HOW TO CHOOSE A PROVIDER FOR E-SIGNING SOLUTION

: a checklist

When choosing an e-signing solution, there are a number of things to consider in order to ensure the security of your documents and data. Here's a checklist to guide you through the most important things.

01 LEGALLY BINDING E-SIGNATURES

According to the eIDAS regulation, defining the usage of e-signatures in Europe, only qualified e-signatures are equivalent to handwritten signatures, and therefore have indisputable legal force. Make sure e-signing provider allows to create and validate e-signatures with qualified certificates that comply with eIDAS regulation, without any additional conditions, such as custom plans, only on-premise solutions, limited eID tools, and similar, as this usually means that not all offered services by the provider meet high-level assurance e-signatures. Be careful not to slip on only supposedly declared compliance to eIDAS.

02 QUALIFIED TIMESTAMPS

To make sure your documents are secure and tamper-proof, consider using a service provider that uses qualified timestamps in all document signings. This will ensure security against forgery and backdating.

03 LONG-TERM VALIDITY OF SIGNATURES

E-signatures have their expiration date. In order to guarantee the trustworthiness of e-signatures with qualified certificates through time, double-check whether the service provider offers long-term preservation service – you won't have to worry after some years about needing to find an additional service provider for this.

04 HIGH AVAILABILITY OF SERVICES

The availability of services and their track record moderately indicate the solution provider's commitment to make sure the entire service infrastructure is monitored and works uninterrupted, thus securing your business continuity. The higher provided service availability and — more importantly — its actual track record, the less you should worry that the systems won't work when you need them the most. Don't forget to double check the service provider's responsibility on this, i.e., what actions and compensations they offer if the service is down after all.

05 MEASURES TO ENSURE INFORMATION SECURITY

Information security measures in place make sure your data is protected. Look for a solution provider that has an implemented Information Security Management System of their own, which is audited and certified by independent accredited auditors. Be extra careful here as it is easy to get confused: sometimes service providers use data centers with implemented assurance programs, however, those by no means determine the information security management practices of the service provider itself.

06 TRANSPARENCY

Transparency equals trust. Check how much and what kind of information about the company's compliance is available publicly. To make sure you're on the right track, third-party certificates, certification statement of applicability, audit reports, policies on data processing, and other legal documents are the things you should look for. The more transparent the company is, the more sure you can be that they have nothing to hide and are not drafting different answers about their operations you or other potential customers want or need to hear.

07 QUALIFIED VALIDATION SERVICE

If you are about to use e-signatures, you need to make sure you are able to check their validity. Choose a solution that has a built-in option for validation of e-signatures or is able to offer a side service for that. However, you want to make certain that the service provider holds responsibility for the validation process and results provided, so make sure to check their signature validation policy, as well as the responsibilities and liabilities defined in it. As validation of e-signatures and e-seals is a regulated area, choose an eIDAS-certified qualified service since only qualified validation services can be fully trusted as established by eIDAS regulation.

08 VARIETY OF DOCUMENT FORMATS AND EIDS

Before choosing your e-signing and signature collection service provider, check what kind of document formats they support because although there is an internationally recognised format in Europe, each country has its own format as well. The variety of supported eIDs, besides the ones that you are going to use, might also be important if you are planning to sign documents cross-borderly.

09 FRIENDLY USER EXPERIENCE

If you are ready to go digital, you want to make sure the system you choose to sign your documents at is user-friendly, intuitive, and works on multiple operational systems and devices, so you don't need a user manual and the switch of your processes is as smooth as possible. This is also extremely important if you are choosing a platform to collect signatures from your clients – customer experience is too important to compromise on.

10 CONFORMITY TO YOUR NEEDS

However secure and compliant the solution might be, it won't matter if it doesn't conform to your needs. Make sure your chosen provider offers whichever you need, either a cloud-based or an integrable into your own systems solution, plus all the additional features you might need, whether it's a branded user experience, workflows, or document forms.

11 COMPANY REPUTATION

Although all of the above are strong proof that you've found a solid provider, their reputation can be the last confirming factor to look at. The list of well-known names as their clients and positive reviews can help you support your choice.

COMPARE E-SIGNING PROVIDERS

Use this cheat sheet to easily compare your shortlisted e-signing providers.

	Dokobit By Signicat		
Legally binding e-signatures	Dokobit works with: • **Qualified Electronic Signatures** that have the same legal effect as handwritten signatures • **Advanced Electronic Signatures** that are considered as a strong evidence in court • **Simple Electronic Signatures** that do not require strong signer authentication but are nontheless founded on the signer's consent		
Qualified timestamps	• Dokobit uses **qualified timestamps** in every document signing		
Long-term validity of signatures	• Dokobit has all the means to ensure **long-term preservation** of electronic signatures on all the documents when needed		
High availability of services	• Not lower than **99,95 % service availability** • **History** of service uptime available here • Uptime monitoring provided by an independent monitoring software Pingdom • In case of downtime Dokobit applies **discounts** for a monthly invoice (additional conditions apply)		

Measures to ensure information security	• Dokobit has an implemented **Information Security Management System** (ISMS) in place • **ISO/IEC27001 certification with the certification** scope of "cloud-based services for e-signing, e-sealing, e-identification, validation of e-signature and e-seal, and related software development, delivery and support". Certificate available here • **ISO27018 certification** that focuses on the protection of personal data in the cloud. Certificate available here • As a Qualified Trust Service Provider Dokobit ISMS conforms to the European standard **ETSI EN 319 401** • **Audited every year** by two globally respected audit firms: Bureau Veritas (for ISO certificat on) and CSQA (for ETSI certification)		
Transparency	• **ISO/IEC27001 certificate** available here • **ISO27018 certificate** available here • **Certification statement of applicability** is available upon request • **Service availability** available here • **Insurance certificate** can be found here • **All legal documents** (Terms of Service, Data Processing Agreement, Privacy Policy, etc.) available here		
Qualified validation service	• **Qualified Trust Service Provider** supervised by Member State Supervisory Body (Communications Regulatory Authority of the Republic of Lithuania) and included in the **EU Trusted Service List:** see here • **Qualified Trust Service Provider certificate** available here • **Signature Validation Service Practice Statement and Policy** can be accessed here		

Variety of document formats and eIDs	• Dokobit supported **document formats: international** (PDF, ASiC-E) and **used in the Baltics** (BDoc, EDoc and ADoc) • Dokobit supports the variety of eIDs used in Europe, from national ID cards to other notified eID scheme tools. The entire list of supported eIDs can be found here		
Friendly user experience	• Dokobit signing and signature collection solutions are built on **Dokobit Portal**, it's **demo** is available here • All Dokobit solutions are **mobile-friendly** • Dokobit portal is available for all iOS and Android users via **mobile app**		
Conformity to your needs	Dokobit offers: • an **all-in-one online portal** for document signing and signature collection. Its full feature list is available here • **integrable into your own systems solutions** for e-signing, e-sealing, authentication. More information available here		
Company reputation	• Dokobit is **trusted by various businesses across Europe**, from financial sector and telcos to automotive sector and retail. Learn more from Dokobit customers here		