A guide on eIDAS 910/2014

Namirial DTM solution for legally compliant e-signatures

NAMIRIAL GmbH

Legal Office: Seilerstätte 16, 1010 Wien, Austria
Main Office: Haider Straße 23, 4025 Ansfelden | Phone: +43-7229-88060 | www.xyzmo.com
Fiscalnumber 09 258/9720 | VAT-ID: ATU70125036

Table of Contents

1 What is eIDAS?

Regulation (EU) no 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/CE was published in the Official Journal of the EU on August 28, 2014, concluding a legislative process started in June 2012, when the EU commission proposed a new regulation covering the matters established in the title of the same regulation.

The 52 articles of the new regulation cover several different aspects of electronic transactions, including:

- electronic identification;
- trust services, comprising
    - electronic signatures, seals, and time stamps,
    - electronic registered delivery services,
    - certificates for website authentication, and
    - data preservation for signatures, seals, and certificates; and
- electronic documents.

The Regulation went into effect on July 1, 2016, and the news and differences regarding the Directive are numerous. The central figure of the Regulation is the trust service provider, which can issue qualified or non-qualified trust services.

From a legal point of view, both qualified and non-qualified trust services benefit from a non-discrimination clause, as evidenced in the courts. This means that trust services cannot be discarded by a judge only on the ground that they are electronic. Article 46 of the eIDAS Regulation establishes that an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

However, because of the more stringent requirements applicable to qualified trust service providers, qualified trust services provide a stronger specific legal effect than non-qualified ones, as well as higher technical security. Qualified trust services, therefore, provide higher legal certainty and higher security for electronic transactions.

2 Electronic identification

As many member states have already deployed electronic identification schemes (based on quite different technologies), Regulation 910/2014 does not opt for harmonization of the electronic means itself, but instead supports interoperability of the national schemes.

This option protects existing investments, but where the identification is based on official electronic documents or credentials (i.e. German neuer Personalausweis (nPA), Austrian BürgerKarte, Italian SPID, etc.), the EU does not have regulatory competence.

This chapter of eIDAS (eID) is based on notification of national eID schemes. Member states can notify the Commission of their schemes.

The conditions for notification are established in articles 7, 8, and 9 of eIDAS. The most important keywords for an eID compliant with the Regulation are “level of assurance” and

“interoperability framework.” The Regulation mandates the establishment of three *Levels of Assurance,* which describe the notified schemes according to their security, covering the complete lifecycle of the credentials, including enrollment, issuance of the credentials, usage, and finally revocation. The three levels—low, substantial, and high—are substantially compliant with levels 2, 3, and 4 of ISO/IEC 29115 or the STORK quality authenticator scheme.

The interoperability framework is technically compliant with STORK specifications (https://www.eid-stork.eu).

3 Electronic signatures and seals

The eSignatures, as ruled in the 1999/93/EC directive, are developed in the eIDAS Regulation. Starting July 1, 2016, when the trust services provisions under the eIDAS Regulation apply, an eSignature can only be used by a natural person to “sign,” i.e. mainly to express consent on the data on which the eSignature is put. This differs from the 1999/93/EC directive in which the eSignature—which could also be used by legal persons—was defined as a means for authentication. So, under eIDAS, the “signatory” will be a natural person who creates an eSignature.

Therefore, certificates for eSignatures can no longer be issued to legal persons. Legal persons will be able to use certificates for eSeals (whose aim is not to sign but to ensure the integrity and origin of data).

eIDAS (similar to the 1999/93/EC directive) defines the following three signature levels:

- Electronic Signature (ES)
- Advanced Electronic Signature (AES)
- Qualified Electronic Signature (QES)

Whereas electronic signature is just a juridical principle without an evidentiary effect, advanced electronic signature allows you to prove that a certain person signed a certain document at a defined/preserved state.

Qualified e-signatures, on the other hand, are the only signatures that shall have the equivalent legal effect of a handwritten signature on paper—meaning, in some European countries, only the QES satisfies the requirement for “legal written form.”

3.1 Advanced Electronic Signature

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using **electronic signature creation data** that the signatory can, **with high level of confidence**, use under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

The new regulation provides, first of all, a new and broader definition for the key concept of electronic signatures. That concept has been defined as data in electronic form that is attached or logically associated with other data in electronic form and “*which is used by the signatory to sign.*” The text in italics replaces the former definition in the old Directive: “*which serve as a method of authentication.*” This important change in the definition **shifts the**

focus from the authentication of the signatory to the intention of the signatory (from "Who placed the e-signature?" to "Did the signatory want to agree to the signed content?")**.**

In addition to the unchanged requirements—the data must (1) be uniquely linked to the signatory, (2) identify the signatory, and (3) be linked to the signed data—an electronic signature should be created by the signatory, under his or her sole control, "*with a high level of confidence.*"

3.2 Qualified Electronic Signature

Already the old EU Directive 1999/93/CE, which is repealed by eIDAS 910/2014, defined qualified e-signatures as non-reputable, as it required signatories to use their qualified signing certificate, which is issued to them personally and that they have under their sole control. To guarantee their sole control, it is required that recipients of qualified certificates must be identified appropriately and that qualified certificates must be stored and used with a secure signature creation device that requires authentication with every use.

The new eIDAS regulation now defines common rules for all EU members regarding how this has to be done. First of all, the new regulation creates a common market for qualified certificates and signatures. That means that:

- Qualified e-signatures (QES) from one EU country are valid throughout the EU.
- QES certificates issued from a qualified trust service provider (QTSP) are valid in the entire EU.
    - National certificate authorities (CAs) that want to become a QTSP need to be accredited by national supervisory bodies by July 1, 2017. Supervisory bodies grant qualified status to trust service providers after they have successfully been audited by a conformity assessment body (CAB).
    - Until completion of their assessment, accredited national CAs shall be considered QTSP until July 1, 2017.

Next, eIDAS introduces the concept of remote e-signatures, which already existed in a few EU countries, and makes them available to all member states:

- Remote e-signatures (for which an e-signature creation environment is managed on behalf of the signatory) may receive the same legal recognition as e-signatures that are created in a way that is entirely user-managed.
- Generating or managing e-signature creation data on behalf of a signatory—for a qualified remote e-signature—may only be done by a qualified trust service provider (QTSP).
    - E-signatures may be generated or managed either in the data center of the QTSP (Cloud service) or on customer premises (under the control of the QTSP).

In addition, the regulation regulates what a QTSP has to use to create a qualified (remote) e-signature:

- Qualified e-signature creation devices require certification by public/private bodies designated by member states.

Finally, a QTSP can only issue a qualified signing certificate to a recipient (a signatory) after the signatory's successful identification in accordance with national law, using one of the following methods:

- By physical presence (face-to-face),
- Remotely, using electronic identification to ensure a physical presence (live video ID), or
- By using other ID methods recognized at the national level that ensure physical presence (e.g. eID).

The exact processes that a dedicated QTSP has to follow to provide qualified e-signatures are described in its "operating manual" or "certificate practice statement," which must be assessed during the CAB audit.

4 Time stamping

In accordance with eIDAS (article 3, number 33), 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.

Equally important is the definition (article 3, number 34) of "qualified electronic time stamp," which means an electronic time stamp that meets the requirements laid down in Article 42.

These requirements are as follows:

a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
b) it is based on an accurate time source linked to Coordinated Universal Time; and
c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

The description of the time stamp explains that this data in electronic form can be used to acknowledge the circumstance that the stamped object existed before the date and time appointed in the same time stamp.

The data structure for the time stamps is established in the document "ETSI EN 319 422: Time-stamping protocol and time-stamp profiles."

Trust service providers that want to attain qualified status need to be accredited by a national supervisory body after they have successfully been audited by a conformity assessment body (CAB).

5 Electronic registered delivery service

According to the Commission highlights, electronic registered delivery services provide a secure channel for the transmission of documents bringing evidence of (the time of) sending and receiving the message. Nevertheless, the Regulation does not automatically include (qualified) electronic registered delivery services to registered postal mails (registered items) defined under the Postal Directive. Member states remain free to establish such equivalence at national level. In other words, when the law requires compliance with a specific procedure by sending a registered postal mail, using (qualified) electronic registered delivery services would meet the requirements only if the national law has established the equivalence.

The Italian PEC (Posta Elettronica Certificata—Certified Electronic Mail) is compliant with the rules of a non-qualified electronic registered delivery service, because the PEC meets the requirements of Italian law for equivalence with registered postal mail.

6 Qualified preservation service

A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

However, signature preservation is not applicable until an implementing act or delegated Act is published in which there is a reference to a related ETSI standard, which probably could be ready no earlier than the end of 2017.

Furthermore, it is worth noting that preservation is different from electronic archiving, which aims at ensuring that a document is stored in order to guarantee its integrity (and other legal features). The technology underpinning electronic archiving therefore targets the document. Electronic archiving is not a trust service under eIDAS and is in the specific competencies of each member state.

7 Technologies to implement e-signatures

Digital signatures are defined according to the following three file types:

- PAdES to sign PDF files
  The signed PDF is readable in any standard compliant PDF software.
- XAdES to sign XML files
  It is possible to sign all or part of an XML file. The output document is also a 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.

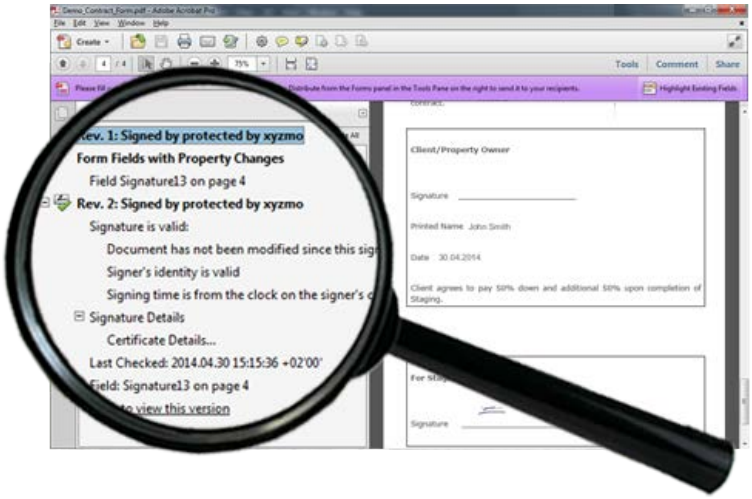
In the next section of this chapter, we focus on PAdES-compliant e-signatures, because PDFs are a widely accepted document standard and thus a perfect fit for digital document-based transactions.

7.1 PAdES Standard

7.1.1 Basic Profile (based on ISO 32000-1)

Digital signatures are well defined in each 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 any proprietary software. This includes the following data:

- A signature image (a visual representation of the signature);
- The document status at the time 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;
- The date and time the document was signed—optionally through a qualified time stamp service;
- The geolocation where the document was signed (GPS data if provided); and
- The identity of the certificate holder, which, if a sealing certificate was used, as it would be for biometric signatures (see 7.2.1) or HTML5 signatures (see 7.2.2), typically points to the issuer of the signed document.



7.1.2 Long Term Validation (LTV Profile)

Validation of a PAdES signature requires data such as CA certificates, certificate revocation lists (CRLs), or certificate status information (OCSP), 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 is thus the perfect equivalent to the PDF variant 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, called Document Security Store

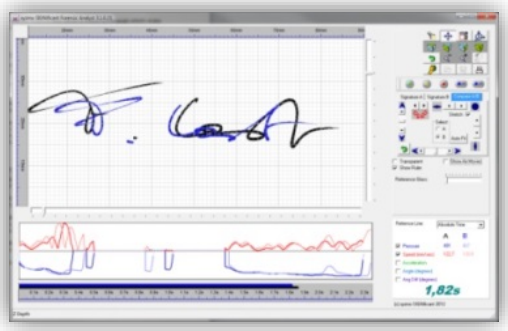
(DSS), to carry such validation data as is necessary to validate a signature, optionally with validation-related information (VRI), which relates the validation data to a specific signature. Additionally, it uses another extension, Document Time-Stamp, to extend the lifetime of protection of the document. The document time-stamp also protects the DSS by binding it to the document to which it applies.

The lifetime of the protection can be further extended beyond the life of the last document. A new time-stamp can be applied by adding further DSS information to validate the previous document's time-stamp at the time of the application of the new document time-stamp.

7.2 PAdES compliant e-signing technologies for AES

Advanced e-signatures, among other things, must be able to identify the signatory. Both biometric and HTML5 based e-signatures achieve this, each in a different way.

7.2.1 Biometric signatures

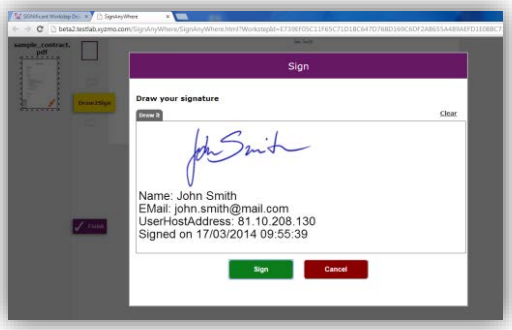


Biometric signatures transfer the process of signing and signature verification 1:1 from the paper world to the digital world. Signatories sign with their handwriting using a pen and, if required, a graphologist forensically verifies the previously captured handwritten signature by comparison with a 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 the behavioural 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 a digitized signature is forensically identifiable (and far more reliable than the signed image alone).

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

Some solutions also provide a signature verification that authenticates a signature against a pre-enrolled signature profile database in real time. This allows you to not only secure the execution of certain transactions, 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.

7.2.2 HTML5 signatures



HTML5 signatures do not record any behavioural biometrical data as described in the previous chapter. Instead, HTML5 uses another method of identifying the signatory, namely an explicit authentication step that is finally logged into a secure server-side evidence book (producing a digitally sealed audit trail).

The big advantage of HTML5 signatures is that they:

1) do not require signatories to use a pen, which they typically are not able to use in a remote scenario in which they sign on their own device (e.g. smartphone), and
2) do not require the signatory to download and install anything to provide
    a. a real-time processing environment for the behavioural biometrical data, or
    b. a secure and reliable client-side encryption environment to protect a user's behavioural biometrical data against misuse.

Their drawback is that a possible identification of the signatory, and thus compliance with 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 done with the use of a PIN, one-time-passwords (OTP), e-mail access, or a combination of these, an identification of the signatory cannot be guaranteed without a dedicated upfront identification step, as is obligatory with digital signatures that are based on personal signing certificates (see chapter 7.3).

How the signatory then executes a dedicated signature field is a secondary question that more or less only addresses user experience. Popular methods are click-, type-, and draw-2-sign. See the whitepaper "Remote e-Signing via the Web" for details.

7.3 PAdES compliant e-signing technologies for QES

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."

The environment that is used to create the qualified e-signature can either be:

- Entirely user-managed on the client-side, which requires the signatory to carry his or her personal certificate on a secure device such as a smart card or special usb token, or
- Remotely managed on behalf of the signatory, which allows the signatory to store and manage a personal qualified signing certificate "virtually" on a secure server.

7.3.1 Entirely user managed environments (e.g. smartcards)

Qualified signing certificates that are managed by the user client side on a secure signing device are typically valid for one or more years. Issuing them requires a physical transaction (e.g. providing the smart card), which means that the required identification of the certificate recipient is typically done face-to-face by a registration authority officer (RAO) who has been appointed by the certificate authority. The issued certificate, which is bound on the issued device (e.g. smart card), then typically lasts one or more years.

While the generation of the qualified signing certificate with the CA-approved RAO must be done online, the qualified signing procedure itself can be done fully offline, e.g. on a desktop or laptop computer using a local standalone signing application that connects to the secure signing device that holds the qualified signing certificate.

To actually execute a qualified signature, the certificate holder needs to be authenticated using two factors. With a physical signing device, one factor is the possession of the device (e.g. smart card), and the second factor is knowledge of how to access the certificate (e.g. the PIN).

7.3.2 Remote signature

Because they are virtual, qualified signing certificates that are managed on behalf of a signatory server-side can be issued on the spot whenever needed during a business transaction. Thus, it is very helpful that eIDAS also allows identification of certificate recipients remotely via a live video session that ensures their physical presence.

Also, as certificates can be issued on the fly whenever needed, a reduction of their life-span may make sense, especially if a reduced life-span reduces costs and simplifies their usage. For example, it makes no sense for a user to have to create his or her own PIN for authentication when it can only be used during a single business transaction.

Remote signing, of course, works entirely online, allowing cross-platform HTML5 clients that do not have any platform dependencies, because they are free from any local components required to access local secure signing devices such as smart cards or USB tokens.

Authentication, in principle, works within entirely user-managed environments, as described in the previous chapter, meaning that the standard is two-factor authentication that is based on possession (e.g., possession of an OTP device such as a phone for receiving SMS or biometry with handwritten signatures) and knowledge (e.g. PIN). As mentioned above, certificates with a short usable time span for signing, which is not to be confused with the validity period of a digital signature, may simplify the process through automated PIN management.

8 A case study on an eIDAS compliant PAdES signature solution

The Namirial Digital Transaction Management (DTM) solution provides products and services to implement eIDAS compliant e-signatures on all three levels (ES, AES, and QES) with all three file types (PAdES, XAdES and CAdES).

8.1 Namirial software for advanced e-signature (AES)

Namirial's xyzmo and SIGNificant product lines enable you to implement simple and advanced PAdES compliant signatures using biometric or HTML5 signature technologies. For more information about them, please visit www.xyzmo.com.

Namirial's Firma Certa product enables users to digitally sign all three file types according to the PAdES, XAdES or CAdES standard, using digital signing certificates provided by the Namirial CA. For more information about this product, please visit www.namirial.com.

8.2 Namirial Trust Center Services for qualified e-signature (QES)

Namiral Spa is a qualified trust service provider that can issue eIDAS compliant qualified time stamps and qualified signing certificates. Its operating manuals and practice statements, audited by a CAB and approved by the Italian Supervisory Body AgID, are available on http://doc.namirialtsp.com and have been published by AgID at the following URL: http://www.agid.gov.it/sites/default/files/documentazione/mo_namirial_v1.9.zip_.p7m.

Namirial is also a member of the Adobe Approved Trust List (AATL), which means that the qualified certificates it issues are trusted by Adobe software, such as the free Adobe Reader. Consequently, Adobe Reader will mark digital signatures done with Namirial signing or sealing certificates as trusted, using a green checkmark (as opposed to the yellow question mark that Adobe Reader uses when a trust level is unknown).

Namirial Spa, as a QTSP, also provides a qualified remote e-signature environment called RES², which allows signatories to digitally sign using a qualified e-signing certificate that is managed on their behalf in a certified high security module (HSM)-based signing environment.

Together with the Namirial product for video identification, called ViSi, customers such as banks, insurance companies, retail merchants, governments, or other industries can **on-board new customers over the Internet**[1] and issue qualified signing certificates on the fly whenever needed.

Qualified certificates can be differentiated by their life span.[2] They can be actively used for e-signing. Namirial distinguishes between the following two certificate types:

- Disposable certificates, valid for 60 minutes during a business case, and

[1] Financial organizations need to find out whether video identification is allowed in their country to satisfy know-your-customer (KYC) needs in national anti-money-laundering (AML) regulations.
[2] Not to be confused with the validity period of a digital signature.

- Standard certificates, which are typically valid for three years.

The standard process for using qualified e-signature certificates can be divided into the following steps:

1) Identification,
2) Enrollment and certificate issuing, and
3) Usage.

While identification only needs to be done once, enrollment and certificate issuing is done each time a new certificate is requested. The certificate recipient can use the certificate during its life span for e-signing.

For more information, please visit www.namirial.com.

8.2.1 Identification

The Namirial operating manual defines face-to-face and remote identification using a live video session. Namirial, as a QTSP, must securely archive the identifications it does when issuing qualified signing certificates for 20 years.

To simplify the process of using qualified signing certificates remotely (they are managed on behalf of the signatory's server-side), the Namirial operating manual includes the following simplifications with local registration authorities (LRA, e.g. a local bank or retail organization) when issuing qualified signing certificates to certificate recipients (certificate holders) with whom the LRA has institutional, corporate, and/or commercial relations, in such a way that the certificates have a "limitation of use" to the relations of the LRA with the holder (e.g., the certificates are only used for banking purposes).

- The identification and registration of holder is carried out by the LRA in compliance with what is described in Namirial operating manuals or, alternatively, on the basis of LRA internal procedures previously communicated in writing to Namirial and expressly approved by the latter. There is no need to appoint registration authority operators, since the LRA is only responsible for identification and registration, while the qualified certificate is issued by Namirial.
- LRAs perform identification either face-to-face or using live video identification. It is the responsibility of the LRA to ensure that the used identification method is legal and accepted in the countries within which the LRA intends to operate.
- Registration of existing customers is performed by the interested third party. This allows bulk registration of customers.
- Identification is made using an electronic ID released and accepted in the country within which the LRA operates. Here, Namirial does not need to receive and store any identification assets, as the organization that issued the eID is responsible for that.
- Identification may have been previously performed according to the anti-money laundering (AML) EU directives. Here, Namirial does not need to receive and store any identification assets, as the financial organization that has to perform the identification according to the AML directive is responsible for that.

- Identification may be performed through credentials released for a previous disposable certificate.

8.2.2 Enrollment (issuing the certificate)

At the end of the enrollment phase, Namirial issues the (qualified) signing certificate to the recipient (holder). To do that, Namirial needs to receive the following base identity data about the holder it should issue the (qualified) certificate to:

- Surname and given name,
- Serial number (social security number, passport number, etc.),
- Country name (may be replaced by the customer country name), and
- Identification document type, number, and expiration date.

This information (except document ID data) will go directly into the issued signing certificate that is deployed into the signing environment (SE) of RES², and thus will be visible by anyone who reads a signed document that is signed using this certificate. The private signing keys referenced from these personal signing certificates are safely managed inside the certified high security modules (HSMs).

In addition, the holder and Namirial need to define an authentication method that allows the holder to control and assess his or her personal signing certificate remotely. This includes the following methods:

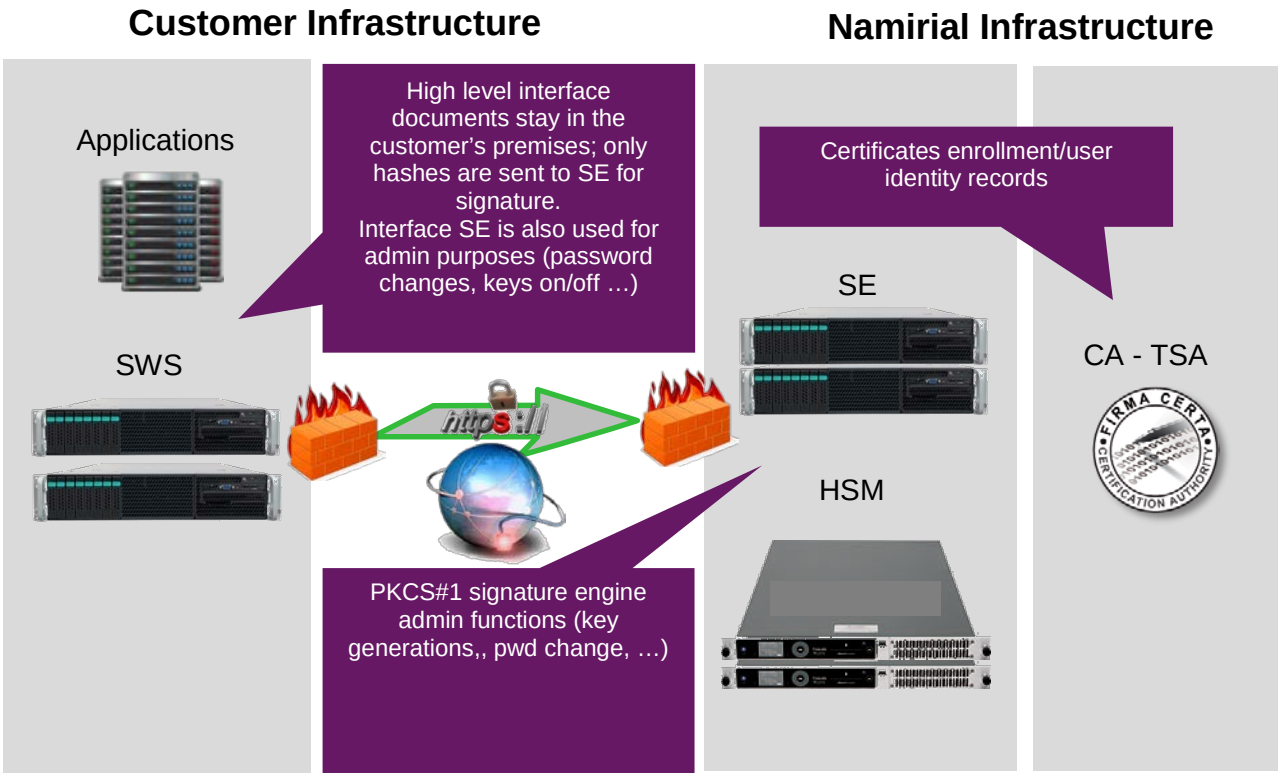
- Password (created by the holder),
- One-time password (OTP; sent to the OTP device of the holder such as his or her mobile phone), and
- Biometric characteristics (e.g. a biometric signature verified in real-time).

8.2.3 Usage

To execute a qualified remote signature on RES², the certificate holder must pass the required authentication on the remote certificate. Once passed, RES² can sign the received document hash using a PKCS#1 signature.

To execute this operation, RES² can either run in the Namirial data center and be consumed as an SaaS service, or be installed on customer premises, but under the control of Namirial when used for qualified e-signatures. As RES² just signs document hashes, the need to deploy the solution on customer premises is typically not very high. The PAdES/XAdES, CAdES compliant signature is finally created using the client application for RES², which typically is an on-customer-premises-deployed server application (e.g. SIGNificant, as shown in the figure below, making it a single platform for both advanced and qualified e-signatures). That means that the signed digital assets—such as PDF documents—always stay private to the customer.

This operation is schematically shown in the following diagram (RES² is shown in green).



Phone numbers used for OTPs, or biometric signatures used for biometric signature verification in real time do not need to be—and preferably are not—known by Namirial. The LRA who is providing application services must simply ensure that its systems guarantee that the holder has exclusive access for signature execution through an appropriate security system.

8.3 Namirial DTM Solution

The Namirial DTM solution binds all the pieces together to deliver an integrated platform to enable document-based transactions in all major use cases, including:

- Customers in the branch or shop,
- Customers directly in the field (mobile),
- External users who sign on their own device, and
- Internal users online in the office.

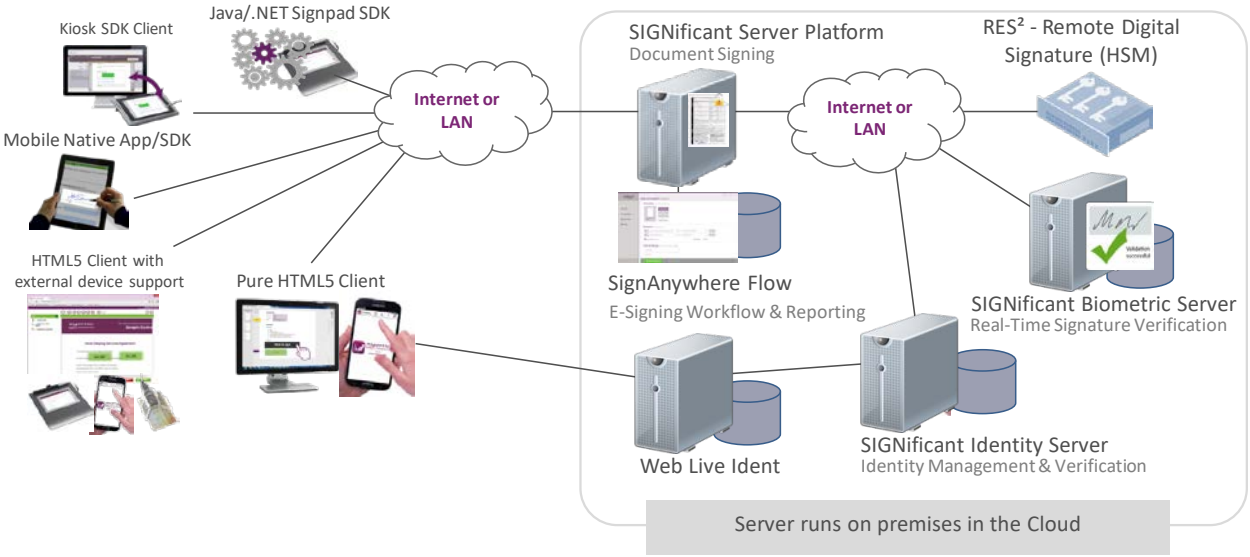
An overview about the solution's building blocks and how they are connected is provided in the figure below. As shown, the SIGNificant Server Platform (SSP), which typically runs on customer premises to keep documents fully private, takes the central role of digitally signing the PDF with a PAdES compliant digital signature on documents that a signatory views 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 just 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.

ViSi 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.



For more information, please visit https://www.xyzmo.com/.

9 References

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/CE.

[2] Commission document (Digital Single Market) —Questions and Answers on Trust Services under eIDAS.

[3] ETSI esignatures standards: http://www.e-signatures-standards.eu/.