CRYPTOMATHIC

Adopting a Global eSignature Strategy for Large Banks and Financial Services

‘Think Globally, Act Locally’: Pragmatic advice when planning an eSignature solution roll-out

A Cryptomathic Business Guide

Introduction

Global insurance providers, banks and other large corporations operate across several jurisdictions but usually consider digitalization as a global initiative to drive growth and innovation.

Digital signatures are an important component for enabling an end-to-end digital customer journey with legally binding consent, e.g. executing contracts. The EU regulation on electronic identification and trust services for electronic transactions, AKA the eIDAS regulation, is a strong growth-driver for the uptake and usage of digital signatures, as it provides very high assurances for digital signatures. The digital signature standard with the *highest* assurance level and legal value is known as the Qualified Electronic Signature (QES) standard. When digitally signing a transaction or a contract, a QES is legally equivalent to a handwritten signature in all EU countries, where the regulation is enforced.

In other jurisdictions, local eSignature laws apply, and contracts governed by a given jurisdiction must be executed in accordance with the requirements applicable in that country for that type of contract. It is difficult to find an eSignature solution provider that can provide a single technical solution and at the same time comply with various local signature laws, contract fulfilment formalities and data privacy requirements. Here we offer the advice of “Think Globally, Act Locally” to organizations eager to adopt a successful digitalization & eSignature strategy.

Think Globally

For organizations with an international reach, it makes perfect sense to think of eSignature services on a worldwide scale since these capabilities can be a key enabler in their global strategy. Strong capabilities can have positive effects on several areas including:

- **Digitalization initiatives:** eSignatures allow for strong non-repudiation and legal assurance in digitalization initiatives. With integrated digital signatures, business owners can offer more convenience, mobility and streamlined services to their clients.
- **Sustainability objectives:** eSignatures mean less paperwork including reduced paper consumption, shipment, scanning etc. When deployed on a large scale, the savings can be enormous.
- **Better compliance and assurance:** Demonstrating the willful consent of a user or customer to a transaction or document is a key question. Certain transactions (e.g. a loan or legal contract) require handwritten signatures or their digital equivalent. Only a Qualified Electronic Signature can provide this with full confidence and remote digital signatures offer the most convenient form factor to achieve the highest assurance level.
- **Increased agility:** Acquiring new clients and ensuring that their demands, in terms of mobility, are met is critical to many organizations. Whether it's digital on-boarding at the local branch or remotely, it is important to have an eSignature strategy with a compelling user experience that's tightly integrated in all business workflows.

For a global eSignature strategy, it's crucial to ensure the solution can address the use-cases of the different departments inside the organization in all countries where you operate.

Usually, the corporate IT team opts for a single technology that is flexible enough to allow for different workflows, layouts and local customization options. By leveraging a single technology, they can lower the implementation, integration and operational costs drastically. This applies to solutions such as SSO, document management systems, eBusiness portals with multiple workflows, etc. That said, the CISO will have to define some logical separation procedures to segregate data in different booking centers and enforce compliance against local data privacy requirements and IT governance principles.

Business cases should come first

To ensure a smooth project it will help to think clearly in advance about the business drivers. We would suggest the following methodology: assign a few business analysts and ask them to draw a list of all business cases which could benefit from the solution, e.g.

Use case	Motivation	Volume	Integration constraints	Assurance required	Business benefits
(Describe use case in a few words)	(Mention the key driver underlying the need for eSignature)	(Rough number of docs / transactions per year)	(Integrate with local applications (user management, web portal) etc.)	(Non-repudiation only or advanced, qualified as per given signature law)	(Use a scoring method to help prioritize your needs using criteria*)
e.g. let users sign insurance claims online	e.g. efficiency, legal certainty and non-repudiation	e.g. 50 000 claims	e.g. integrate with internal DMS and start workflow from My Insurance	e.g. minimum advanced as per eIDAS in EU + CH + Turkey. Compliance with signature law of SG required	e.g. this is important to address

* the scoring can be calculated by multiplying points e.g.

Use case	Motivation	Volume	Integration constraints	Assurance required	Business benefits
	Must have: 10 points Strong add-on: 5 points Nice to have: 1 point	More than 50K: 10 points More than 20K: 5points Less than 1K: 1 point	2 applications or less: 10 points 5 applications or less: 5 points More than 5 applications: 1 point	Qualified (or equivalent): 10 points Advanced: 5 points Only non-repudiation: 1 point	Multiply the points obtained and set some thresholds.

If this is applied on a global scale, you will obtain, in a couple of weeks, a full list of the use-cases and a first-order priority list of where the greatest benefits are to be won. This information will be a valuable asset when presenting to a CISO and for discussions with potential vendors and partners.

The User Experience – essential for success

Another important aspect to consider in your "Think Globally" strategy is that whichever eSignature solution is selected, it needs to convey and support the same trust and confidence your customers and partners have in your global brand.

Providing an enhanced user experience is key to ensuring strong and positive user acceptance - allowing for a smooth migration from centuries-old handwritten signatures to the digital age. Delivering a delightful UX will increase your brand value; get it wrong and users will be very public in their criticism and quick to migrate to other providers. Here is a summary of dos and don´ts based on our experience.

Dos	Don'ts
Build the eSignature process into a workflow that the user is familiar with.	Add a separate signing portal (internal or external) to redirect the user (you could lose the customer).
Leverage the fact that you know most customers - you can often offer Advanced signatures for many cases, so implementing a mix of Advanced and Qualified signatures may be advantageous.	Think that you need to offer Qualified signatures or nothing. Advanced signatures can often serve most of the cases.
Look at the most promising use-cases first, using a lean approach and implement the others later.	Be overly ambitious and think that you can go live with all use-cases at once: the risk is they will be dilute solutions and late.
Make sure the users are aware that they are signing a document with a digital signature. Lack of awareness impairs user acceptance.	Assume that all users will understand the terminology and significance of 'digital signing'.
Keep control over your data.	Forwarding of the document or user data. This can be troublesome as it extends your GDPR scope.
Add your branding to the signing user experience.	Include unnecessary third-party branding within the signature portal. The branding of a third party will reduce the perception that the user has in your brand.
Adopt a modular approach with clear functional scope - ensure the business app is in charge of the workflow.	Overengineer – one signature UX can typically fit all your needs.
Reuse what you have: e.g. your SSO and DMS can be reused.	Invest into additional unnecessary or duplicate technologies.
Use mobile friendly technology.	Require users to download and install additional software or drivers.
Enable signature activation with minimal clicks or typing.	Use signature pads – the rendering is too poor and the total bill is expensive for little assurance in return.
Use form fields to allow for documents with dynamic layouts and multiple signatures.	Think a document is static only.

Additional tip: if the volume justifies it, we can help you become a TSP as you may realize that you already perform large parts of the trust services (audited KYC processes, rigorous IT Management with strong focus on security to demonstrate non-repudiation, insurance coverage, etc.). This does not necessarily require that the entire IT infrastructure is operated by your organization.

Act Locally

Even if the technology stack can be centralized in one location to provide global services, compliance must be handled in accordance with local laws and regulations. It is also important to get the local business stakeholders on board to ensure that they adhere to the digital transition and prepare or adjust their workflow to take advantage of an eSignature service.

Here is a list of some items which local business stakeholders need to consider:

- A strong assurance level requires strong customer identification procedures. It is therefore important that the KYC process is adjusted to meet the requirements with local signature laws.
- Documents need to be amended to automate where the eSignature “stamp” is placed within the document. A human eye can quickly detect where the signature needs to go – a machine will now need to parse the data to know where to place the signature object.
- Try to know what fulfilment level is required to execute the contract.
- Centralizing documents in a DMS to serve several business cases without reinventing the wheel. Integration is much easier with access to a central document pick-up point.
- Educating client-facing staff to make them aware of the new functionality and show that it can reduce the administrative part of the job so they can focus on their core function.
- Integrating the signature client inside the local business applications.

Local Jurisdictions

When operating globally, it is important to consider the jurisdiction covering the client relationship. If we take a global wealth management bank as an example, a client of a Swiss booking center will have contracts ruled under Swiss law and should get a Qualified Electronic Signature (QES) which is valid under Swiss signature law (i.e. ZertES). For this to happen, it is important to select a Trust Service Provider (TSP) to issue certificates valid under the law ruling the contract / eBanking relationship.

Cryptomathic Signer supports multiple policies and we can source certificates from multiple providers in different jurisdictions including the EU, CH, SG, HK, US, BR and more.

While the Qualified Electronic Signature standard is primarily a European concept, other jurisdictions have set related standards. Some examples are:

- Singapore requires secure electronic records and secure electronic signatures. ETA Part III to be granted the best legal effect. https://sso.agc.gov.sg/Act/ETA2010
- For Hong Kong (and China - thanks to a bilateral agreement) all Electronic Records / Contracts signed using digital signatures supported by a recognized certificate will be granted a legal effect Part III of the ETO https://www.elegislation.gov.hk/hk/cap553!en?xpid=ID_1438403431885_004

Contact Cryptomathic for questions on other jurisdictions.

As mentioned above, a customer is typically attached to one or several booking centers and can be given a certificate to sign a contract which will be valid under that jurisdiction. The client may however not always be located in the country of the booking center and this can lead to some challenges. In certain situations / countries, you may be asked to provide evidence that a digital transaction / signature effectively took place in the country / jurisdiction where the bank is registered.

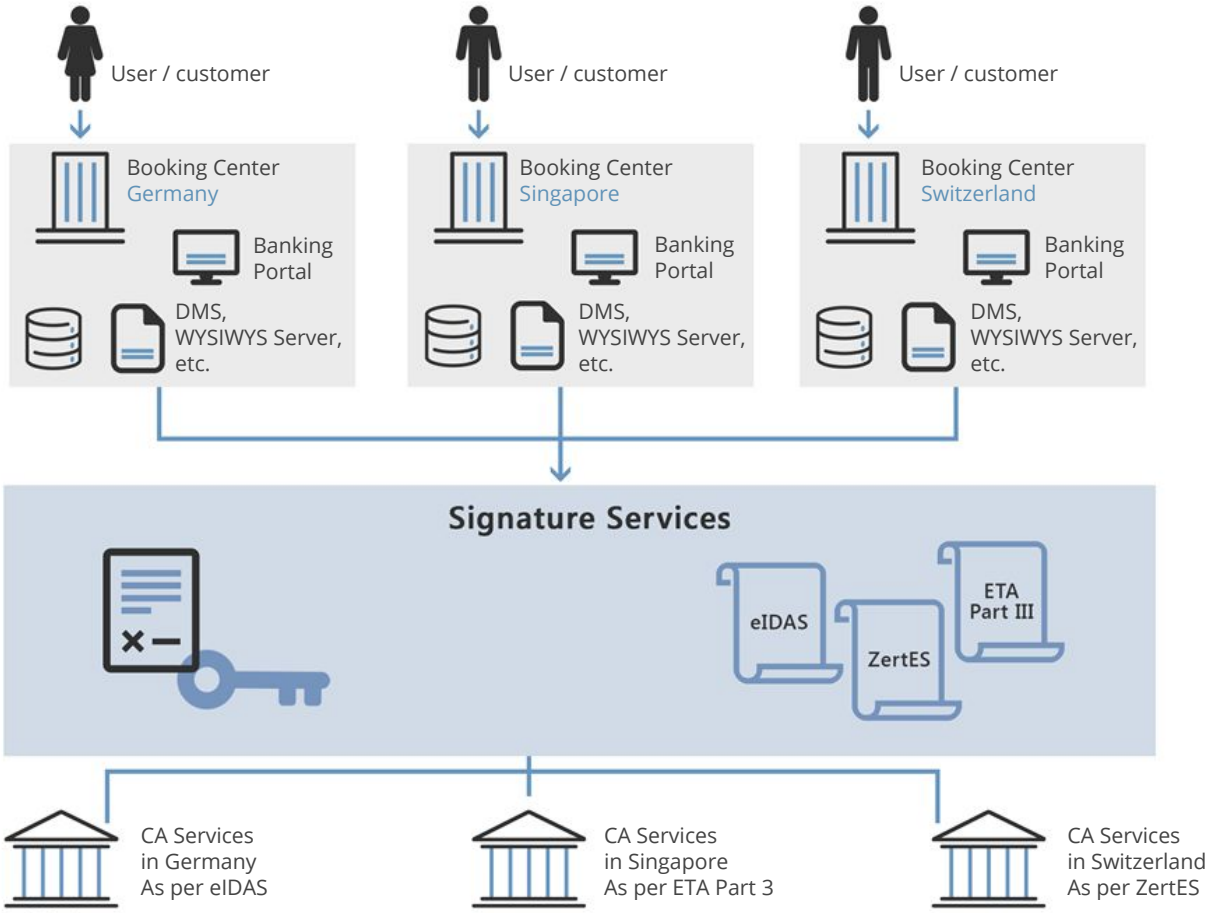
With Cryptomathic Signer, we tackle this with installing the WYSIWYS server (What You See Is What You Sign) in the local booking center(s). In this way, we can ensure that the document is present in the booking center at time of signing. The users/signatories are only given a visual representation of the document, which they can provide their consent to / sign remotely, but the signature value is effectively added to the document in the location & country of the booking center. In the PAdES signature profile of the signed document, we can then specify the location of the booking center and an auditor can inspect the logs of the WYSIWYS server to verify that the document remained in the booking center at the time of signing.

Cryptomathic Signer - One Solution, Multiple Policies

Cryptomathic Signer is a remote digital signature solution, incorporating Cryptomathic's certified Qualified Signature Creation Device (QSCD), which abstracts all the complexity and helps banks, governments and trust centers provide a smooth digital signing experience to their clients. With Signer, organizations can offer a highly versatile, non-repudiable and legally binding signing service.

Cryptomathic masters the legal and technical standards so that your signing service can provide both Advanced Electronic Signatures (AdES) and Qualified Electronic Signatures (QES) anywhere in the world.

The Cryptomathic Signer solution is best positioned to enable global providers to implement a global eSignature strategy and is designed to be most cost-effective for large scale operations, allowing for on-premise signature services integrated with existing business workflows. The diagram below illustrates how a central e-Signature service, using Cryptomathic Signer, can support multiple policies for different jurisdictions to deliver a truly global e-Signature solution with the highest possible assurances. Signer's WYSIWYS component ensures the digital signature is added in the country of the booking center.



In addition, the WYSIWYS design strengthens non-repudiation and offers an elegant signature experience so that end-users may sign PDF or XML data from a browser or smart phone and can recognize the signature afterwards.

Thanks to Signer's multi-instance / multiple policy concept, it is possible to serve customers in different jurisdictions, with various assurance levels in accordance with business requirements and local prerequisites in regards to contract fulfilment and execution. The central signature service can thereby be segregated and be linked to several CA services to ensure legal certainty in all circumstances.

Contact your Cryptomathic representative or email us on enquiry@cryptomathic.com for more details.

Further Reading

Additional collateral on Cryptomathic Signer is available via www.cryptomathic.com.

Read the White Paper:
eIDAS Compliant Remote eSigning
Download the Case Study:
UBS Deploys Qualified Electronic Signatures

About Cryptomathic

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV and Crypto & Key Management through best-of-breed security solutions and services.
We pride ourselves on strong technical expertise and unique market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of world renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as long-standing clients.