



IDENTITY PROVEN
TRUST DELIVERED



1

Security is our number one priority!

- ▶ Unlike our competitors, our digital signatures are not just based on squiggles drawn with a mouse (or your finger if you happen to be a lucky iPad user). The problem is these squiggle images can be easily cut/pasted from one document to another. That would be bad enough but it actually is much worse – these signatures don't even help detect later edits to your signed documents! So not much use if you want to later rely on these signatures when handling disputes.
- ▶ Instead we use advanced digital signatures with unique PKI keys for each one of our users. Yes, you heard correct, we don't rely on a single central server key, which can only create "proxy" signatures on behalf of users.
- ▶ Before signing users are authenticated using various options from simple username/passwords, to SMS based OTP authentication, to tamper-resistant USB tokens and smartcards (so ensuring that the signing keys are under the sole control of the owner). Because of this we are compliant with EU Qualified Signature specifications – the gold standard for digital signature security.
- ▶ By the way just, because we take security as the number one priority doesn't mean we are sloppy when it comes to ease-of-use. We ensure that security doesn't get in the way of a great user experience. Don't take our word for it, create a trial account and judge for yourself!

2

We are fully standards based, no weird proprietary stuff!

- ▶ Again unlike our competitors, the security of our solution is not based on weird server-side security logic and then having to sift through audit trail records to prove a signature was valid!
- ▶ Because we use standard PDF digital signatures (ISO 32000-1), anyone with a freely available PDF Reader can easily verify our signatures. No need to upload the document to a server get it verified or searching through reams of logs to prove a point.

3

We provide long-term signatures!

- ▶ With important documents it's essential that any digital signatures can be proven to be valid many years into the future (e.g. after the signer has left an organisation and/or their signing key has expired).
- ▶ To cater for this we create enhanced PDF signatures based on latest ETSI PAdES specifications (ETSI TS 102 778). Such signatures contain embedded secure timestamps to independently prove time of signing and also signer's status at time of signing.



- ▶ We even convert documents to PDF/A (ISO 19005-1:2005) format as part of the signing process. This is an open standard so not dependent on any particular software vendor, plus with PDF/A all fonts and other dependencies are contained within the document so it can be opened and viewed without any external resources, which may not be available in future. It's an ideal format for long-term archiving and preservation!

4

We allow reuse of existing Identity Management infrastructures!

- ▶ Our solution can utilise existing signing keys which may already have been issued to your end-user population, be these on smartcards (e.g. PIV cards, national eID cards, corporate PKI-based logical access cards, etc) or soft tokens.
- ▶ Your existing PKI (CAs, OCSP responders and Time Stamp Authorities) entities can be easily registered and trusted within our system as part of your custom Service Plan.
- ▶ SigningHub can be configured to re-use your existing signing credentials from industry initiatives such as Adobe® CDS program, Identrust® and SAFE-Biopharama.

5

We understand the flexibility that real-world business application need!

- ▶ Although we provide a cloud-based web service here, you may prefer to run your own internally hosted service, if so no problem just license the technology.
- ▶ Features such as delegated signing, department/role based signing and batch signing ensure the solution fits in within your business processes rather than the other way round.

