CRYPTOMATHIC

Guidance on Achieving Qualified Remote eSigning

Navigate legislation, technology and security challenges to deliver user freedom and confidence

A Cryptomathic White Paper

Abstract

The ability to offer an end-to-end digital service with legally binding user consent can reduce costs, increase security and offer greater confidence in transactions. Digitalization enables paperless processes, which reduce emissions and support sustainable business growth.

eIDAS (electronic Identification and Trust Services) legislation offers the promise of digital signature acceptance and legal assurance throughout the European internal Market – giving freedom to users and transparency to service providers. On a global scale, complying with the ETSI and CEN standards behind eIDAS is becoming increasingly important for remote signing.

There are, however, challenges to offering an attractive, seamless and legally binding digital signing experience: How can you or your users be sure exactly what they are consenting to when they commit to sign a document or transaction? Will a solution disrupt existing workflows? How will a solution integrate with existing IT infrastructure and services?

This white paper presents the benefits of remote e-Signature technology and offers guidance on navigating the technological and regulatory challenges. Clear, pragmatic advice is given to help assess the different solutions available. The apparent complexity of the eIDAS legislation is exposed to give clear information about what components of an e-signature solution must be certified - and to which standards - to obtain the full legal benefits available.

The security of any proposed solution must be carefully assessed – we give concise information about best practices to ensure the integrity of this vital business process.

Cryptomathic's Signer product offers a secure digital signature solution for remote signing, delivering the highest assurance of Qualified Electronic Signatures (QES) combined with a seamless user experience. You can confidently assert who gave consent to which transaction and provide legally admissible evidence when required.

Available in different commercial models to suit the requirements of your business, Cryptomathic Signer delivers user mobility combined with a high assurance infrastructure and integrates easily with your existing systems and processes.

Introduction to electronic signatures

An electronic signature refers to data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to indicate their approval or commitment to the content. A digital signature is a specific technical implementation of electronic signing by applying cryptographic algorithms. Profiles for digital signatures and their legal implications deviate from region to region.

In general, there are two different methods for generating secure digital signatures, 1) Local signing using smart cards, where users must retain and protect their private signing key, or 2) using remote signing technology, where the users' private signing keys are stored and protected in a central location but can be accessed remotely by the user.

For electronic signature usage in Europe, there is a strong drive towards remote signing solutions compliant with eIDAS legislation. This paper examines the two main digital signature standards that provide the strongest legal value: the Advanced Electronic Signature (AdES) and the Qualified Electronic Signature (QES).

Secure digital signatures that provide proof of 'who signed what and when' also benefit markets with other legal frameworks or regulatory requirements.

Business drivers for remote digital signatures

There are various business benefits to be realized through implementing electronic signature services that allow remote digital users to consent to contracts and transactions in a legally binding manner.

Bring online what was previously offline

Being able to communicate electronically rather than by paper can deliver significant savings for governments, companies, individuals and the environment. A final hurdle to overcome is the ability to commit and be held liable for a transaction without resorting to a 'wet' signature: to keep the entire process digital whilst benefiting from the same legal weight of the traditional handwritten signatures.
All stakeholders can benefit from such a move, including:

The business domain

- Ensure higher conversion and greater satisfaction rates for clients with a seamless, no paper, user experience

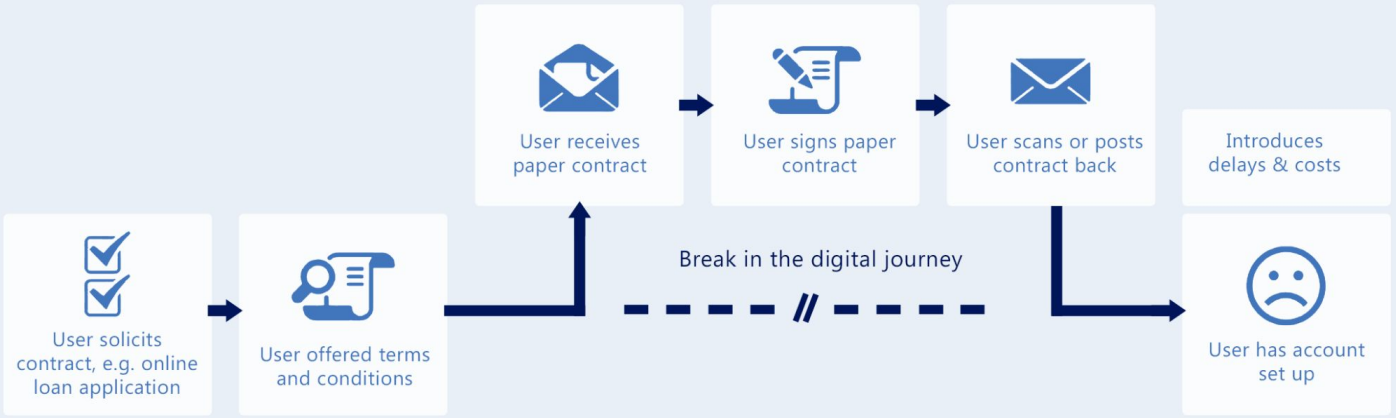
- Reduce cost and approval times with a fully digitalized process
- Improve sustainability – going paperless helps reduce office expenditures and all the hidden costs and environmental impact around printing, shipping, scanning, archiving and managing multiple copies of paper documents
- Enable new business offerings – a flexible solution can be extended to deliver new services or access new customers.

The legal and compliance functions

- Gain a confident legal position – frameworks such as eIDAS and the use of Qualified Electronic Signature (QES) can ensure digital signatures that are legal equivalent to a hand-written signature
- Achieve cross border recognition - eIDAS can also give interoperability across national boundaries within EU, to reduce legal complexity
- Reduce risk - a system that delivers QES provides effective nonrepudiation, reduces liability and exposure to challenges about exactly who consented to what & when.

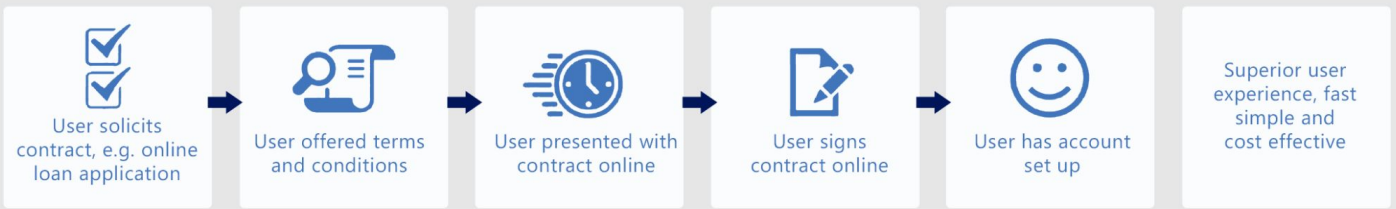
TRADITIONAL USER JOURNEY

User falls back to paper and pen when legally binding contract is required



END-TO-END DIGITAL USER JOURNEY

User enjoys an unbroken digital experience while giving immediate and legally binding consent



IT and integration

- Reuse systems – such as 2 factor authentication systems for efficient utilization of existing infrastructure and services to significantly reduce deployment costs
- Ease integration and access - solutions allowing zero-footprint, browser-based signing reduce configuration headaches & security concerns
- Enhance security and integrity – Advanced and Qualified Electronic Signatures ensure data integrity, security and control of online transactions and documents.

Market sectors & use cases

The need to offer legally strong and convenient user approval exists across many different markets and applications. Some of the most common areas are:

Banking and finance

Most banking processes, ranging from loans to credit card applications, require an authorizing signature from the end-user. Producing, handling and storing large amounts of paper documents is time-consuming, expensive and has negative environmental impacts. Digital signatures can deliver data integrity and non-repudiation required to go paperless through digital banking services. Online transaction processing can also benefit from QES to guaranty integrity protection and user intent in a PSD2 context.

E-government

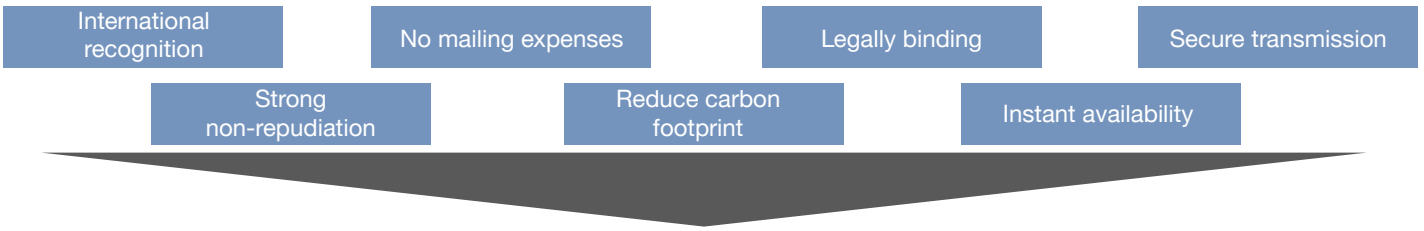
The processing of paper-based documents is error prone and resource intensive. Digitalizing the interactions between governments and individuals and organizations will minimize errors, delays and costs. Digitalization can also establish closer relations between a government and its citizens. Many countries have launched initiatives where a common Identity, authentication and Signature scheme is shared between the private and public sectors.

Legal documents

It is a common requirement for individuals or businesses to apply their signature to a document in order to legally commit to a contract. It is also common practice to have multiple signatories on a contract (multi-signing) or to sign multiple documents at once (batch signing). Digital signatures can help simplify and speed up these procedures. Legal documents typically need to be archived or stored for long term preservation. The cost of storing and accessing digital documents is far lower than their paper equivalents.

EU Regulations - eIDAS

There are different regulatory standards on e-signatures throughout the world. In this section we explore the EU regulation known as eIDAS. The eIDAS regulation offers a common legal framework to make it easier for citizens, businesses and public authorities within the EU internal market to use Electronic Identification and secure digital services. eIDAS is a strong digitalization driver, which gives qualified electronic signatures the same legal status as



those that are paper-based, thereby enhancing the confidence and integrity of e-transactions.

Since 1st July 2016, the regulation has been enforceable across the EU, replacing the previous directive on electronic signatures. It has been undertaken to steer the 'digital enablement' of traditional paper-based services. e-Signatures lie at the heart of the eIDAS regulation which defines the legal framework and the prerequisites for providing, certifying and using (qualified) trust services across the entire EU including EEA countries. The establishment of common rules and technical standards are the key to making it happen.

eIDAS classifies two types of secure electronic signatures: Advanced and Qualified Electronic Signature. Cryptomathic provides remote signing solutions for both types.

Advanced Electronic Signatures (AdES)
Under eIDAS, an electronic signature is considered to be advanced if it has met several requirements, including:

1. It uniquely identifies and links to its signatory
2. The private key used to create the electronic signature is under the sole control of the signatory
3. If the data is tampered with after the message has been signed, the signature must identify that this has happened
4. Invalidating the signature in the event its accompanying data has changed

Note that Advanced Electronic Signatures do not benefit from cross-border recognition, this requires a Qualified Electronic Signature.

Qualified Electronic Signatures (QES)
A Qualified Electronic Signature is an Advanced Electronic Signature that has been generated by a qualified signature creation device and has a qualified digital certificate attached to it. The qualified certificate is issued by a qualified trust service provider, and it attests to the authenticity of the electronic signature to serve as proof of the identity of the signatory.

Simply put, a qualified electronic signature increases the level of security over that which an advanced electronic signature provides. By law, it is considered as the equivalent to a handwritten signature within the EU.

Liability
A business application that does not require a user's signature may be exposed to legal challenges from both the user and third parties.

By using an advanced electronic signature, the burden of proving intention or negligence lies with the person or legal entity claiming the damage. By using a qualified electronic signature, the trustworthiness of the signature process is legally assured.

The eIDAS regulation thus enforces a liability shift: in case of legal proceedings, the business providing the application is not liable for the fact that a document or transaction was signed or approved by a user, this liability is passed through to the appropriate Trust Service Provider.

The business benefit for a bank or merchant is the opportunity to reduce the appropriate insurance coverage significantly.

Data integrity and non-repudiation

Under pressure from sophisticated attacks and rising fraud, many applications providers use 2-Factor Authentication (2FA) technology to mitigate risks of identity theft. An important security requirement, which 2FA does not address, is the possibility to offer transaction data integrity and non-repudiation. Application developers will typically wish to solve these two problems pragmatically and with a well understood risk profile.

The most elegant way to ensure transaction data integrity is to implement a digital signature. The legal value conveyed by a digital signature is significant. It is essential to prove integrity: meaning one is sure the data/document received is unaltered while in transit. If challenged in court, a judge should be confident that the data/document is complete, has not been amended and nobody is able to reject its integrity.

Non-repudiation is the assurance that someone cannot deny the validity of something. In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

A digital signature is the ideal mean to achieve non-repudiation. In case of litigation, the application provider or signature generation service provider must be able to provide sufficient evidence that the process was duly performed by the user in a non-repudiable way, and must be able to provide the entire audit trail to demonstrate this. Many organizations including the European Central Bank and the US Internal Revenue Service mandate service providers to implement means to ensure and demonstrate non-repudiation.

For non-repudiation to be exhaustive and accepted beyond reasonable doubt, three challenges need to be solved:

1. Ensure that the signature key is bound to an identifiable individual (natural person) or organization (legal person/entity)
2. Guarantee that the end user has sole control over his/her private key used for signature operations
3. Provide strong confidence that the document or transaction the user is committing to cannot have been tampered with.

These three aspects are discussed later in the security and compliance section of the document.

Checklist for e-signature solutions

When assessing e-signature technology, careful consideration needs to be taken to ensure the visible and hidden costs of a solution balance against the value of solution that is offered. The following aspects need to be considered:

User experience
What confidence can an end-user be given that they are consenting to the transaction they are presented with? (protection from spoofing) How much freedom is given to the choice of device (desktop or mobile) that can be used?

Security
How strong is the system design to protect against tampering and subversion of documents and processes? Does the system make use of trusted hardware (HSMs) to protect vital cryptographic material and sensitive processes?

Legal admissibility
What promises are given regarding the strength of signatures in a court of law? For the European market – does this system offer full Qualified signatures and compliance with eIDAS regulations? What quality of audit materials is provided to prove a transaction took place?

Integration effort
How well will the solution integrate with existing applications and processes?
If desired – can existing user-authentication methods / tokens be reused?

Scalability / Extensibility
Can the solution be scaled to meet the needs of the business? Are there different deployment models to available to address different business priorities – e.g. hosted vs. as-a-Service models?

Reputation and experience
Does the vendor or partner have high quality references available in the relevant market sectors? Does the vendor or partner have credibility with certifications at the highest assurance levels?

Introducing Cryptomathic Signer

Signer is a secure digital signature server solution that offers eIDAS certified remote eSigning, giving users the freedom to digitally sign documents at any time, from anywhere in the world, on any device. Cryptomathic Signer is a strong enabler of large organizations' digitalization strategies. Signer offers enhanced security, ease of deployment and user mobility with remote signature generation. It is a zero-footprint signing technology that can offer an appropriate security assurance level while being compatible with all types of devices. Cryptomathic Signer can be used to generate Advanced or Qualified Electronic Signatures (AdES or QES).

Cryptomathic Signer allows for easy integration with web application servers and can leverage existing 2FA deployments.

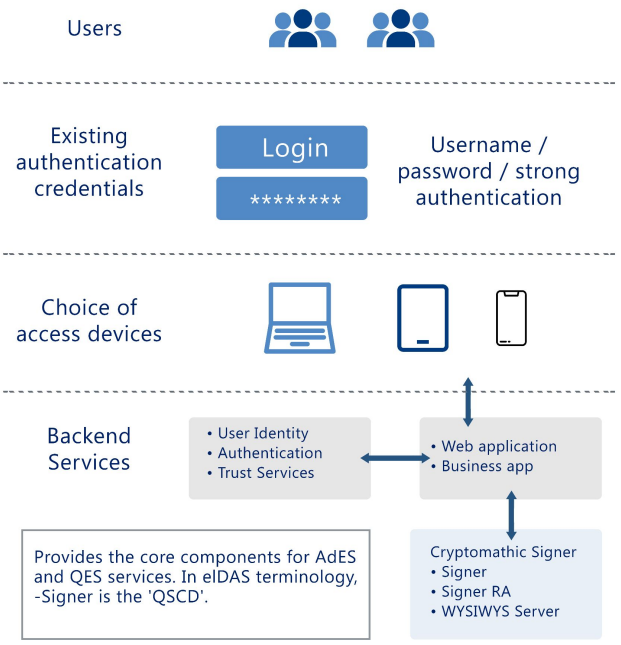
Deploying Signer - functional overview

Signer offers different integration options with existing applications, systems, processes and user-workflows - based on your requirements. The illustration on the right is a general overview of the entities in a remote signing service.

Signer: end-user experience

Users typically start by logging into a web application that controls the business workflow. When a document needs to be signed, the user is invited to click on a "View and Sign" button. The document is automatically prepared and securely rendered into the browsing session using Cryptomathic WYSIWYS technology which acts as "trusted viewer" for user confidence and non-repudiation. WYSIWYS ensures that only the authentic document can be signed by the user.

The user can view the document again before committing to it. To ensure only the correct user can generate their signature, the user is required to use strong authentication to invoke and authorize the signature operation.



Once the signature is generated, it is then embedded into the PDF or XML document in a standard format so that the user or any relying party may validate the signature afterwards.

Behind the scenes

To commit to a document or a transaction, the user routes a signing request to Signer, authenticates him/herself (using strong authentication) to retain remote control over their signing key. The signing key is stored centrally in the secure, tamper resistant/ evident environment. Signer then generates the signature value and returns it to the client for secure embedding into the document or transaction using the appropriate signature profile. Cryptomathic Signer offers a direct path from the browser into the hardware security module (HSM) holding the user´s key using an advanced security protocol.

Why Signer?

Signer uniquely offers the combination of:

- Excellent user-experience: on desktop, tablet & mobile devices
- Compliance with European standards for issuing advanced and qualified electronic signatures
- Ability to reuse existing 2-factor authentication methods
- Full audit-trail of what was signed, when and by whom supports strong non-repudiation
- Protection against tampering with What You See Is What You Sign (WYSIWYS) technology
- Reduced operational costs compared to paper based and other e-signature solutions
- Support for different business models: can be provided as a complete solution on premise, as a hybrid managed service or in a pure service mode.

Commercial models

Different customers will vary by size, technical capacity and have their own preferred business model. Signer's secure and adaptable architecture makes it ideal for most applications requiring remote signing. Signer can be deployed in different arrangements to suit the desired business model. It also offers flexibility to organizations that wish to provide 'signing services' as a commercial offering.

Cryptomathic Signer can be deployed in three main commercial models:

A) On-Premise: Where the entire solution is installed on premise. An organization, such as a trust service provider (TSP), wishing to offer a signing service to its customers, acquires the certified QSCD and internally hosts all the supporting infrastructure.

B) Hybrid Signing Service): Where the organization, such as a bank, offering signatures to their end-users, integrates the modules within their applications, while the TSP elements are consumed as a service.

C) Fully Managed TSP: Whereby the customer receives a full service. Signer is offered as a fully managed service by a TSP for delivering a QES service to the market.

The different models offer flexibility in where liability resides and also address different appetites and abilities to host services as well as time to market (see overleaf).

Liability implication for different models

Model A On-Premise	Model B Hybrid Signing Service	Model C Fully Managed TSP
Cryptomathic offers some software license and specialised hardware for use of the Signer/ WYSIWYS/authentication technology to be fully installed in the customer's data centre.	Cryptomathic delivers a service on your behalf and operates some of the IT infrastructure (CA, Signer, HSMs, etc.) The customer deploys and manages the integration in their own systems including the WYSIWYS, etc.	A TSP offers trust services (OES, Sealing, time stamping etc.) branded under the their name with the corresponding policy.
Cryptomathic delivers software, hardware, prof services to integrate the solution into your environment. You are then responsible for the SLA (backed up with a maintenance and support contract).	Cryptomathic hosts the solution and delivers a QES service under high SLA to integrate with your existing infrastructure.	The TSP delivers an SDK to integrate with your application and exposes an interface with a high SLA.
You are free to use your own CA or Cryptomathic's partner services. The CP/CPS are then in charge of the CA service provider regulated on a national level.	You may decide the CA Name and the general terms incl. CP/CPS depending on requirements.	The CA Name is that of the TSP and so are the general terms incl. CP/CPS which can be adapted upon request.
You become a TSP in the eyes of the public and are legally responsible for the services provided to the end users and in charge of the audit process. (we can help with compliance demonstration).	You are legally responsible for the services provided to the end users and are partially in charge of the audit process under the national supervision body	The TSP is legally responsible for the services provided to the end users and is in charge of the audit process under the supervision body
You are generally in charge of the RA function (possibly delegated) and may leverage existing KYC processes	You are generally in charge of the RA function (possibly delegated) and may leverage existing KYC processes	The RA function is delegated if you sign an RA delegation contract and undergo an audit.

Responsibility and time frame	On-Premise	Hybrid Signing Service	Fully Managed TSP
Implementation	SW & HW deployed in clients' environment	Client integration with SDK & SW deployment	Client integration with SDK
Liability	Client	Client	TSP
Audit process	Client	Partially Client	TSP
Time to Market for QES	1 year	6 months	As little as 1 month

Responsibilities and time to market

Alternative solutions

When developing a QES service, there are core functions which must always be considered:

- Identifying your customer
- Providing qualified certificates
- Providing a QSCD
- Integrating the signature process in the business workflow
- Delivering a user-friendly signing experience.

A signature service cannot be regarded as just another server. One needs to take into account the legal and procedural obligations around client identification. Additionally, there are policy enforcements and necessary practice statements that must be put in place for issuing qualified certificates.

Buying a best-of-breed remote signing solution is not the only route available to provide QES services. There are some potential attractions in considering 'making' a solution from components using internal or external development resource as well as the "traditional" personal PKI smart card approach. Nevertheless, there are some risks or limitations with these approaches, including:

High certification costs: when wanting a solution to comply to external standards (e.g. eIDAS) there are some large hurdles to overcome to gain certification, such as the costly Common Criteria certified QSCD signature devices. Certification typically takes upwards of 12 months and can cost 100s of thousands of €/$/£.

Security design expertise: to engineer a solution that protects against both obvious and subtle attacks and subversions requires expert security architects and use of specialist devices such as HSMS (Hardware Security Modules).

Patented technology: Many e-signature technologies are patented by various vendors. Developing a solution in-house may inadvertently lead to patent infringement.

High deployment cost: A distributed system where users hold their signing key in a personal PKI device/smart card has several limitations, such as device compatibility, user mobility and high management overheads.

For customers who wish to deploy a cost-effective solution with predictable timescales, acquiring a remote signing solution such as Cryptomathic Signer will have less risk, a quicker time-to-market and will allow a focus on their core business strengths. It is therefore advisory to team up with a skilled partner and outsource parts or all of these activities to ensure that the deployment and the conformity assessment are successfully passed.

Cryptomathic Signer – architecture

Cryptomathic Signer is deployed in a 3-tier environment, where we distinguish between the:

- User domain - the user who is typically in possession of laptop, tablet or mobile phone and uses a browser for zero footprint signing
- Application Provider domain - The business application provider manages the workflow and prepares the data to be signed
- Trust Centre domain - the trust center ensures that the signing server operates securely and manage the processes to ensure provisioning of users keys and certificates.

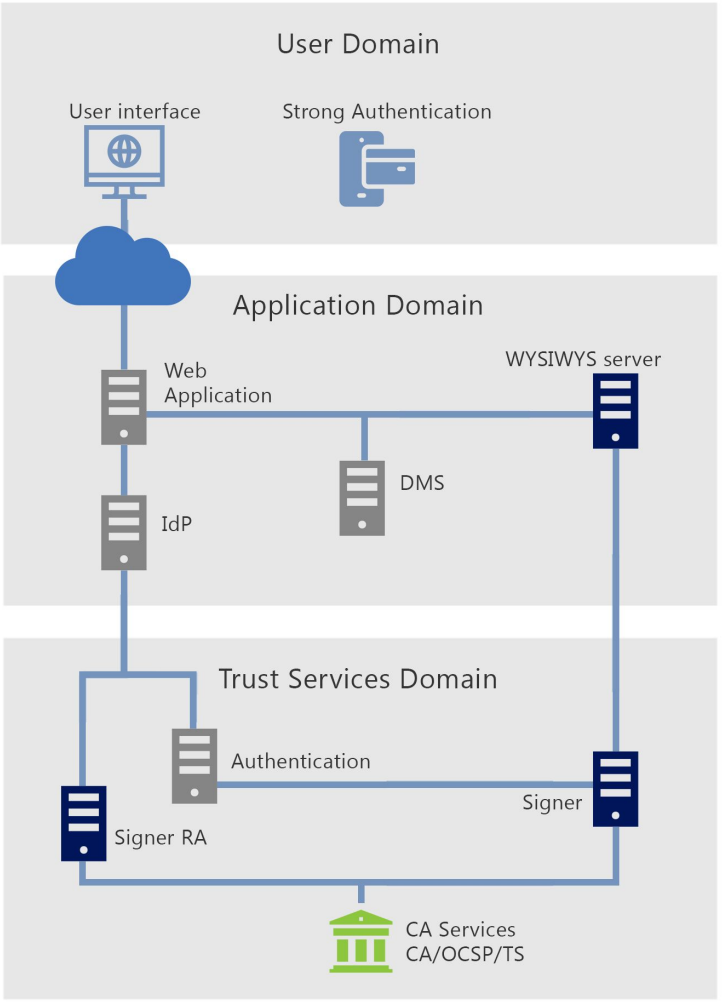
The location and hosting of the components in these domains is flexible and can support different business models, as described on the previous page, but all components need to be available and integrated to deliver a complete solution.

The architecture overview of the three domains is illustrated on the right. The blue components are provided by Cryptomathic. The grey components are supplied by the business application provider and the component in green can be outsourced to a TSP if required. The three domains are explored in more detail in the following sections.

The User domain

The user domain contains end-users provided with the ability to give informed agreement to a particular document or transaction by applying their digital signature. Users will have an internet connected device to view the document they wish to sign, and use strong authentication to invoke the signature process retaining sole control of their signing key.

Signer provides a unique and strong capability of rendering an exact version of the document that the user is consenting to. Cryptomathic's patented 'What You See Is What You Sign' (WYSIWYS) technology ensures that a document can only be signed by the end-user if it is the authentic document that was intended by the business application to be signed.

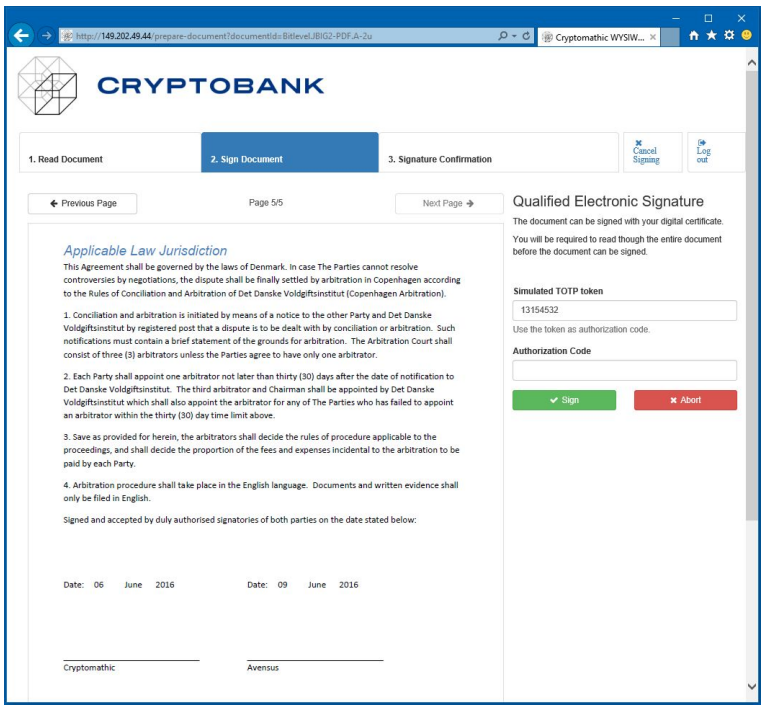


WYSIWYS user interface

The Cryptomathic WYSIWYS presents the user interface to view and sign documents. Embedded into HTML pages of the business application, it acts as a trusted viewer, that securely presents the data that the user is prepared to sign.

The trusted viewer (known as Signature Interaction Component in CEN documents) can control whether a user has seen all pages and handles the necessary interaction with the different back-end components. In particular, this is the component that initiates the sole control channel with the QSCD.

The Cryptomathic WYSIWYS user interface can be executed by any browser with no download and can also be embedded into a mobile app. It also offers document thumbnails, zooming and functions to navigate through documents as shown below.



The Application domain

This is the domain of the business provider. A portal or web application typically manages the business processes. It normally interacts with the user domain using HTML pages transported over TLS.

The following functions need to be available:

- Web application: a web server with business logic presenting HTML pages
- Document Managment System (DMS): a managed repository of documents available for signing
- IdP: Identity provider responsible for user authentication and access control
- Cryptomathic WYSIWYS Server: Signer component that delivers protection against attacks, i.e. man-in-the-middle.

The above list is simplified and might need to be integrated in the overall architecture.

The WYSIWYS Server

The Cryptomathic WYSIWYS Server is a web application which handles the signature workflow and user experience.

In simple terms, it receives a document to be signed as input (optionally converts it to PDF-A as it is the ISO format for PDF for Long-term Preservation), then securely renders the document to the end-user and creates a signed document as output without breaking the browsing experience.

WYSIWYS enables:

- The signatory to visually observe exactly what is being signed
- The signatory to inspect the result (the signed document)
- The signed document to be recognizable to the signatory afterward.

WYSIWYS is a key element for non-repudiation. To help establish trust and confidence, the secure design and protocols of the WYSIWYS server ensure that only the authentic document provided by the business application can be signed by the user.

At the end of the signature process, the WYSIWYS server outputs signed PDF data with PAdES signature profiles. In addition, the WYSIWYS server can also add visual signature stamps to the signed document to allow the user to visually observe that the document was signed. Visual stamps are supported in the PAdES standard.

The Trust Services domain

A remote signing service needs to have the following functions available.

- Certificate Service Provider (CSP) Services
  - Certificate Authority (CA)
  - OCSP Services (optional)
  - Time Stamping services (optional)
- Signer Server Application (supplied by Cryptomathic)
  - Incorporates the QSCD
- Signer Registration Authority (RA) function (supplied by Cryptomathic)

Note that these functions can be existing services within an enterprise, or hosted 'as-a-service' from third parties.

The optional components are relevant if the signature profiles require the presence of these services. Please contact your Cryptomathic representative for full details of how Signer provides or integrates with these services.

CA Services

CA services (optionally offered by a Cryptomathic partner) are used for issuing and managing advanced or qualified certificates in accordance with the eIDAS regulation and relevant ETSI standards including in particular ETSI EN 319 411-2. The certificates produced by the CA are issued under a trusted root recognized by Adobe Approved Trust List (AATL). The certificates are valid in the EU and in other countries as well.

The CA can also feature an Online Certificate Status Protocol (OCSP) service, as described in RFC 6960, and/or Time Stamp Services, as defined in RFC 3161.

Signer Server Application

Cryptomathic Signer is the cornerstone of the remote signing solution and offers a unique signing experience, which is integrated into the business workflow. The signing keys are deposited in a central repository and protected by Hardware Security Modules (HSMs). Signatories seamlessly retain sole control over the signing process using their existing strong authentication tokens.

At the heart of Signer is secure code running inside the FIPS boundary of an HSM that will only allow a digital signature to be performed when a registered user has authenticated themselves sufficiently. This is how we can be certain of offering the highest standard of certification of the signature. The trusted code is part of the Signature Activation Module (SAM) engine - in eIDAS terms, it is the QSCD (Qualified Signature Creation Device).

Signer conforms with the requirements of CEN 419 241 [Security Requirements for Trustworthy Systems Supporting Server Signing] and is Common Criteria certified.

Signer is designed for large-scale deployment and it is a stateless solution, which supports different clustering strategies to meet the highest SLA and performance requirements.

Signer RA
The Signer Registration Authority Component (Signer RA) is an integration component sitting between the User management system and the Trust Services Provider. It exposes a RESTful web services interface so that users can be generated and certificates established or revoked.

The Signer RA handles all the necessary interaction with Signer as well as with the CA services for certificate issuance. It can support multiple key/certificate policies.

External integration points

Cryptomathic Signer is turn-key solution which can be integrated easily into an existing environment. The external integration points are as follows:

- **User registration (Signer RA interface)**
  Cryptomathic Signer RA exposes a lightweight RESTFul API with user management functionality. The functionality of the API includes function calls for user generate, query and establish certificate for a given policy.

- **Signature process (WYSIWYS user interface)**
  Cryptomathic deliver a WYSIWYS SDK in Javascript together with a sample client and a cookbook in order to deliver a custom signing experience that is browser and mobile friendly. The WYSIWYS interface is directly integrated into the user experience using an iFrame or similar technology.

- **Authentication services**
  Cryptomathic Signer can leverage an existing OpenID Connect or SAML v2 compatible IdP. More details on the supported authentication profiles for initial logon and actual signature operation authorization are detailed in the product manual.

- **DMS Services**
  Cryptomathic WYSIWYS exposes a lightweight RESTFul API for integration with a DMS system. The interface for document pick-up and remittance is detailed in the product manual.

- **CA services**
  The integration with a CA may also be required. The following functions need to be implemented:
  - Certificate Generation

  A CSR (Certificate Signing Request) is sent from Signer RA to the CA. Typically, this CSR has a PKCS #10 format. In some cases, this PKCS #10 object can be wrapped in a CMP (Certificate Management Protocol) or CMC (Certificate Management over CMS) object.

  - Certificate Revocation

  A certificate revocation request is sent from the Signer RA to the CA. Common implementations are CMC, CMP or even proprietary web services.

Security and compliance

Cryptomathic Signer security design is, together with end-user convenience, of the utmost importance. The solution is designed to deliver Advanced and Qualified electronic signatures, as per the eIDAS and ZertES regulations.

Security and assurance

The security design has various layers, including:

- A strong security kernel that enables, by means of firmware extensions, all the security sensitive operations inside the tamper evident environment of the Common Criteria EAL 4+ certified HSM
- The signing protocol that allows the data intended for signing to be sent over a secure communication channel so that all communication can be encrypted and integrity protected.
- Administration is privilege-based and all logs are stored in a high capacity integrity-protected database.

Compliance

The EU Commission together with the ETSI and CEN normalization committee has set standards around remote server signing and offers a clear legal framework for the roll-out of this technology.

Customers implementing the Signer technology need to undergo an audit performed by a security assessor recognized by a supervision body if they want the signature services to be certified as delivering Qualified Electronic Signatures. eIDAS is the EU regulation that enforces the following standards.

Relevant Standards

For an eIDAS compliant implementation allowing for the issuance of Qualified Electronic Signatures recognized across the EU member states, the following standards need to be observed:

CEN 419 241 - Security Requirements for Trustworthy Systems Supporting Server Signing, including:

- Existing CEN TS 419 241:2014
- New version 419 241-1
- Protection Profile for the QSCD 419 241-2
- Protection Profile for the HSM doing the signature operation (419 221-5 mentioned in the above standard).

ETSI EN 319 411-2:2015 for issuance of qualified certificates, including:

- CEN/TS 419 261:2015 Security requirements for trustworthy systems managing certificates and time-stamps.

Signature profiles must follow the PAdES (PDF signing), XAdES (XML transaction signing) and CAdES (CMS signing) family.

Other national regulations

Cryptomathic also supports other signature laws beyond the European Union.

In Switzerland, the ZertES regulation offers mutual recognition of TSP / Qualified Certificates using multilateral contracts.

Around the world signature laws generally follow two approaches:

1. A Tiered model like eIDAS where assurance models are verified by a conformity assessor. Legal value is clear and guaranteed and typically offered at different levels, e.g. AdES and QES.
2. An Open model where everything has legal effect but admissibility can always be questioned. The US and aligned countries follow this model.

Other counties that support the eIDAS-like tiered model include Hong Kong, Singapore and Japan.

Please contact your Cryptomathic representative for more details about compliance in these, and other, territories.

Certification

In order to provide AdES or QES within the EU, a business or TSP must go through a certification process, which is described in the following section.

The figure below illustrates the general workflow around service certification.

The European Commission is the entity that has defined the pan-European legal framework (eIDAS regulation and implementing acts) for the provisioning of (qualified) trust services including Qualified Electronic Signatures and for publishing the EU Trust List.

The European Commission has also commissioned standardization bodies ETSI and CEN to publish technical standards for amongst other issuance of qualified electronic certificates and electronic signatures.

The *Supervisory Body* is the national entity in charge of granting the qualified status to a Trust Service Provider (TSP). It relies on conformity assessment reports to verify the conformity of a TSP. It shall notify the European Commission on which TSPs operates in the member state. It has a regulation function.

The *Conformity Assessment Body* is the legal entity that performs a conformity assessment of the TSP against eIDAS regulation and relevant standards. It submits a conformity assessment report.

The *Trust Services Provider* is the legal entity that provides (qualified) trust services to individual and/or businesses. It is legally liable for the services provisioned.

The *EU Trust List* contains for each member state a list of trust service providers, what services they offer and what level it is recognized (qualified or advanced).

Certificates and CA domain

In the EU, an accredited certificate service provider (CSP) must comply with eIDAS and, depending on which services are offered, the CSP must meet specific technical standards, including:

- ETSI EN 319 411-2, for issuing qualified signature certificate
- ETSI EN 319 421, for issuing timestamp token
- ETSI 102042 NCP+, for issuing authentication certificate.

eIDAS qualification requires recurring audits (every 2 years) by an accredited evaluation body, the evaluation is a means to prove the trustworthiness of the CA and other IT systems.

An eIDAS security audit is based on a review of the existing documents and an inspection of the implemented mechanisms and security controls; therefore, the CA trust center should have up-to-date, proper and adequate documentation.

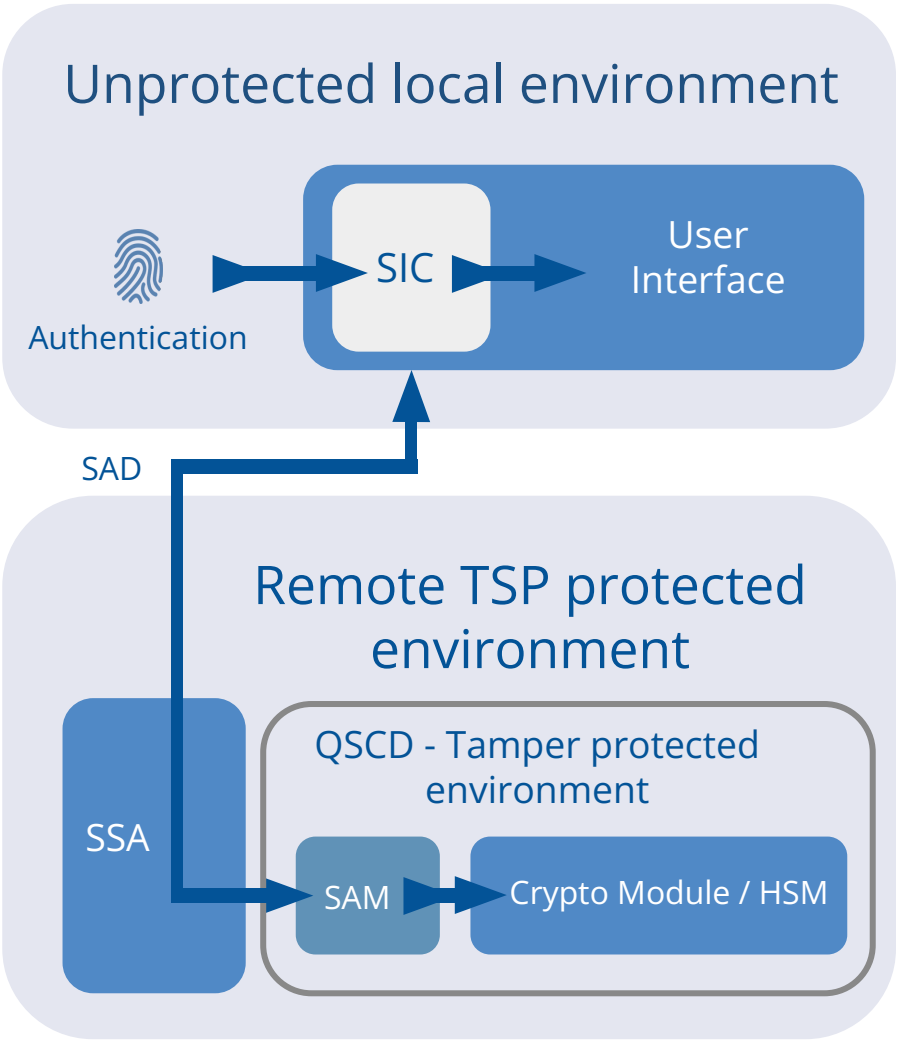
An essential part of the conformity assessment is to ensure that the procedures and practice statement set forth in the Certificate Policy / Certificate Practice Statement (CP/CPS) are effectively enforced.

Signature Generation Service Provider domain (SGSP)

eIDAS requires that qualified electronic signatures are created by qualified electronic signature creation devices (QSCDs).

Cryptomathic Signer – an eIDAS QSCD

Since the regulation includes requirements for QSCD, the conformity of the QCDSs shall be verified through certification. CEN TC224 WG17, as appointed by the European Commission, has created standards targeted for certification of products like Cryptomathic Signer. From CEN EN 419 241-1 the following architecture containing two parts can be derived:



1) Unprotected local environment - The local environment with all components running on the client side (user, device, and browser). This includes, in particular, the browser used to render the data to be signed as well as the Signer's Interaction Component (SIC) for communication with the remote TSP. The SIC corresponds to the JavaScript based WYSIWYS client. The environment is unprotected as it is not under the TSP's control.

2) Remote TSP protected environment - The remote environment corresponds to the back end of the TSP containing a Server Signing Application (SSA), like Cryptomathic Signer, which uses a HSM. The HSM contains two modules, a Signature Activation Module (SAM), which authorizes the signature operation, and a Cryptographic Module, which generate and use signing keys. The HSM must conform with EN 419 221-5 (Published December 2016) and the SAM with EN 419 241-2 to be a QSCD.

The SAD in the diagram is the Signature Activation Data, which cryptographically binds together information about:

- Who is the signatory
- What is to be signed
- Which signature key is to be used for signing.

The SAD is transmitted from the SIC to the SAM, where it is verified and used to activate the signature key.

The CAB Audit

The Conformity Assessment Body (CAB) is the legal entity that performs a conformity assessment of the TSP against eIDAS regulations and relevant standards and submits a conformity assessment report to the Supervisory Body (SB).

The SB reserves the rights of additional audit or conformity assessment at any time to confirm that requirements are fulfilled. European Accreditation (EA) defines common rules for all national accreditation bodies to implement. The common rules are based on ETSI and ISO standards.

eIDAS certified CABs perform two audits to verify compliance against the eIDAS regulation:

- Pre-assessment: This includes documentation assessment (i.e. technical, functional, and organizational security measures) and their appropriateness for fulfilment of eIDAS requirements. This also includes identification of applicants (qualified, experienced and reliable staff, sufficient financial resources, liability insurance, communication with supervisory body).
- On-site audit: This includes verification of implementation of security measures, processes, network, systems. The technical testing includes penetration testing.

A Conformity Assessment report detailing the findings of the audit is then submitted to the Supervisory Body, which ultimately decides if the TSP is entitled to receive the qualified level of certification and be referenced in the EU Trust List.

Conclusion

Why Cryptomathic?

By selecting Cryptomathic a business will gain:

- Proven technology from an industry pioneer in remote signing
- A partner with a strong track record with first class references
- A long-term partnership that will allow a strong footprint on the solution delivered.

Why Signer?

Cryptomathic Signer allows governments, banks and other businesses to offer a fully secure, end-to-end digital service experience to their citizens or customers. Utilising QES, trust service providers, organizations can deliver an eSignature service that conveys the same legal weight as hand-written signatures. The solution is deployable across all common digital channels.

The signature operation is triggered using a regular browser or mobile app and does not require any download or smart card. It relies instead on remote signing technology and can leverage existing authentication technology and supplement it with enhanced security and transaction data integrity which many financial regulators desire and is now being mandated. This not only makes the completion of digital transition possible, but also makes the process elegant and convenient for end-users.

Signer can offer the confidence of compliance with eIDAS legislation combined with a first-class user experience delivered in a modular and highly secure architecture, designed to lower operating costs and deliver faster and more agile digital services.

How to implement

The implementation and deployment of a QES service is highly dependent of the selected commercial models. The QES deployment and sub-projects would typically go through the three following phases:

1. **Kick off and design:** The kick-off phase will start with an onsite kick-off workshop define/refine the actual scope of the solution to be delivered, including workflow, policy settings and integration needs. We also outline the project plan, the inter-dependencies and present the reporting methodology.

2. **Implementation:** Cryptomathic will then onboard the pre-production environment to offer the signature services in accordance with the project requirements. If required, a project development team is assembled to start programming activities for any custom features.

3. **Go Live:** Once the release of the signature software and the signature service have been delivered, the project moves into QA phase. Tests will be performed based on a pre-production environment. In parallel the Conformity Assessment body is invited to conduct an audit.

Next Steps

To support your journey towards an optimal remote signing solution, Cryptomathic is pleased to offer the following additional resources:

Product Sheet - Cryptomathic Signer

Case Study - UBS deploys QES

Case Study - LuxTrust Central Signing Service

Case Study - Remote Signing Platform

e-Book - Digital Signatures for Dummies

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

Contact us at enquiry@cryptomathic.com

Disclaimer

© 2022, Cryptomathic A/S. All rights reserved Aaboulevarden 22, 8000 Aarhus C, Denmark

This document is protected by copyright. No part of the document may be reproduced in any form by any means without prior written authorization of Cryptomathic. Information described in this document may be protected by a pending patent application. This document is provided “as is” without warranty of any kind. Cryptomathic may make improvements and/or changes in the product described in this document at any time. The document is not part of the documentation for a specific version or release of the product, but will be updated periodically.

Note: This material has been prepared for general informational purposes only.

© 2022 Cryptomathic.
All Rights Reserved.

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 two-thirds 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.