

The electronic signatures used in DeepSign are issued by recognised and certified trust service providers and certification authorities. With any type of electronic signature, the document will receive a digital certificate in keeping with the currently applicable technological standard. This guarantees to both the sender and the receiver that the document has not been tampered with. In addition, when using the AES and QES, the signatory's identity is determined in advance, so that the signatory's link with the document can be traced.