eIDAS compliant authentication and digital signature service

Agrello ID is a signature creation device, which is a smartphone application that uses phone stored private keys to enable highly secure use of online services through permanent 2-factor authentication and location independent 2-factor authentication based digital signing.

For additional trust, Agrello ID is supported by other services hosted by Agrello and its partners.

Agrello ID is an authentication and digital signature solution built in accordance with the advanced electronic signature requirements set by the REGULATION (EU) No 910/2014 of the European Union (commonly referred to as the “eIDAS” regulation). The regulation is complemented by standards that are put down by a European standards organization called ETSI.

The eIDAS regulation provides requirements for trust services and electronic signature and seal services. For electronic signatures, the regulation has described two levels of electronic signatures where the first level is required to proceed to the next one.

1. Advanced Electronic Signatures
2. Qualified Electronic Signatures

Agrello ID has been built following the Advanced Electronic Signature requirements.
Agrello ID according to eIDAS Advanced electronic signatures

It is uniquely linked to the signatory

A signature created with the private key inside Agrello ID is mathematically linked to the public key of the signatory, where a standard validation formula must be used to prove its validity.

It is capable of identifying the signatory

The public key of Agrello ID is mathematically tied with an identity verification session and the same identity verification session can be tied with only one Agrello ID account.

It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control

and Agrello ID is linked to the device of the ID holder, while the private keys are also generated and stored only in that device and are protected by PIN-codes that are set by the user.

It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable

Agrello ID uses the ASIC-E signature container format (.asic) including the XAdES signature standard put down by ETSI.

This way any digital files can be signed in the way of hashing the data and signing the hash of the data with the private key of the signatory. A hash of data is a set of numbers and letters and sometimes other symbols, which is unique to that set of data and which is derived from the calculation of a hashing algorithm together with a set of data.

The signature validity is always checked by having the public key and the hash of the original data that was signed. The hash of the data can be validated by hashing the original data again to see, whether the newly generated hash matches the hash that is being validated.

ASIC-E container packs the original data that was signed and includes an XML format signature data file that includes all the data that is needed for signature validation and reference to the algorithms that were used for generating the hashes and signatures and that are needed for validation.

It is recommended for signatories to store the ASIC-E signature containers at databases, which are under their sole control. This way the validity of the signature can always be checked without any support from Agrello.

Authentication with Agrello ID is technologically the same procedure as a signature but uses a different pair of a private and a public key for extra security and legal certainty in order to clearly separate the act of accessing information (authentication) and giving consent (signing).

eIDAS is accepted as the highest standard for giving consent electronically. Nevertheless, in most countries outside the European Union a written signature is not necessarily required for giving consent – contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document. To prove a valid contract, parties sometimes have to present evidence in court. A signature system built according to eIDAS guarantees permanent existence of such evidence in a very comprehensive form.

It must be noted that each country can have specific cases stipulated by local laws, which require more or something else than a digital signature for giving consent.

In the US, digital signatures are solidified by the Uniform Electronic Transactions Act (UETA) in most states and the passage of Electronic Signatures in Global and National Commerce Act (ESIGN). Both of them establish that electronic records and signatures carry the same weight and legal effect as traditional paper documents and handwritten signatures, stating that a document or signature cannot be denied legal effect or enforceability solely because it is in electronic form. The Federal Rules of Evidence and the Uniform Rules of Evidence generally allow for electronic records and their reproductions to be admissible into evidence.