Namirial
Digital Transaction Management

Get Documents Signed. Anywhere. Anytime.

NAMIRIAL GmbH

Legal Office: Seilerstätte 16, 1010 Wien, Austria
Main Office: Haider Straße 23, 4025 Ansfelden
Phone: +43-7229-88060 | www.xyzmo.com

Icon UK Ltd.

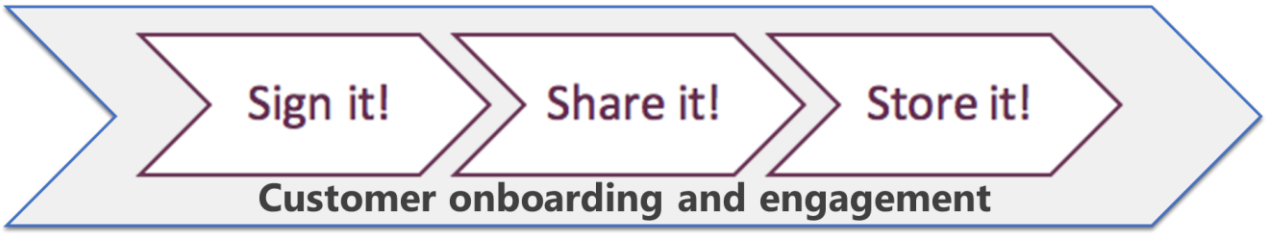
Legal Office: Griffins Court, 24-32 London Road, Newbury, Berks RG14 1JX, UK
Phone: +44 (0)203 150 1081 | www.icon-uk.net

Table of Contents

1 Executive Summary

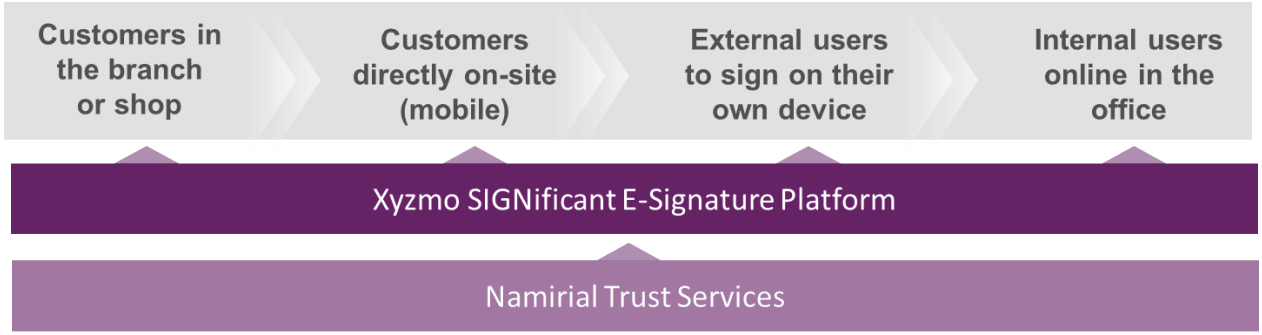
In everything we do, we believe in simplifying the way business gets done by transforming slow, complex, costly, manual and paper-based processes into frictionless and adaptable digital ones.

Namirial is a software company that develops and sells its own enterprise solution for **Digital Transaction Management (DTM)** through direct and indirect sales channels. Among other services, Namirial DTM provides IT solutions to capture legally compliant electronic signatures, manages and tracks the flow of documents between contractual parties, conducts secure document-based transactions, and guarantees the secure storage of data, while simplifying how business gets done, especially also onlin.



Namirial is a DTM vendor that integrates products from the following core areas:

- An omni-channel enterprise software solution for **e-contracting** that can even include cases of multiple uses within a single transaction. The e-signature and workflow products that implement this are sold under the brands xyzmo, SIGNificant and eSignAnyWhere as an on-premise or Cloud-based SaaS solution.
- **Online customer onboarding and engagement** solution based on WebRTC technology enabling video-based identification (KYC-AML), real-time document-based collaboration and together with SIGNificant real-time signing
- A **Qualified Trust Service Provider** that operates as a separate business unit called Namirial Trust Service Provider (TSP), which is a certification authority for (qualified) eIDAS-compliant trust services such as digital signing certificates, digital remote signature, qualified time stamps and digital archiving for more than 500,000 customers.



Both parts, the e-contracting solution and the trust services, can be used together or independently of each other. The advantage of the combined solution is that it is pre-integrated and tailored to the strengths of each other.

Namirial is uniquely positioned as a leading provider in the DTM market thanks to this seamless integration of an omni-channel e-contracting solution that supports all types of signatures and deployment methods (on-premises, in cloud, or hybrid) with a qualified trust center and services that are certified by eIDAS legislation.

2 Business Perspective

Digital Transformation is one of today's top three initiatives employed by CxOs in any industry. Their priority is on leveraging the changes and opportunities relating to digital technologies and their impact across society so as to implement a profound and accelerating transformation of business processes. Digital transformation is not just about technology alone however; the adoption of technology often leads directly to transformation, or at least enables such a transformation to happen.

A simple way to start a Digital Transformation journey is to digitalize all business transactions, which, with all the paperwork and signatures required by processes, have represented the last mile of the journey—until now.

The capability of conducting fully digital transactions, which includes legally compliant electronic signatures, managing and tracking the flow of documents, conducting secure transactions and guaranteeing secure storage of data, is the real enabler of digital transformation.

We have recently seen a rise in the uptake of Digital Transaction Management (DTM) as a fast-growing product category that promises to help companies to improve their "eco" credentials by going paperless. Embracing DTM allows companies in any industry to accelerate revenue by simplifying how business gets done, shortening the transaction life cycle, driving efficiency by eliminating all the paper printing, delivery and management costs, and promoting their corporate and social responsibility by reducing their carbon footprint.

DTM is often seen as the one-size-fits-all solution to the digitalization of business transaction. We believe, however, that DTM should provide different models, sizes and colors to fit the customer use case and context, the country-specific regulations (including the type of electronic signature, privacy and the long-term archiving requirements), the delivery model (on-premises, cloud, hybrid) and the user experience.

This is how we see Digital Transaction Management in Namirial and how we came to build a solution that allows our customers to sign anywhere, at any time, on any device.

2.1 Company Background

Namirial SpA was founded in 2000 in Italy by two visionary entrepreneurs, who started a company whose mission was to enable its customers to digitally transform their business.

At the start of the decade, DTM emerged as a global market opportunity and the e-signature industry initiated a consolidation process. Moreover, a new regulation of the European Parliament and of the Council on electronic identification and trust services ("the eIDAS Regulation") was approved in 2014, with the objective of standardizing and promoting e-signature adoption across the region.

To capture this opportunity, Namirial executed an M&A strategy with the objective not only to extend its product and service portfolio, but also to gain access to the European and global markets through a partner and reseller network linked to the acquired companies.

This strategy led to the acquisition of 2CSolution in 2014 and xyzmo/SIGNificant (now Namirial Gmbh & Srl) in 2015, and positioned the company as one of the global players in the DTM market with over €40 million in revenue per year and approximately 300 employees.

Key facts:

- Headquartered in Senigallia, Italy, with subsidiaries in Ansfelden, Austria, and Bucharest, Romania
- >€40 million revenue in 2015, with 350 employees
- >2,000,000,000 pages digitally archived annually
- >350,000 signature stations of handwritten biometrics
- Member of the Adobe Approved Trust List (AATL)
- Certification Authority (accred. by AgID)
- Qualified Trust Service Provider (accred. by Bureau Veritas)
- Electronic Registered Delivery Provider (accred. by AgID)
- ISO 9001:2008 (accred. by Bureau Veritas, no. 223776)
- ISO 27001:2013 (accred. by Bureau Veritas)

2.2 References

Automotive:

BMW (Italy); Daimler (worldwide for service processes, Germany and Italy for retail POS), Fiat Chrysler Automobiles (FCA), Skoda SZ, Volkswagen (Italy), One Eighty (Canada), Seriti Solutions (South Africa), (Italy), Ducati (Italy), Jaguar (Italy)

Banking:

Poste Italiane, Unicredit Italy, Intesa San Paolo Bank (Italy), Banco Popolare (SGS, Italy), BNL Italy, Handelsbanken, Pireäus Bank, Bred Banque Popolaire (France), Zagrebacka Banka (Unicredit Croatia), GE Money Bank (Czech Repbublic), Tatra Banka (Slovakia), Banco BMG (Brasil), Raiffeisen Bank (Croatia), Regiobank (Netherlands), BCEE Luxembourg, BGL Luxembourg, BNP Paribas Fortis, Belfius, Bank Austria, Fineco Bank (Italy), Carige (Italy), Alpenbank, Creval (Italy), Cofidis (Italy), Mutui on-line (Italy)

Banking Service Providers:

CSE (Italy), Cabel (Italy), Cedacri (Italy), SEC Servici (Italy), Sabemi Group (Brasil), Central Bank of Honduras (CNBS)

Insurance:

Deutsche Vermögensberatung AG (Germany, Austria, Switzerland), Ceska Pojistovna (CZ), NN Group (CZ + SK), Nürnberger Versicherung (Austria), Helvetia Versicherung (Austria), Upper & Lower Austrian Insurance, Swiss Life Select (Austria), Azimut (Italy), Reale Mutua (Italy), Pramerica (Italy), Sermetra (Italy), Groupama (Italy), Allianz (Croatia), Triglav Insurance (Slovenia)

Telco & Media:

Vodafone (Italy, NL, Greece, Romania), Orange (Romania), Carphone Warehouse / Dixons UK, Phonehouse (NL, SWE), KPN, BelCompany (NL), T-Mobile (NL, SL, Cro),

Wind (Greece), Cosmote (Greece), Vivacom (Bulgary) T2 (Slovenia), Mediaset (Italy), Sky (Italy)

Central and Local Government:

Department for Work and Pensions / JCP (UK), IHSS (National Social Security Agency, Honduras), Department of Public Works - DPW (South Africa), Avepa (Italy), INAS - Istituto Nazionale Assistenza Sociale, Patronato CISL (Italy), Ministery of Environment Romania, Ministry of Justice Angola – City of Milano, City of Genova, City of Cesena, City of Ivrea, Guardia di Finanza (Italy), Ministero degli Interni (Italy)

Utilities:

VSE (East Slovak Electricity), ZSE (E.ON SK), Saipem Construction (Italy), E-Werk Wels (Austria), Latvenergo (Lithuania), CCEE (Brasil), Citgo (USA), Axopower (Italy), Energrid (Italy), Lifegate (Italy)

Retail:

REWE (DE), Botanic (France), Nespresso (Italy), L'Oreal (Italy), Mariannaud (Italy), Dynamica Retail (Italy)

Pharmaceutical and Healthcare Industry:

Icon Plc (UK), Maquet Cardiopulmonary (DE), Olympus (DE), BOC Healthcare (Australia), Abbvie (Italy), Menarini (Italy), Guerbet (Italy), Istituto Europeo di Oncologia (Italy), several local healthcare public providers in Italy

Other Industries:

Carl Zeiss (DE), Bechtle (DE), Randstad (Italy), AMP Logistics (NL), Groeneveld Group, Humangest (Italy), Teamsystem (Italy), Nuova CS (Italy), Intesi Group (Italy), Eismann (Italy), Sapio Life (Italy), Medigas (Italy), Magaldi (Italy), Sorgenia (Italy), Seat Pagine Gialle (Italy), Tribal eLearing (UK)

2.3 Partners

Namirial sells mainly through channel partners to its customers.

Our partners in Europe are listed at https://www.xyzmo.com/partners

3 Key Characteristics

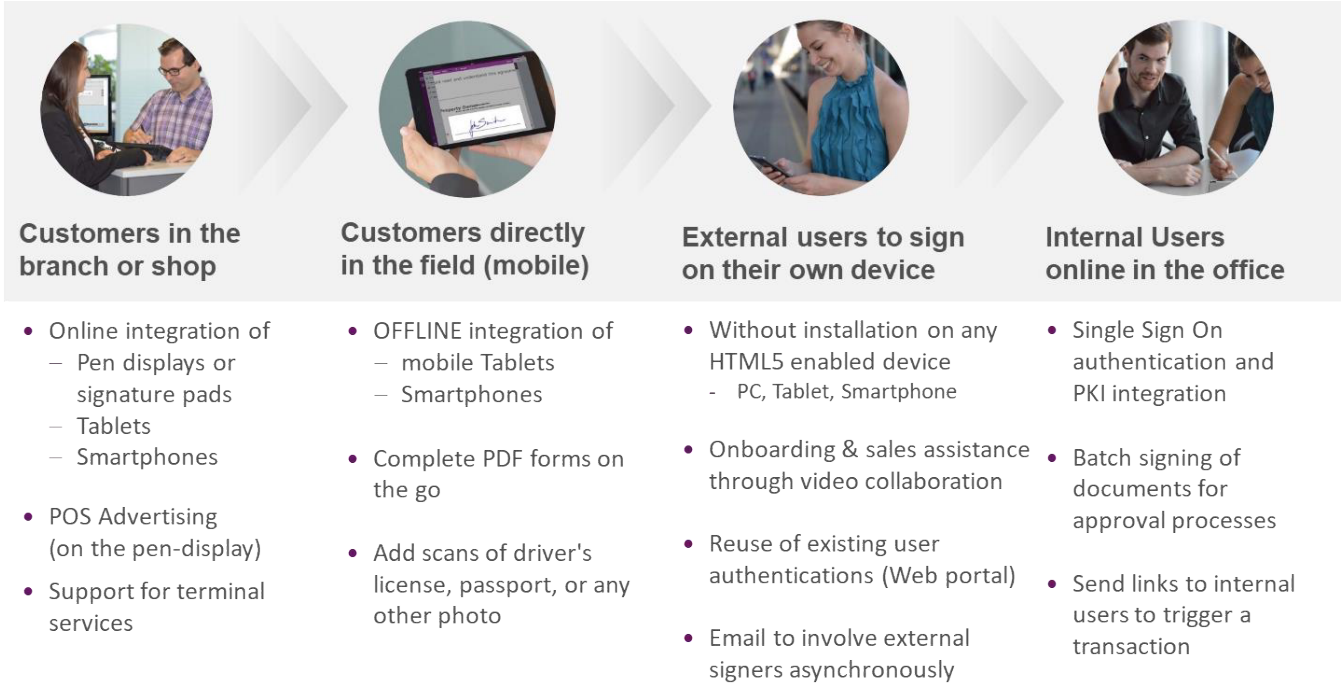
To understand the breadth of a DTM solution like Namirial's, it's important to understand how to categorize business processes according to certain key requirements. Overall, these requirements can be grouped into the following categories:

- The use case, i.e. the specific context in which the e-signature is executed,
- The legal signature level, which defines the legal validity of the e-signatures,
- The user experience, i.e. how the user interacts with the business application to execute the signature,
- E-signature technology,
- The document model,
- The deployment method.

The Namirial DTM solution ticks the boxes on the key requirements for each of these categories, which are described in detail in the following sub-sections.

3.1 Use Case and Context

The most popular use cases and their requirements are shown in the figure below:



Here it is important to understand whether your e-contracting / e-signature solution treats those use cases as individual silos, or—like SIGNificant—can combine all those channels with different participants into a single transaction (see section 4).

3.2 Levels of Legal E-Signatures (eIDAS)

The required legal level an e-signature needs to achieve mainly depends on the following two factors:

- The country in which the e-signature is executed,
- The business process that would be digitalized upon completion of the e-signature

Namirial DTM is designed for global compliance with key components of:

- eIDAS 910/2014 – see the eIDAS whitepaper for details http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
- the European Directive 1999/93 EC on a Community Framework for Electronic Signatures, including the UK Electronic Communication Act,
- the U.S. ESIGN Act
- US state laws modeled after 1999 UETA
- Rules from the FDA, FTC FHA, IRS, and FINRA, among many others

As the EU has with eIDAS a very strict e-signature legislation, we concentrate here further on this legal framework. eIDAS defines the following three legal e-signature levels:

- **Electronic signature (ES)**—can be viewed as a "placebo". Document integrity and audit trails for process evidence are needed for such signatures to be legally stronger;
- **Advanced electronic signature (AES**)—can be viewed as "provable signature". Indicates that a signature can identify the signatory, is unique to them, is under the sole control of the signatory, and is attached to a document in such a way that it becomes invalidated if the contents are changed;
- **Qualified electronic signature (QES)**—satisfies the "legal written form" and has the characteristic of "non-repudiation". It is an advanced electronic signature with a digital certificate encrypted by a secure signature creation device, e.g. smart card or HSM.

Electronic signatures are only as secure as the business processes and technology used to create them. High-value or more important transactions need better quality electronic signatures - signatures used for these transactions need to be more securely linked to the owner in order to provide the level of assurance needed and to ensure trust in the underlying system. In such cases, a minimum of AES level is recommended.

Qualified e-signatures are required when the local business laws of a country require a certain transaction to be documented in written legal form. The advantage of QES is that such signatures have the characteristic of "non-repudiation". The disadvantage is that they are more complicated to execute as they:

- Require a personal qualified signing certificate issued to the signatory;
- Require certain identity checks from the CA when the certificate is issued to the holder (signatory);
- Must be stored on, and used with, a certified signature creation device.

However, the eIDAS legislation has simplified the QES process as it enables the establishment of "remote signature" environments, where a "Qualified Trust Service Provider" (QTSP, see 4.4.1) manages the e-signature creation environment on behalf of the signatory. This means that users do not need to manage the e-signature creation device within their own environment, which means that the user can also receive the required "qualified e-signing certificates" at any point throughout the business process (after an appropriate identification of the recipient).

3.3 User Experience

The user experience, i.e. how the user interacts with the business application to execute the signature, is key to the adoption rate of an e-signature system. Typical user experience options are:

- Handwritten signatures (such as those on paper)—captured either on the same device on which the document is displayed/edited or on a peripheral device (e.g. sign pad);
- Signatures using a password-protected personal device that you need to possess (e.g. a smart card or USB token);
- Click2sign signatures with an upfront identification/authentication step.

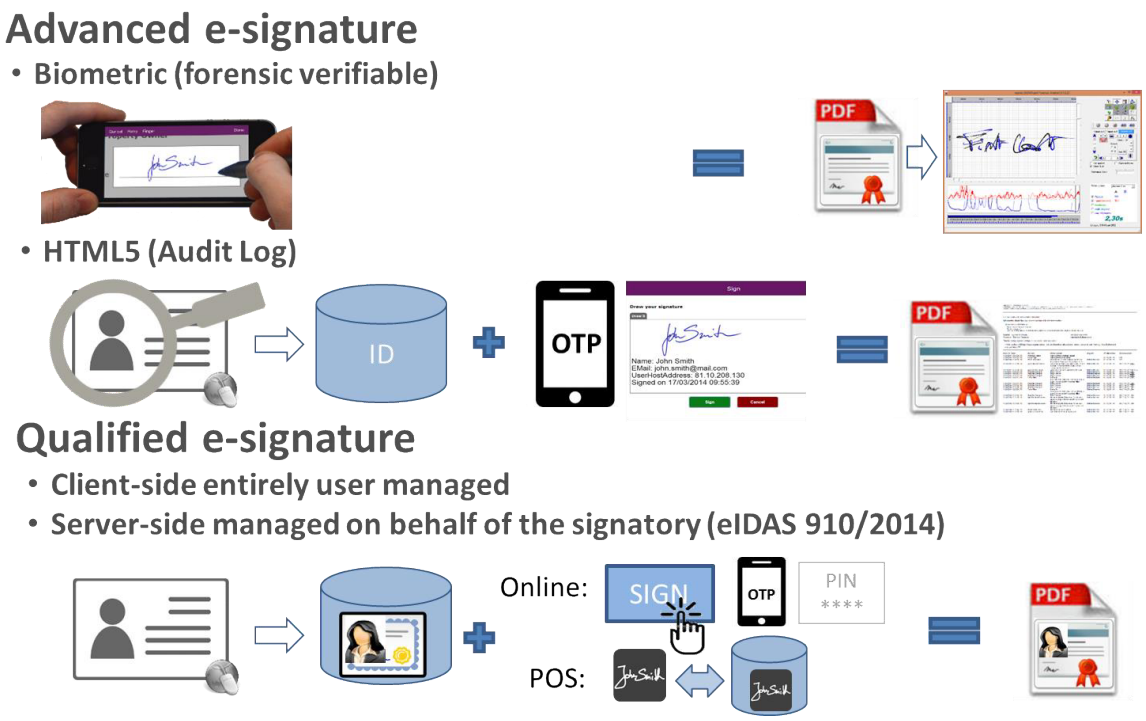
Each of these user experience options can be executed via an SES, AES or even QES when combined with Namirial Trust Services.

User experience is also significantly influenced by how the signatory is guided through the transaction process. Here, the following two models have been proven useful:

- Auto-stepping and workflow rules within a document, which define what a user has to do in order to eliminate expensive process failures such as missing signatures, data entries, or attachments;
- Integrated video chat support that allows both contracting parties to meet and discuss contracts synchronously simply via the web on any device—in a similar way to conducting physical face-to-face meetings, but just remotely using the internet. You even can authenticate a user through video in many countries if complying with national KYC/AML rules (see also section 4.3 on LiveID).

3.4 E-Sign Technology

Below is an overview of the three most common signature technologies used for signing PDF documents (but potentially can also be another digital asset) and how they map to the legal e-signature level and user experiences defined in the previous section. While the result is always a signed PDF that complies with the PAdES standard, verification differs according to each technology used.

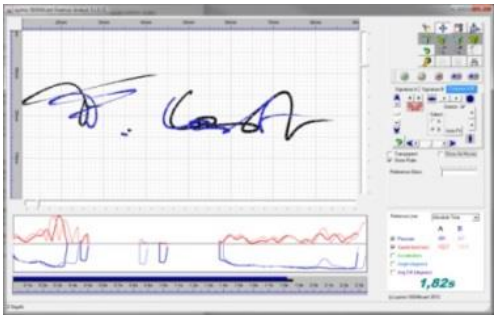


Use of a digital sealing/signing certificate (see sections 4.4.1 and 4.4.2) ensures that the requirement that the signature "is linked to the data to which it relates in such manner that any subsequent change of the data is detectable" is always achieved, regardless of signature type.

The other three requirements (that the signature is uniquely linked to the signatory, is capable of identifying the signatory, and is created using electronic signature creation data that the signatory can use under his/her sole control) are satisfied differently depending on the technology of each signature:

- Biometric signatures ensure that the requirements are met through (behavioral) biometrical data that is recorded uniquely, e.g. from one's own handwritten signature;
- HTML5 signatures ensure this through:
    - Step 1—identification: registering the signatory,
    - Step 2—enrollment: assigning a virtual identity to the signatory and agreeing on an authentication method (e.g. one-time password (OTP) send to a registered phone number),
    - Step 3—signing a document/asset through authenticating the signatory and subsequently executing certain signature fields;
- Pure certificate-based personal signatures follow the same process as HTML5 signatures, but they store the identity data inside the signing certificate that is used to execute the signature. This is the only method that can achieve the legal level of a qualified e-signature.

3.4.1 Biometric signatures (forensically identifiable)



Biometric signatures transfer the process of signing and signature verification 1:1 from the paper world to the digital world. Signatories sign with their handwriting using a pen, and if required a graphologist "forensically verifies" the previously captured handwritten signature against a set of available known sample signatures, either from digital or paper-based sources. Consequently, the recorded data of a biometric signature must include much more than its digitized image. In addition, it requires recorded data on "behavioral metrics" of the handwritten signature, which includes time-based data on writing rhythm (speed and acceleration), graphics (angle and angle difference) and, optionally, pressure. These dynamic parameters are unique to every individual and cannot be reproduced by a forger. That's why such a digitized signature is forensically identifiable (and far more reliable than with the signed image alone). Consequently, it is crucial that the biometric signature data is appropriately encrypted and safely bound to the document it has been applied to avoid misuse such as copy/paste attacks. To enable a graphologist to use their preferred tool for analyzing and verifying a biometric signature, the ISO /IEC 19794-7 biometric data exchange format on signature/sign time series data has been created.

When someone claims "I didn't sign that," a forensic expert is able to perform a thorough manual signature verification at any time afterwards, using specialized software to achieve an admissible result in the same way as the expert would with a signature on paper.

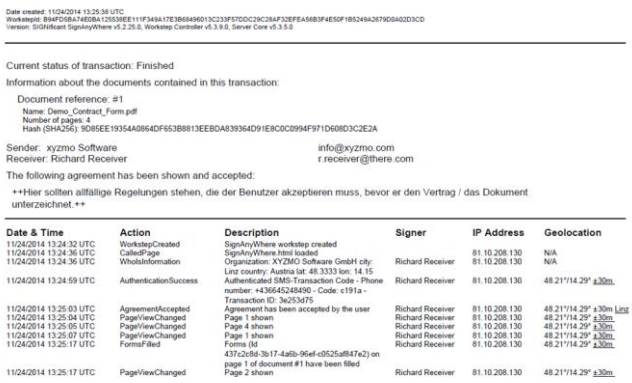
In addition, biometric signatures can be verified in real time to authenticate a signature against a pre-enrolled signature profile database. This allows you not only to secure the execution of certain transactions while signing, but also to provide a ready-to-use audit trail in case of a dispute, thus placing the burden of proof immediately on the signer. To ensure that a verification response is authentic, it has to be signed. Embedding this signed response into the encrypted signature data stored in the PDF itself ensures the signed document is self-contained and thus easily archivable. To get more info on biometric signature verification in real-time please refer to this white paper.

While biometric signatures are a very secure form of technology that delivers a reliable proof of the signatory's declaration of intent, it is not deemed equivalent to a wet signature in many countries (such as in the EU, where an advanced e-signature level is sometimes required). Additionally, according to EU data privacy regulations, the signatory has to give consent to processing and storing his/her biometric signature data.

When legally allowed, the biometric signature is the de-facto industry standard for B2C scenarios (POS in a branch office or in a mobile door-to-door situation) where both parties meet face to face, and thus it is ensured that the signatory is actually using a pen or capacitive stylus (instead of just using the finger). Additionally, as reliable capture-and-save encryption of the biometrical signature data is an absolute requirement, biometric signature capture demands the use of installed native apps that provide a stable real-time processing environment.

3.4.2 HTML5 signatures (process-evidence based)

HTML5/Process signatures do not record any “behavioral biometrical” data as described in the previous section. Instead, they use another method to identify the signatory, namely an explicit authentication step that is eventually logged in to a secure server-side evidence book (e.g. a digitally sealed audit trail).



Date created: 11/24/2014 13:25:38 UTC
Workstepid: B94FD5BA74E0BA125538EE111F3349A17E3B6849601 3C233F57DDC29C28AF32EFEA56B3F4E50F1B5249A2679D8402D3CD
Version: SIGNificant SignAnyWhere v5.2.25.0, Workstep Controller v5.3.9.0, Server Core v5.3.5.0

Current status of transaction: Finished

Information about the documents contained in this transaction:

Document reference: #1
Name: Demo_Contract_Form.pdf
Number of pages: 4
Hash (SHA256): 9D85EE19354A0864DF653B8813EEBDA839364D91E8C0C0994F971D608D3C2E2A

Sender: xyzmo Software — info@xyzmo.com
Receiver: Richard Receiver — r.receiver@there.com

The following agreement has been shown and accepted:

++Hier sollten allfällige Regelungen stehen, die der Benutzer akzeptieren muss, bevor er den Vertrag / das Dokument unterzeichnet.++

Date & Time	Action	Description	Signer	IP Address	Geolocation
11/24/2014 13:24:32 UTC	WorkstepCreated	SignAnyWhere workstep created			
11/24/2014 13:24:36 UTC	CalledPage	SignAnyWhere.html loaded		81.10.208.130	N/A
11/24/2014 13:24:36 UTC	WhoIsInformation	Organization: XYZMO Software GmbH city: Linz country: Austria lat: 48.3333 lon: 14.15	Richard Receiver	81.10.208.130	N/A
11/24/2014 13:24:59 UTC	AuthenticationSuccess	Authenticated SMS-Transaction Code - Phone number: +436645248490 - Code: c191a - Transaction ID: 3e253d75	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m
11/24/2014 13:25:03 UTC	AgreementAccepted	Agreement has been accepted by the user	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m Linz
11/24/2014 13:25:04 UTC	PageViewChanged	Page 1 shown	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m
11/24/2014 13:25:05 UTC	PageViewChanged	Page 4 shown	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m
11/24/2014 13:25:07 UTC	PageViewChanged	Page 1 shown	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m
11/24/2014 13:25:17 UTC	FormsFilled	Forms (Id 437c2c8d-3b17-4a6b-96ef-c0525af847e2) on page 1 of document #1 have been filled	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m
11/24/2014 13:25:17 UTC	PageViewChanged	Page 2 shown	Richard Receiver	81.10.208.130	48.21°/14.29° ±30m

The major advantage of HTML5/Process signatures is that they:

1) Do not require the signatory to use a pen, which they typically are not able to use in a remote scenario when they sign on their own device (e.g. smartphone), and
2) Do not require the signatory to download and install anything for the purpose of providing:
    a. a real-time processing environment for the behavioral biometrical data, and
    b. a secure and reliable client-side encryption environment to protect a user’s behavioral biometrical data against misuse.

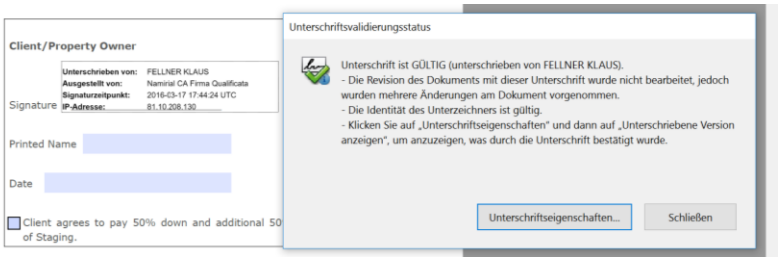
Their drawback is that a possible identification of the signatory, and thus compliance to the advanced e-signature standard, is fully dependent on the proper authentication of the signatory and the secure logging of all user interactions. While the authentication can be easily achieved via use of a PIN, one-time password (OTP), email access, or a combination of these, an identification of the signatory cannot be guaranteed without a dedicated upfront identification step—as with digital signatures that are based on personal signing certificates (see next section).

How the signatory then executes a dedicated signature field is a secondary question that more or less just addresses user experience. Popular methods are Click-, Type-, or Draw-2-Sign. See the white paper “Remote e-Signing via the Web” for further details.

HTML5/Process signatures best fit use cases where both contracting parties only meet virtually (remotely) and where the form is legally accepted. It requires no installation by the client and can be executed on virtually any HTML5-compliant device. The legal value of such a signature very much depends on the authentication method used and can be employed to the level of biometric signatures. It is very popular in remote B2C and B2B scenarios and scenarios within your own organization.

3.4.3 Pure digital signatures (using a personal signing certificate)

Digital signatures that are based on personal signing certificates include the identification of the signatory in the signing certificate itself. This means that every reader of a signed PDF document can see who has signed the document simply by looking at the



properties of an applied digital signature, in particular by looking at the signer certificate, tab details and field “subject”.

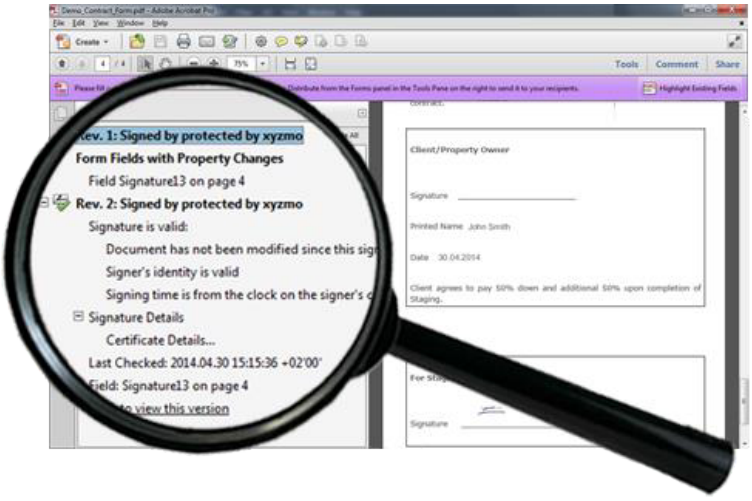
Pure certificate-based personal signatures can reach the equivalent of wet-ink signatures (written form) in most countries, but are hard to use in a pure client-side, entirely user managed environment. Solutions for acquiring remote digital signatures overcome this issue by issuing certificates “on the fly” and managing them server-side on behalf of the signatory. To deliver a signer experience at the POS, such as in the paper world, it is possible to use biometric signatures for authentication instead of an OTP (see section 5.1).

3.5 Document Model

PDF is typically chosen as it is an open document standard where digital signatures are well defined in the PAdES ISO standard. PAdES enables signed documents to be “self-contained”, which—according to Gartner Research (Publication ID Number: G00159721)—is the best document format, so it includes the content to be signed, the signature, and the metadata to make it searchable. In addition, it should store the signature process evidence data, such as the signing date, geolocation, and so forth. Last, it should require only a reader that’s freely and universally available to show the document in its original form.

3.5.1 PAdES Basic Profile (based on ISO 32000-1)

Digital signatures are well defined in PDF itself (Adobe PDF Reference PDF 32000-1:2008 12.8.3.3 PKCS#7 Signatures, as used in ISO 32000-1), meaning that every standard compliant viewing application, such as Adobe Acrobat Reader, correctly shows digitally signed PDFs without the need for any proprietary software. This includes the following data:



- Signature image (the visual representation of the signature);
- Document status when each digital signature was applied (the embedded signature history), even if you are not connected to the internet;
- The document’s integrity, meaning whether the signed document is still original or whether it has been altered since the signature was applied;
- Date and time the document was signed—optional, via a trusted time stamp service;
- Geolocation where the document was signed (GPS data if provided);
- Identity of the certificate holder, which in cases where a sealing certificate is used (e.g. for biometric signatures) typically points to the issuer of the signed document.

3.5.2 PAdES Long-Term Validation (LTV Profile)

Validation of a PAdES signature requires data to validate this signature such as CA certificates, Certificate Revocation List (CRL) or online certificate status profile (OCSP) information, commonly provided by an online service (referred to as validation data). If the document is stored and the signatures are to be verifiable long after first created, in particular after the signing certificate has expired, the original validation data may no longer be available or there may be uncertainty as to what validation data was used when the document was first verified. Also, the cryptographic protection afforded by the signature may not be guaranteed after the certificate has expired.

The PAdES LTV profile addresses this issue and thus is the perfect equivalent to the PDF variant, being designed for long-term storage and activation, defined as a PDF/A in ISO 19005-1:2005. PAdES LTV uses an extension to ISO 32000-1 known as a document security store (DSS) to carry such validation data as necessary to validate a signature, optionally with validation-related information (VRI), which relates the validation data to a specific signature. Additionally, it uses another extension known as document time-stamp to extend the protection lifetime of the document. The document time-stamp also protects the DSS by binding it to the document to which it applies.

The protection lifetime can be further extended beyond the life of the last document time-stamp applied by adding further DSS information to validate the previous document time-stamp along with a new document time-stamp.

3.6 Deployment Method

Some platform providers focus solely on cloud deployments. You should not choose a vendor that presents you with only this one option unless you are certain that you will never need to adopt another approach across your entire organization! There are still good reasons—data protection and legal data residency issues being a couple of the obvious examples—to deploy on-premises behind a trusted firewall, providing maximum control over data and systems.

There is no one-size-fits-all solution. Enterprises and large organizations might even decide that, for different needs, different deployment models are selected. At a minimum, it is vital to consider the following questions:

- What level of dependency regarding internet issues and support from the vendor is acceptable?
- Which type of documents do I produce?
- Are there legal and data privacy issues to be considered if I store documents on an internet-based public server?
- Does it matter whether this server is owned by a US company?
- Since registering with a cloud service is much easier than de-registering from that service, how do I remove myself from the cloud service if I choose not to continue with the provider?
- If I do leave the service, what happens to my signed documents and how can I prove, in the future, that they have been properly signed without becoming dependent on that provider again?

Typical choices are listed in subsequent sections.

On premises

- All applications and documents are held within your data center.
- You are not dependent on external systems or internet issues.

Private cloud

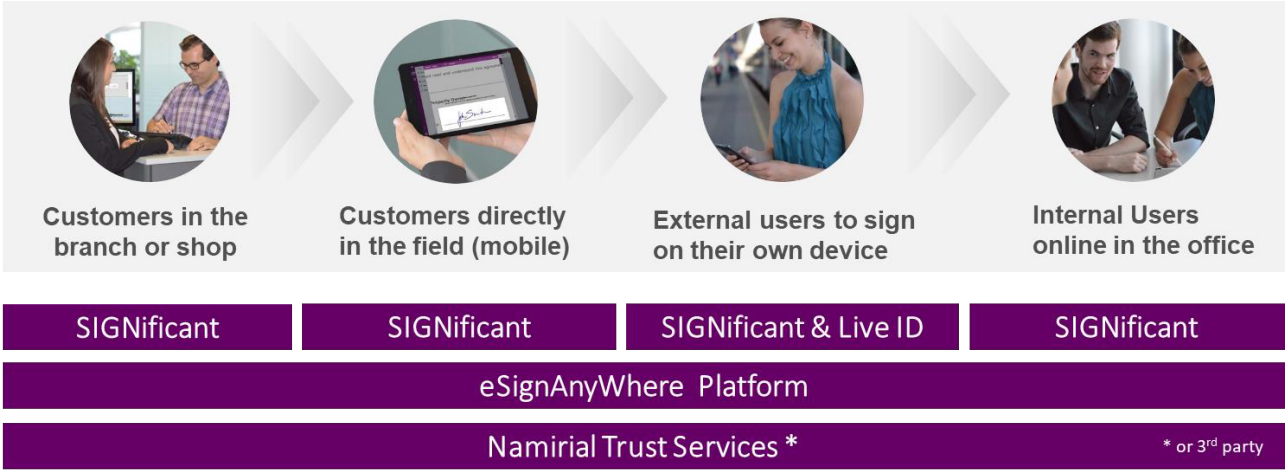
- Applications are managed by the e-signature provider.
- The server is dedicated to you.
- You can choose among different geographic regions and maybe even select the hosting provider itself.

Public cloud

- Applications are managed by the e-signature provider.
- The server is not dedicated to you.
- You can choose among different geographic regions but you cannot select the provider itself.
- Your documents are stored on a public server. In many cases they are encrypted but remain publicly accessible with the appropriate authorizations or in the case of successful hacking attempts.

4 Solution overview

Namirial can provide a modular e-signing solution which fulfils the requirements of each use case and which can run transactions that even span multiple channels—making it a modular omni-channel e-signature platform.



eSignAnyWhere is the heart and the backbone of the Namirial DTM solution. It manages the document flow between all transaction participants (signatories), ensures transaction security on envelope level (including its signed documents) and provides status updates and reports on user and organizational level.

SIGNificant is the core signing engine that enables a user to read, edit and sign an envelope and its containing documents. For more information about how eSignAnyWhere and SIGNificant support each of the use cases shown above, please refer to these papers:

- **E-Signing at the Point of Sale**
  Paperless B2C contracting through direct or indirect sales channels
- **Mobile E-Signing**
  Paperless contracting in mobile sales and service delivery
- **Remote e-Signing via the Web**
  Send and sign documents online. Anywhere. At any time. On any device.

LiveID is used to extend the remote e-signing use case to online customer onboarding and real-time customer engagement to reduce transaction abortion rates. Using its WebRTC based technology it provides video-based identification (KYC-AML), real-time collaboration with document/screen sharing and real-time signing.

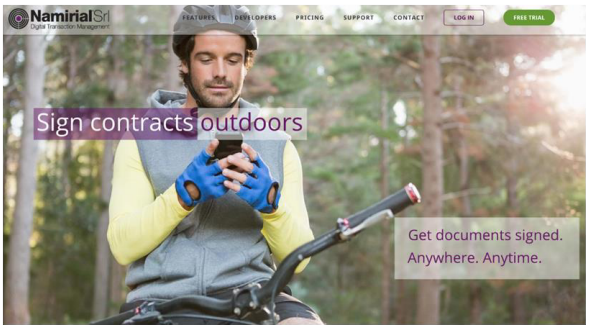
Trust Services provide the basis of this platform. SIGNificant may use the Namirial Trust Services, or operates with trust services from another certificate authority (CA). At a minimum, it requires a digital sealing certificate that is typically issued to the name of the customer organization (but instead customers may also use the standard sealing certificate, which is issued simply to Namirial GmbH). More advanced trust services on e-signature level (e.g. qualified time stamps, qualified remote digital singing) and document level (e.g. long term archive for storing signed documents) are purely optional.

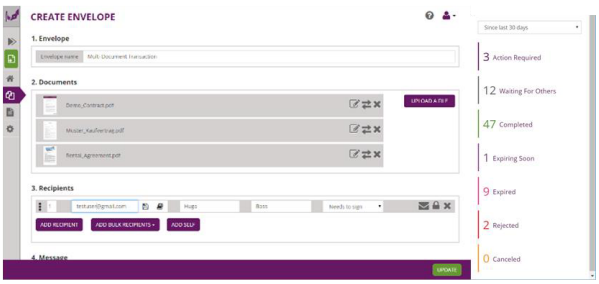
4.1 eSignAnyWhere

The eSignAnyWhere component of the SIGNificant platform allows you to involve participants in transactions whenever needed—even when they are remote. Using its workflow engine, it even provides transaction security over multiple use cases and client applications. Thus, it ensures that transaction initiators cannot access documents that are not yet signed by all defined transaction participants – even if this involves participants at the POS in a branch office, in a door-to-door meeting that is executed offline, or participants that sign documents on their own device remotely.

The highlights are shown below:

- **Workflow engine for e-signing**
  - Routing to multiple recipients (sequential or parallel)
  - Delegation of signing requests
  - Batch signing
  - Transaction security
  - Reminders & alerts
- **Dashboard with transaction drill-down**
  - View document status (e.g. viewed, signed, rejected)
  - Organize documents (Inbox, Sent, Templates, Drafts
- **Web Designer, API or Plugins to define transaction**
  - Envelopes
    - Include multiple documents into one transaction
  - Workflow and participant roles
  - Document ceremony per participant/recipient
    - Authentication & sign types
    - Obligatory & optional tasks (e.g. form fields & signatures)
  - E-mail messages, alerts & reminders for recipients
  - Retrieve and archive
  - https://content.signanywhere.com/developers





To find out more what eSignAnyWhere can do for you please visit:
https://www.xyzmo.com/e-signature-products/sign-anywhere-anytime

4.2 SIGNificant

SIGNificant provides the following key features to execute a digital transaction through signing one or more PDF documents contained in an envelope. Overall, it guides transaction participants in reading, editing and singing the relevant documents and allows them to work on those documents as they would on paper–in cases where the transaction definition on the supports that. Alternatively, you can force a user into an exact workflow within the envelope and its included documents. Using the envelope concept, you can ensure that a user either signs all included documents or none.

The core features of SIGNificant are shown in the figure below:

Govern user activities per transaction

- Tasks: Obligatory or optional (e.g. signatures, form fields, picture annotations, necessary attachments, etc.)
- Polices: Define what the user is allowed to do (edit, save, etc.)

Show all documents of the envelope

Enable the user to comfortable read all documents of the transaction including text written in small font sizes

Fill Out Any PDF Form

Text data that can be extracted automatically from the data fields

Add Annotations

Text, freehand, marker or Image/photos

Add Attachments

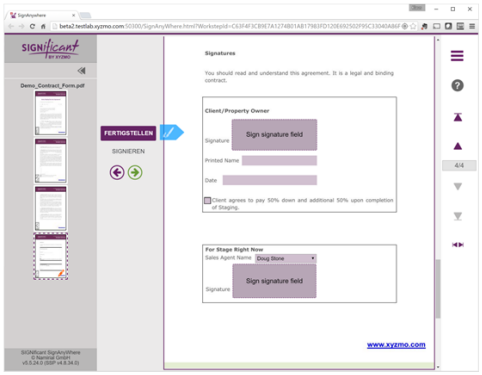
Files of all formats

Sign document

Enable the user to sign the document using pre-defined signature fields assigned to him or her

Automated finish actions

Automate tasks that need to be done once the user completed its actions such as triggering workload actions (e.g. document archiving) and displaying response messages



SIGNificant provides applications for document signing within all-important platforms including:

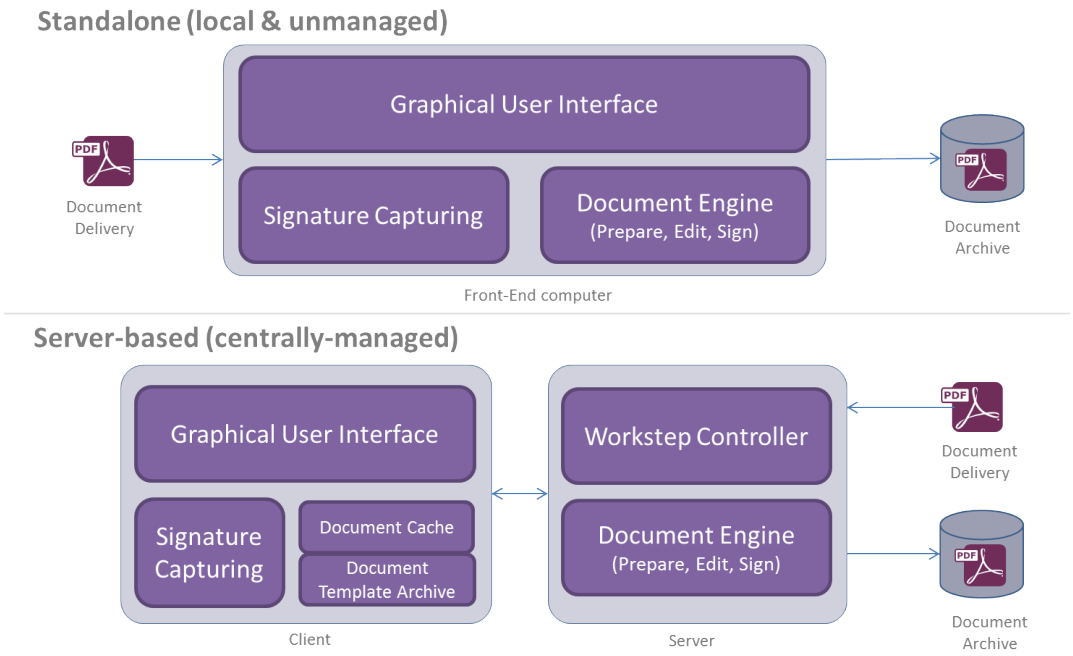
- Web (as pure HTML5, with native plugins or with signature capturing on smartphones),
- Windows Desktop,
- Windows Modern UI,
- Thin clients running on Windows or Linux,
- Android,
- iOS.

4.2.1 SIGNificant architecture and deployment

Server-based vs. standalone application

SIGNificant is typically deployed as a server-based platform solution. Alternatively, Namirial also provides standalone e-signing software for Windows Desktop, iOS, Android and Windows Store. These apps are marketed under the brand name “xyzmo”.

The SIGNificant server platform can be deployed on the customer premises or be consumed as a software-as-a-service (SaaS) solution from the Cloud. The SaaS solution is marketed under the name eSignAnyWhere. For on-premise solutions, customers can choose between a standalone and a server-based approach.



Customers choose the server-based approach over the standalone option because:

- The integration to existing systems is purely server-side, which is the natural choice for a server-based back-end architecture;
- Clients only have streaming access to the PDF via a secure link, while the signed original document is stored and managed server-side in the secure data-center — as opposed to copying the PDF to the clients where access to the signed original can hardly be managed securely.;
- Digital sealing/signing certificates (which include private keys) shall be managed purely server side such as in a High Security Module (HSM)
- A central audit trail documents all user interactions;
- Contrary to the opinion that server-based approaches need a constant network connection from the client, duly built apps can provide offline support for mobile tablets and smartphones through document caching and templating within the app itself;
- There is only one back-end integration necessary for all supported channels / use cases and e-signing technologies;
- It is perfect for companies that centralize their front-end software through terminal service solutions as e-signature client applications provide a much better scalability than “fat apps” that are not distributed across client and server.

In contrast, purely desktop/local-based signing approaches are typically preferred if:

- The document to be signed is created dynamically by the client itself and should not be sent to a server before it can be signed by the client;
- Server-side integration is not necessary;
- Very poor network connectivity exists between clients and server, resulting in low stability, under-provisioned network bandwidth and high latency (which, however, can be widely mitigated through local caching and background syncing).

Separate application (user interface) vs. seamless integration via SDK

If you require a fast and cost-efficient deployment, a ready-to-go graphical user interface is typically the best choice. This option usually still allows easy customization of color schemes, logos, etc., to suit your requirements.

If you do require a seamless integration into an existing application (without a UI context switch), then the SDK approach will be the most appropriate. Here you can manage the detailed user experience and all GUI elements yourself through advanced coding. Powerful SDKs allow much more than simple integration of core functionality, such as providing a complete adaptable user interface with a framework to seamlessly integrate it.

Device options for capturing biometric signatures

To capture biometric signatures, customers can choose between:

Smartphones

IndirectSales

+ Lowest common denominator
+ Captures biometrics on every smartphone (iOS, Android, Windows)
+ High security through native app with on-device encryption
+ Allows customers to also sign on their own device
+ Practically zero HW-costs
– Requires PC screen for document reading
– Requires pairing with PC/document
– Response time of 2-3 sec

Signature pads

POS with little space

+ Very robust (Wacom EMR)
+ Can already show the document
+ High security through on-device encryption
+ Battery free
+ Very cost effective
○ Not mobile, but plug'n play
– Requires PC screen for comfortable document reading
– Limited use for POS advertising
– Response time of 2-3 sec (color)

Signature Monitors

POS with eContracting

+ In-document signing experience
+ Fast (zero delay as it is a screen)
+ Parallel usage to operator PC
+ Client monitoring with assistance mode
+ Very robust (Wacom EMR)
+ High security through on-device encryption
+ Great for POS advertising
+ Battery free
○ Not mobile, but plug'n play
– Pen operation only
– More expensive

Tablets

Consulting

+ Great when sales and client can work with the same device
+ Simple & familiar touch UI for page browsing and editing
+ In-document signing experience
+ Mobile & offline support
+ High security through native apps with on-device encryption
+ Great for POS advertising
+ Multi-purpose device
– Battery required
– Separate computer to manage
– More difficult to secure
– More expensive

While signature monitors and tablets allow the user to directly sign on the same device on which they read the document, smartphones and signature pads typically just capture a signature, and the document is usually read on a different device such as a PC screen. However, signature pads with a color screen also can render the document or show transaction information, though font-size may be small.

4.2.2 Scalability and performance

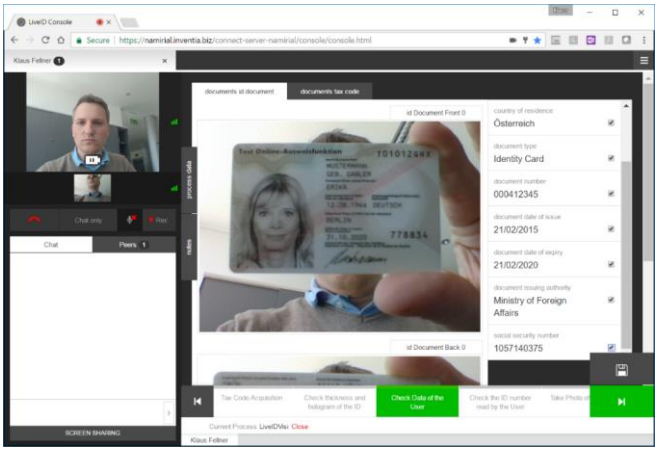
The largest installations in a branch office POS use-case scenario (e.g. bank branches) have more than 30,000 client seats connected to the SIGNificant Server. These include Poste Italiane, Unicredit, Intesa Sanpaolo and the Department for Work and Pensions UK. The clients for those SIGNificant Server installations are deployed "nationwide" in each branch office and their POS.

Remote singing scenarios that directly include users from home or on the go (= eSignAnyWhere) use exactly the same back-end system (= SIGNificant Server Platform), but a different front end (= HTML5 signing client) that is tailored towards its use case.

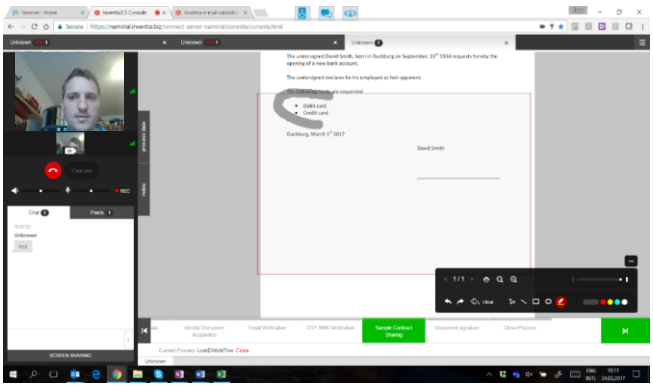
4.3 LiveID

LiveID integrates online customer onboarding and real-time customer engagement into a single process. Integrated in eSignAnyWhere and/or SIGNificant it even provides a real-time signing experience to the remote singer.

Its easily adaptable video-based identification process is designed to onboard new customers online in compliance to the Know-Your-Customer (KYC) rules of national Anti-Money-Laundry (AML) regulations. To accelerate the logging process, an OCR service may be plugged in. To further secure the online identification processes additional services maybe plugged in as needed.



LiveID enables customers to provide sales assistance to their online clients to reduce transaction abortion rates enabling them to close even complex contracts online. This includes video chat, text chat, voice chat, screen and document sharing incl. mark-ups and co-browsing of Web pages.



User can access the WebRTC based LiveID application from PC, mobile phone or tablet simply from a compliant Web browser or via an app. Here, LiveID opens a direct peer-to-peer communication with the client. Built-in signaling services help to establish that connection in case either party is blocked by firewalls.

Typical use cases are consumers on their own device (e.g. smartphone at home or on the go) or on a kiosk system in an unattended branch office.

4.4 Namirial Trust Services

4.4.1 Digital signing certificates

The Namirial Trust Service Provider (TSP) is a Certification Authority registered in Italy (see http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi) that operates according to directive 1999/93/EC and eIDAS 910/2014.

As of July 1, 2106, the EU directive 1999/93/EC has been superseded by EU Regulation 910/2014, known as “eIDAS”. Namirial is a Qualified Trust Service Provider (QTSP) according to eIDAS (see http://tlbrowser.tsl.website/tools/index.jsp).

Namirial can issue to an individual both qualified and non-qualified signature certificates through its Certification Authority Services. All qualified certificates released by Namirial

are natively trusted by Adobe Reader since Namirial is a member of the Adobe Approved Trust List (AATL – see https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html).

> The Adobe Approved Trust List is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in Adobe® Acrobat® or Reader® software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the high-assurance, trustworthy certificates on this list is trusted by Acrobat and Reader.

Issued qualified certificates have to be stored on qualified e-signature creation devices. Such devices can either be:

- Entirely user managed (e.g. smart cards), or
- Server-side managed on behalf of the signatory (remote signatures, see section 4.4.4).

In user-managed environments, Namirial can issue Qualified Electronic Certificates stored on a smart card, USB stick or microSD card. Moreover, it can provide the means to apply electronic signatures to clients, SDKs and platforms not only with its own digital certificates but also in cases where the signer already has a Local Certificate released by another Certification Authority or Trust Service Provider.

To issue a qualified signature certificate, Namirial TSP has to ensure that the individual to whom it issues the certificate is properly identified. When issuing certificates on a smart card or similar physical device, this identification has to be done face to face through a registration authority operator (RAO).

To support the issuing of certificates for remote signature over the internet, the certificate holder can also be identified through video identification (see section 4.4.6) by a local registration authority (LRA). Identification can be simplified or even waived (only with financial organizations) for certificates that have a “limitation of use” to the relations of the LRA with the holder (e.g. the certificates are only used for banking purposes). See the white paper “A guide on eIDAS 910/2014” for further details.

4.4.2 Digital sealing certificates

Namirial TSP can also issue sealing certificates that, in contrast to signing certificates, are not issued to an individual, but to an organization. These sealing certificates are typically used together with a biometric or HTML5 signature, as those e-signature technologies identify the signatory using other means (see section 3.4).

Sealing certificates themselves can again be qualified or non-qualified. Qualified sealing certificates are a new development allied with eIDAS legislation and have similar requirements as signing certificates, meaning that they also need to be stored on a qualified e-signature creation device.

4.4.3 Time stamping services

Namirial is a Qualified Trust Service Provider that can issue Qualified Time Stamps according to eIDAS Regulation (EU) 910/2014. An ‘electronic time stamp’ means data in electronic form that binds other data in electronic form to a particular time, establishing evidence that the latter data existed at that time. Such service is useful to archive and/or fill electronic documents digitally signed, especially documents having legal validity.

Namirial is certified as a qualified trust service provider (QTSP) for the creation of Qualified Time Stamps under the “eIDAS” regulation EU 910/2014 (ETSI EN 319_401, 411-1, 411-2, 421, 422).

- To be granted qualified status, Namirial was audited by a Conformity Assessment Body (CAB), which certified the Time Stamping Services;

- The Italian supervisory body (AgID), after analyzing the CAB audit report, granted qualified status to Namirial.

The CAB certification was granted by Bureau Veritas on 25 July, 2016, and is valid for three years.

4.4.4 Private key management

Namirial TSP provides trust services to manage decryption keys, such as that required to decrypt biometric signatures.

Here the trust-center issues a custom biometric protection certificate (public and private key) and safely stores the private key in RES² and for backup reasons on three smart cards that are stored in three different locations. Access to the private key is only possible through the trust center plus the customer together. In the case of a dispute, Namirial TSP also offers to support the customer with legal experts at court.

4.4.5 Namirial RES²: remote digital signing solution

Some use cases, industries and countries demand certificate-based personal digital signatures. In such cases, the highest legal value of a signature—which is deemed to be equivalent to a wet ink on paper signature—can only be realized by using certificate-based signatures. This generally applies to the so-called Qualified Electronic Signatures (QES) used in the European Union under the eIDAS Regulation.

A remote signature is a QES essential in several scenarios, especially online where the document recipients need to sign remotely without the need to use USB sticks or smart cards with local certificates.

To execute a remote signature, a user needs to input a PIN and a one-time password (OTP) to access his/her digital certificate, which is stored on a tamperproof hardware security module (HSM).

Namirial provides qualified certificates, clients, apps, SDKs and platforms for remote electronic signatures that ensure proper process execution, maximize automation of all steps, and only raise alerts and reminders if something goes wrong.

In addition to the Digital Transaction Management and remote electronic signing trust platforms, the following Namirial products allow the apposition of a remote electronic signature.

Namirial provides a solution for executing remote electronic signatures that can meet several legal and architectural requirements and has been used to process hundreds of millions of customer documents.

RES^2 is based on digital certificates with keys stored in HSMs. It is based on two components:

- The SignWebServer Virtual Appliance (SWS), which integrates with the customer applications and operates at a high level (i.e. at document level). When integrated with SIGNificant, SIGNificant itself takes this role;
- The SignEngine (SE), which controls the HSM and operates at a lower level (i.e. hash file).

As an alternative, Namirial can also provide a Signing Client (on Windows, MacOS, iOS, Android) that provides an interactive user interface to sign documents and interacts directly with the SE.

RES^2 provides web services to:

- Create, suspend or revoke a digital certificate,
- Sign a document (with or without a time stamp),
- Sign a list of documents (with or without a time stamp),
- Verify the signature on a document (also on a specific date),
- Send a one-time password via SMS,
- Sign or verify very large documents.

The following OTP mechanisms are supported for two-factor authentication with PIN (= user password) and:

- OTP token (a physical device),
- Virtual OTP (on iOS and Android),
- SMS OTP,
- Biometric authentication – such as through handwritten signatures as provided by SIGNificant (see section 3.4).

Standard certificates are valid for three years. Disposable certificates, which have a reduced time span of just 60 minutes, do not require recipients/holders to actively manage their own PIN because the certificate cannot be reused for executing new signatures once this time span of 60 minutes has expired anyway. Instead, the PIN is here automatically managed by the application, which makes time-limited certificates the perfect choice for non-recurring business cases.

Automatic signature that digitally signs a large number of documents in a batch process automatically (e.g. e-invoice signature, company-side contract acceptance, other) is also supported. As users do not read such documents, automatic signatures do not require an OTP.

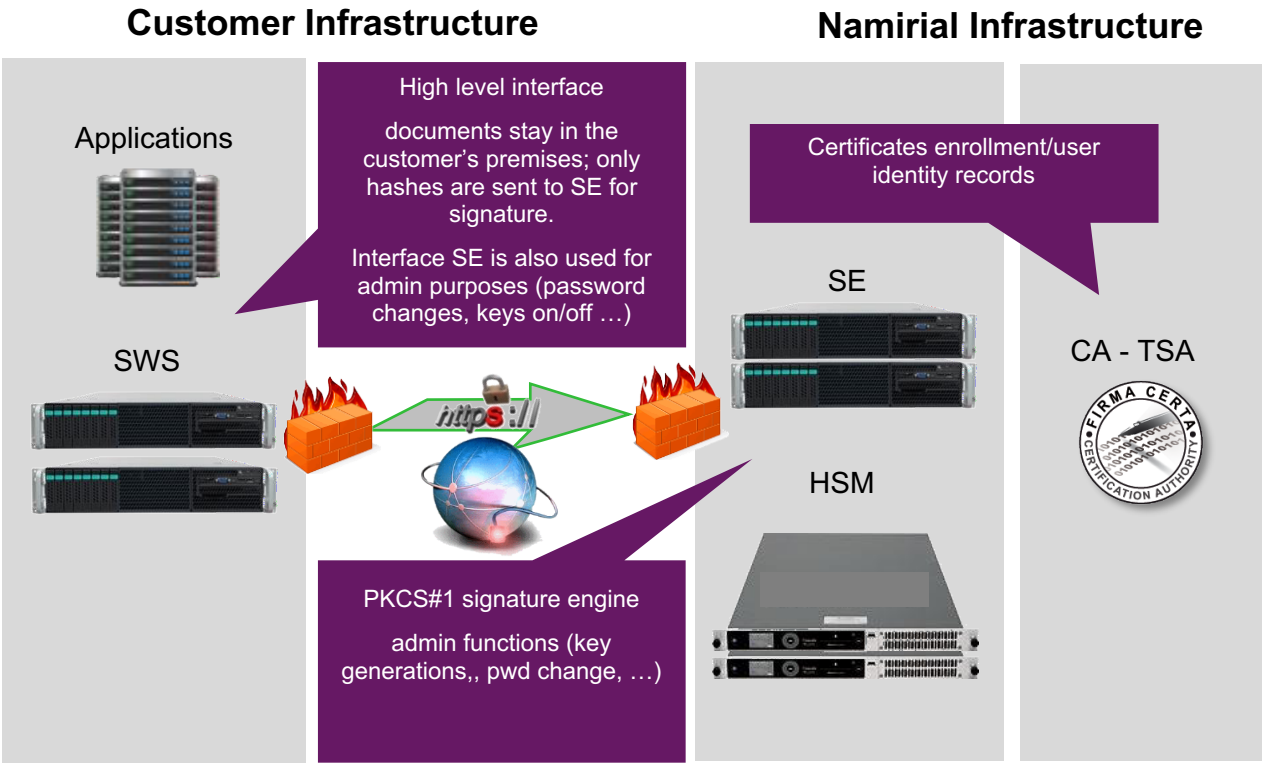
All of the following Advanced Electronic Signature (AdES) file types are supported:

- PAdES, to sign PDF files
  - The output document is a PDF;
  - Templates can be used to position the signature at a specific page/position;
  - Password-protected documents are supported and generate a signed and password-protected document;
  - Non-password-protected documents may be signed and encrypted to generate a signed and password-protected document;
- XAdES to sign XML files
  - The output document is an XML file that can be processed by the same application that generated it;
  - It is possible to sign all or part of an XML file;
- CadES to sign every type of file (text or binary)
  - The output document is a .P7M file that requires a specific viewer to open/verify the file (Namirial provides a free client to sign/verify .P7M files).

A Cloud architecture is the recommend solution for up to 1,000,000 signatures per day. In the RES^2 Cloud architecture (illustrated below), the HSM and the SE are installed in the Namirial Certification Authority Data Center.

The customer needs only to install SWS in his/her data center and to integrate its applications.

- SWS and the customer application (that are in the same data center) may efficiently exchange large volumes of documents within the same network environment;
- SWS and SE exchange only the document hash (7–10 KB) for optimum performance;
- There is no need for the customer to invest in HW since SWS is a virtual appliance. Only a virtual machine is required.



While not recommend, an on-premises solution may be deployed, where SWS, SE and the HSM are hosted in the customer data center.

Scalability and performance

Namirial Remote Signature Solution is currently supporting on average more than 100,000 signatures per day, with peaks exceeding 1 million per day.

The solution can scale to process tens of millions of transactions per day, by supporting multiple HSMs, including customer-dedicated HSMs.

4.4.6 Video identification to release a qualified e-signing certificate

The standard procedures for activating a Qualified Certificate require a face-to-face identification performed by a Registration Authority Operator. This is of utmost importance because the Qualified Certificate is the electronic equivalent of an ID document and it identifies and qualifies an individual or an entity in a digital way.

LiveID (see 4.3) allows remote web-based identification where a user interacts with a remote operator in order to perform the identification procedures needed to release an eIDAS-compliant Qualified Certificate. The LiveID platform provides security procedures approved by the National Supervisory Body to mitigate the risk of frauds and identity theft.

Once the identification process is complete, the operator starts the enrollment to release a Qualified Certificate to the identified user.

4.4.7 Electronic Registered Delivery

Electronic Registered Delivery is a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving of the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations.

According to the Italian supervisory body (AgID), the Italian PEC (Posta Elettronica Certificata—registered email) fulfils all the requirements of an Electronic Registered Delivery service, but only some of the requirements of a qualified electronic delivery service.

4.4.8 Long-Term Archiving

Long-Term Archiving allows all documents generated while performing digital business transactions to be protected, preserved and made easily searchable. Current legislations may require long-term archiving for various kind of documents such as invoices, contracts, fiscal books and other documents originated and signed in electronic form.

Namirial has been accredited by AgID for Long-Term Archiving/Digital Preservation Services through its StrongDox product. StrongDox is a SaaS, high-availability, multi-company solution that can be used to archive large volumes of documents. Today, more than 2 billion document pages are archived according to the existing regulations.

Key facts about StrongDox:

- Available as SaaS and on-premise deployment
- Based on a Web UI + Digital Preservation Engine
- Web UI provides simple way to archive documents and ensures their availability
- Digital Preservation ensures authenticity, integrity, reliability and accurate logging
- Scalable architecture based on redundancy enables massive document volumes
- Standard-based preservation engine on ETSI TS 101 533 V1.1.1 (2011-05) Part 1: Requirements for Implementation and Management & Part 2: Guidelines for Assessors
- ISO 27001 certification on architectural design
- Supports a preservation process in compliance to the Open Archival Information System (OAIS ISO 14721: 2012)

Additionally, StrongDox for SaaS adds the following:

- Verification of human readability of the document
- Insurance to cyber threats of at least €100k per incident
- Web-oriented and multitenancy enabled

- Based on a redundant infrastructure in high availability with geographical replication and disaster recovery managed in data centers certified ISO / IEC 27001.
- Certified by AgID/Italy – Namirial is Digital Preservation operator
- Datacenter in AWS (e.g. Dublin or Frankfurt)

5 Namirial DTM Solution for Qualified E-Signatures

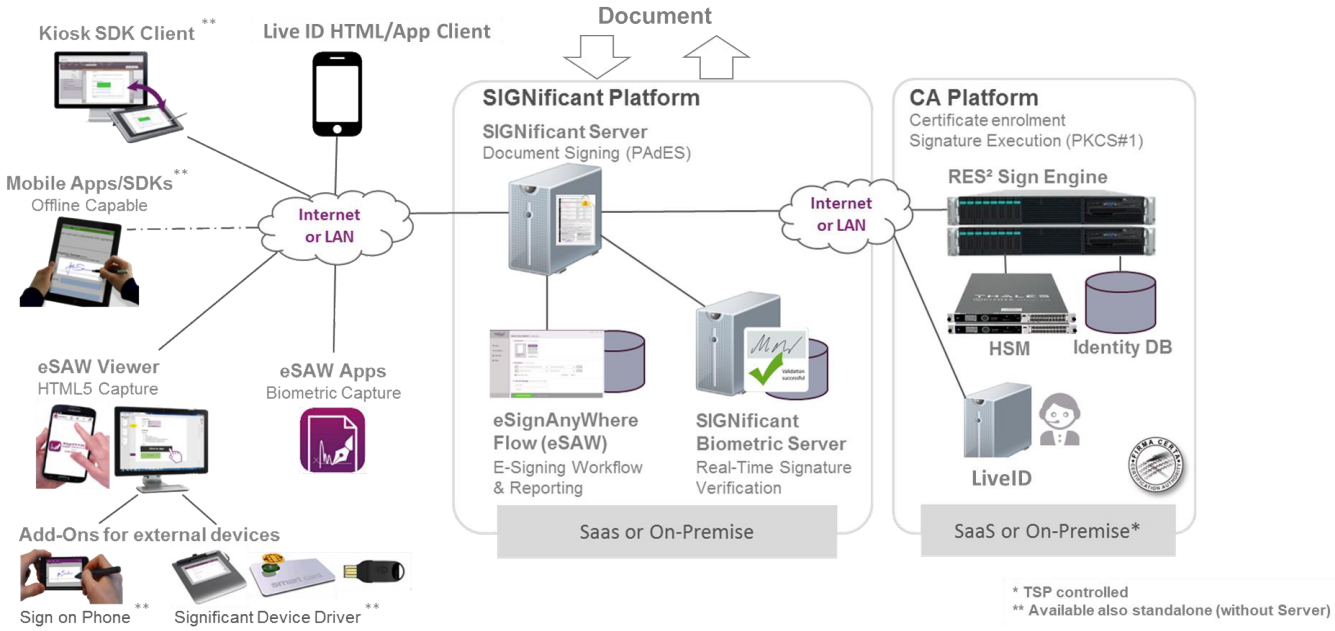
To satisfy the “legal written form” in the EU, which is required in many countries (e.g. for consumer credits such as car leasing, sales financing and mortgages), Qualified E-Signatures (QES) are required. Now that the new eIDAS regulation allows a “Qualified Trust Service Provider” such as Namirial (see section 3.2) to manage the qualified e-signature creation environment on behalf of the signatory, the main obstacle for implementing a QES solution in a B2C scenario has been removed. Instead of having to issue a QES certificate on a physical device (such as a smart card), Namirial can simply issue it virtually and manage it in its Remote E-Signature environment, RES².

To fully unleash the potential of qualified remote e-signature, Namirial has combined it with the SIGNificant e-contracting platform. An overview about the solution’s building blocks and how they are connected is provided in the figure below. As shown, the SIGNificant Server Platform (SSP), which typically runs on customer premises to keep documents fully private, takes the central role of digitally signing the PDF with a PAdES-compliant digital signature on documents that a signatory view on one of the connected client applications.

When required to use a remote signature certificate, such as in the case of a qualified signature, SSP uses the Namirial RES² qualified remote signature system to create the necessary PKCS#1 signature string that is the core of a PAdES-compliant signature; otherwise, it simply creates it using its own local digital signing engine.

RES², which Namirial uses to control the qualified trust service provider, typically runs as a Cloud service to make it easily accessible. It simply receives the hash of the document to be signed and the authentication proof for using a specific remote signature certificate that it manages on behalf of a signatory. Once the authentication is verified, it creates the PKCS#1 signature data and returns it to SIGNificant.

LiveID may be used to identify a user by requesting a qualified signature certificate over the internet through video identification. Using the SIGNificant Biometric Server, customers may replace the standard OTP authentication with biometric signature verification in real time—which is typically done for qualified e-signatures at the point-of-sale.



5.1 POS in branch offices (e.g. car dealers or banks)

Here, both contractual parties meet face to face, which means that the organization that runs the POS has full control over the e-signing experience. While it is possible that clients may sign on their own device (e.g. smartphone), the standard scenario is that they read and sign contracts on a device that is set up for the use case, meaning that it has the proper size to comfortably read and sign documents and all necessary software is pre-installed.

On paper, the process known to clients comprises printed documents that they sign with their own handwritten signature. Now, Namirial enables sales organizations to digitalize this process without changing the basic user experience—meaning all it takes to interact with the user is a device that can display documents and capture a handwritten signature. The Namirial DTM solution is implemented through the following steps:

1) Identify the client
   —using face-to-face identification and storing the identification assets for audit purposes (the latter is only required by non-financial organizations as they are not under AML rules);
2) Ask the client to sign the certificate request form to receive a qualified e-signing certificate using SIGNificant for biometric e-signatures;
   a. Create a biometric signature verification profile using the just recorded signature to enable biometric authentication for executing a QES using the client's qualified e-signing certificate
3) Ask the client to sign the document that requires a QES
   —using SIGNificant for biometric e-signatures
   a. Automatically issue a disposable QES certificate once the client signs qualified for the first time using the SOAP API of RES²;
   b. Authenticate the just-captured biometric e-signature vs. the previously created signature verification profile (see step 2a) to execute a QES using the client's personal qualified signing certificate managed in RES²
      —using SIGNificant Biometric Server;
   c. Replicate this step on every signature field that requires a QES
      —using SIGNificant Biometric Server;
4) Delete the signature verification profile after the end of the e-signing session

5.2 Online on the Web using LiveID and eSignAnyWhere

Here, both contractual parties meet only virtually over the internet, which means that the client needs to use whatever device they own (e.g. smartphone). The more limitations you put on that (e.g. certain device types, operating systems, installation required), the more potential customers you lose. Thus, the consensus view is that the ideal client app is a pure HTML5 application that works on any device and does not require any installation.

Over the internet, customers are used to signing using a one-time password, e.g. from their home banking application. Also, a biometric signature can typically not be used here as such signatures require a) a native app to be installed on the signing device, and b) the client to use a pen to write a handwritten signature. Both requirements can typically not be met in a remote scenario.

The Namirial DTM solution is implemented through the following steps:

1) Open the LiveID session
2) Identify the client using a pre-defined process via video (KYC-AML compliant);
    a. Register the one-time password (OTP) device (cell phone)
3) Ask the client to sign the request form to receive a qualified e-signing certificate simply with Click2Sign
4) Display the contract to be signed in SIGNificant SignAnyWhere Viewer
    a. Assist the client as needed with video, voice, text chat while document views are synchronized
5) Ask the client to sign the document that requires a QES online —using SIGNificant SignAnyWhere Viewer
    I. Automatically issue a disposable QES certificate once the client signs qualified for the first time
    II. Authenticate the client's use of his/her personal qualified signing certificate managed in RES² for executing a QES
    —using OTP on the previously registered phone number;
        a. You may combine multiple signatures within a batch signature
    III. Replicate step II as needed for additional signature operations

For the client, the process outlined above simply involves a regular video session and the use of an OTP on their mobile phones, which clients are already accustomed to in their online banking software.

6 Current key differentiating features vs. competing products

Namirial is uniquely positioned today as a leading provider in the DTM market thanks to seamlessly integrating:

- the SIGNificant e-contracting platform
- with the Namirial trust center.

While the SIGNificant platform supports all use cases, types of signature and user experiences and can be deployed as desired by the customer (on-premises, in cloud, or a hybrid), the Namirial trust center is a Qualified Trust Service Provider, certified under eIDAS, that allows a relatively effortless implementation of qualified e-signature, even in B2C processes. While both can be used in isolation, it is the pre-built integration of the Namirial platform that makes it even more attractive.

By selecting Namirial as its DTM provider, a customer can be sure his/her investment is preserved over time, as needs evolve and new types of use cases, signatures or user experiences may be required.

Moreover, an extensive partner network supports Namirial products and services and allows a fast adoption of e-signature technologies.

Finally, the scalability of products and services has been tested in very large installations. The company has deployed more than 250,000 sets of handwritten biometric signatures and has stored more than 3 million biometric profiles, processes more than 100,000 signatures per day with peaks of 1 million in its cloud services, and stores in Long-Term Archiving more than 2 billion document pages per year. Our estimate, including on-premise installations, is that millions of transactions are processed daily by Namirial products.

Need some help to decide how to start?

At Icon UK we have a team of experience experts who can quickly help you identify the options for implementation e-signing based on your specific requirements.

Please contact us by phone +44 (0)203 150 1081 or e-mail: info@icon-uk.net