Electronic Signature Guide

The Electronic Signature Guide covers topics regarding the configuration of digital signature types. It covers the perspective of the sender. For information about the perspective of the signer please see the Signer Guide.

eSignAnyWhere supports different kinds of signatures and these will not only affect how the signer signs the document, it also affects the legal aspect of the signature. We recommend that you verify with your legal consultant, which would be the best signature for your specific use case. Within the European Union a clear regulation is available under the eIDAS 910/2014 regulation. Nevertheless, there are still some national limitations affecting the electronic signature and its possibilities, therefore a validation is recommended.

Within the European Union you can categorize the signatures into two categories, defined by the EU regulation 910/2014 eIDAS (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) regulation:

- Advanced Electronic Signature (AES)
    - provides unique identifying information, that links to its signatory
    - signatory has sole control of the data used to create the electronic signature
    - must ensure that the signature is invalid after changes of the document (e.g. PAdES [PDF Advanced Electronic Signature] in PDF)
- Qualified Electronic Signature (QES)
    - is a signature, created via a qualified electronic signature device (e.g. SmartCard or Remote Certificate of a TSP)
    - equivalent to written legal form
    - no reputable by signatory
    - requires an identification of the signer, which can be executed by a LRA (Local Registration Authority) or its sales partners

It also defines the terminology for natural persons as "electronic signature" and for legal persons (e.g. companies) as electronic seal.

Signature Types in eSignAnyWhere

Signature type	AES	QES	Description
Click to Sign	depending on a second factor or use case	no	Is a simple signature, where the signer has to click on the signature to sign the field. In combination with an additional element (under sole control of the signer) it is a AES. We recommend to use the authentication (e.g. SMS-OTP) to ensure it. Please verify the use case to ensure that the authentication methods are under sole control of the signer.
Draw to Sign	depending on a second factor or use case	no	Is a simple signature, where the signer can record a signature (e.g. via mouse, finger) to sign the field in form of a picture (no biometric data). In combination with an additional element (under sole control of the signer) it is a AES. We recommend to use the authentication (e.g. SMS-OTP) to ensure it. Please verify the use case to ensure that the authentication methods are under sole control of the signer.
Type to Sign	depending on a second factor or use case	no	Is a simple signature, where the signer can type his signature, which is used as picture for the signature. In combination with an additional element (under sole control of the signer) it is a AES. We recommend to use the authentication (e.g. SMS-OTP) to ensure it. Please verify the use case to ensure that the authentication methods are under sole control of the signer.

Biometric Signature	Yes	No	The biometric signature records & (asymetrically) encrypts in real time the data points of the handwritten signature. The encrypted signature will be stored & bind to the PDF document to be validated. So the biometric data is the element under sole control of the signer, so no additonal authentication is required (except the use case requires it). Please note that the biometric signature is not recorded directly via Browser, it typically requires a specific hardware (Signature Pad, Tablet PC with Pen, Convertible with Pen) to ensure a high quality of the biometric signature, so it is mostly used for Point-Of-Sale use cases. Please contact your Namirial Sales Consultant for more information.
SMS-OTP Signature	Yes	No	The SMS-OTP (One-Time-Password) signature is similar to the Click to Sign signature, where the signer clicks on the signature field and confirms via SMS OTP (a numeric number sent to the signers phone) to sign the field. The phone is under sole control of the signer.
Local Certificate	Depending on Local Certificate	Depending on Local Certificate	This signature allows to access via the SIGNificant Device Driver (download is available via Signing Interface) local devices (e.g. Smart Cards, USB Token, Windows Cert Store). The signature level (AES, QES) depends on the used device.
Digital Remote Certificate	Yes	Depending on Certificate	This signature allows to access remote certificates (stored in a CA/TC) to sign the document. The credentials are under control of the signer. Depending on the certificate it is either an AES or QES.
Disposable Certificate	QES	QES	This signature uses a disposable certificate via the Namirial TSP. The disposable is a QES, which is only valid for a short time and allows a simpler usage for the signers (via confirming the T&C with Namirial TSP and the QES via SMS OTP or Namirial OTP App).
Custom Signature Types	Depending on the configuration of the custom signature	Depending on the configuration of the custom signature	On demand we can integrate for you custom signature types (customer TSP integrations, use case depending signature types).

All envelopes write a detailed audit trail (except if disabled), which is documenting the signing process and its actions and events (such as the authentication of the signer). The audit trail gets signed digitally by eSignAnyWhere.

Recommendation

eSignAnyWhere supports different kinds of signatures, most of them are designed for a specific use case to ensure a good user experience and acceptance.

In general you can define a

- Remote scenario, where the signer is using his own devices (e.g. Smartphone or PC)
- Point-of-Sale (PoS) scenario, where the signer can use the device available at the PoS

Remote Scenario

Remote scenario is using the signer's device for the signature, typically at home or at the office. Therefore, a recommended signature type is "**Click to Sign**", because it shows a good user experience and acceptance. In combination with a **SMS-OTP (one time password) for the authentication**, it is considered as an AES. Other authentication methods (PIN, OAuth2 or SAML) might also have a good user experience.

Alternatively, you can choose the SMS-OTP signature option. However, please be aware that it requires a SMS-OTP for each signature field, which may require extra effort from the signer when dealing with multiple signature fields (if batch signing is not activated, with the batch signing it is possible to sign multiple signature fields at once please see Batch Signing Dialog. It is important to note that SMS-OTP is an optional feature and not the default setting of eSignAnyWhere.

For a QES the best option is a disposable certificate, because the signer has to accept the Namirial TSP terms and conditions for the disposable certificate (personal certificate for the signer). The signing is performed by clicking on the signature field and confirming with SMS-OTP or Namirial OTP App.

Point-of-Sale (PoS)

The PoS scenario is typically used in combination with API integrations and extended use cases. At the point of sale there is typically a hardware for signing, such as a Signature Pad, Tablet (e.g. iPad) or a PC with touch screen and pen. In that case for AES a **biometric signature is a natural way of signing**. You also can use the signers devices by transforming it to a "remote" scenario and the signer uses his own device at the point of sale.

QES is supported via Disposable Certificate e.g. with the SIGNificant Kiosk in combination with a Signature Pad (e.g. the Namirial NT10011).

Evidence and Validation of Signed PDF/A Documents

The PDF document is a powerful document standard (ISO 32000) and **PAdES** (PDF Advanced Electronic Signature) ensures secure documents and signatures. The evidence is stored on the one hand directly in the PDF document and in a corresponding process documentation (audit trail).

Signed Document ⟷ Evidence directly saved in the document

Audit Trail ⟷ Evidence in form of the corresponding process documentation

If you open a signed PDF document with a PDF Reader (e.g. Adobe Reader), you can verify embedded data, such as:

- Digital certificates show the signatory or the document issuer
- protects document integrity and make changes visible
- display signing graph and document history
- trusted time-stamps (optional)
- geo-location (optional)
- information on the validity of the signature certificate on signing time (OCSP / CRL)
- EUTL – European Trust List for EIdAS for Trust Service Providers
- encrypted biometric signature data embedded in the document
- Adobe Reader – Adobe Approved Trusted List (AATL)

In addition to the evidence in the signed document a corresponding sealed process documentation (audit trail) is written:

- envelope with hashed of document
- send notifications and recipient addresses
- authentication (PIN, SMS-OTP, etc.)
- reader's IP addresses
- reader's location
- date & time of actions
- actions on the document/envelope: page open & view, confirmations, form field edits, signatures and many more

The following sample shows the structure of the audit trail xml:

```xml
<?xml version="1.0" encoding="utf-8"?>
<AuditTrail Version="1" CreationDate="2018-10-01T13:07:21.2795797Z">
  <EnvelopeId>[Envelope ID]</EnvelopeId>
  <EnvelopeName>[Envelope Name]</EnvelopeName>
  <EnvelopeStatus>[Envelope Status - possible values: Completed]</EnvelopeStatus> <!-- note: at the moment, the
Audit Trail is only generated for completed envelopes -->
  <EnvelopeCreationDate>[Create Date, e.g. 2018-10-01T13:05:10.927Z]</EnvelopeCreationDate>
  <EnvelopeSendDate>[Send Date, e.g. 2018-10-01T13:06:21.13Z]</EnvelopeSendDate>
  <EnvelopeExpirationDate>[Expiration Date, e.g. 2018-10-29T13:06:21.13Z]</EnvelopeExpirationDate>
  <Sender>
    <FirstName>[Sender First Name]</FirstName>
    <LastName>[Sender Last Name]</LastName>
    <EMail>[Sender E-Mail]</EMail>
  </Sender>
  <ElectronicDisclosures>
    <!-- list of "Disclosure" elements (see below) -->
  </ElectronicDisclosures>
  <Recipients>
    <!-- list of "Recipient" elements (see below) -->
  </Recipients>
  <Notifications>
    <!-- list of "Notification" elements (see below) -->
  </Notifications>
  <SendFinishedDocuments>[true|false]</SendFinishedDocuments>
  <PreventMailSending>[true|false]</PreventMailSending>
</AuditTrail>
```

Electronic Disclosures

```
<Disclosure Culture="[language ISO code, e.g. de, de-AT]">
  <Subject>[Message Subject]</Subject>
  <Text>[Message Body]</Text>
</Disclosure>
```

Recipients

General

```
<Recipient Id="[Recipient ID]" OrderIndex="[Recipient OrderIndex]" EMail="[Recipient E-Mail]" Deleted="
[true|false]">
  <FirstName>[Recipient FirstName]</FirstName>
  <SealingProfileName />
  <LastName>[Recipient LastName]</LastName>
  <Type>[Recipient Type, possible values see below]</Type>
  <FinishDate>[Finish Date, e.g. 2018-10-01T14:01:32.6354943Z]</FinishDate>
  <Status>[Recipient Status, possible values see below]</Status>
  <RejectReason>[Reject/Delegate reason]</RejectReason>
  <WorkstepId>[Workstep ID]</WorkstepId>
  <History>
    <!-- list of "Entry" elements (see below) - info about previous changes of this recipients -->
  </History>
  <AuthenticationMethods>
    <!-- list of "AuthenticationMethod" elements (see below) -->
  </AuthenticationMethods>
  <MailSubject>[Mail Message Subject]<MailSubject>
  <MailContent>[Mail Message Content]<MailContent>
  <DelegatorId>[OPTIONAL: Recipient ID of the delegator recipient]</DelegatorId>
  <DelegateeId>[OPTIONAL: Recipient ID of the delegatee recipient]</DelegateeId>
  <WorkStepInformation><!-- OPTIONAL: Workstep Information XML - details see below --></WorkStepInformation>
  <auditTrail><!-- OPTIONAL: Workstep Audit Trail XML - details see below --></auditTrail>
  <PreventMailSending>[true|false]</PreventMailSending>
</Recipient>
```

Values for Type:

- Signer
- CC
- Acknowledge
- Pkcs7Signer
- Automatic

Values for Status

- NotSigned
- Signed
- Rejected
- Delegated
- DelegatedAutomated

History

```
<Entry ValidFrom="[When was this recipient setting valid? e.g. 2018-10-01T14:00:41.54Z]" ValidTo="[When was
this recipient setting valid? e.g. 9999-12-31T23:59:59.9999999Z]">
  <FirstName>[FirstName]</FirstName>
  <LastName>[LastName]</LastName>
  <EMail>[E-Mail]</EMail>
  <Modifications>
    <!-- List of "Modification" elements -->
    <Modification>[Modification]</Modification>
  </Modifications>
</Entry>
```

Values for Modification:

- RenameEmail

- RenameRecipientName
- RestartEnvelope
- RenameRecipientFirstName
- RenameRecipientLastName
- RenameRecipientMessage
- ChangeAuthenticationSms
- ChangeAuthenticationLive
- ChangeAuthenticationPin
- AddedAuthenticationSms
- AddedAuthenticationLive
- AddedAuthenticationPin
- RemovedAuthenticationSms
- RemovedAuthenticationLive
- RemovedAuthenticationPin
- ChangeRecipientCulture
- ChangedRecipientDisposableCertificateData
- ChangedRecipientRemoteSignatureData
- ChangeAuthenticationOAuth
- AddedAuthenticationOAuth
- RemovedAuthenticationOAuth
- RecipientDeleted
- ChangeAuthenticationSaml
- AddedAuthenticationSaml
- RemovedAuthenticationSaml
- ChangedRecipientOtpSignatureData
- ChangedRecipientPkcs7SignerData
- ChangedRecipientSwissComCertificateData

Authentication

```
<AuthenticationMethod>[Authentication Method]</AuthenticationMethod>
```

Values for AuthenticationMethod:

- Pin
- Sms
- WindowsLive
- CustomOAuthProvider
- CustomSamlProvider

Notifications

```
<Notification Type="[Notification Type - possible values see below]" Added="[Added Date, e.g. 2018-10-01T14:01:
32.6354943Z]" Sent="[Added Date, e.g. 2018-10-01T14:01:32.6354943Z]" Recipient="[OPTIONAL - Recipient ID">
  <ExtraInformation />
</Notification>
```

Values for Type

- SendSignNotificationToRecipient
- SendAcknowledgeNotificationToRecipient
- RecipientChanged
- EnvelopeFinished
- SendCcDocs
- SendCcDocsWithDownloadLink
- SendCcDocsNoLink
- SendCcDocsNoLinkWithDownloadLink
- EnvelopeParallelSigned
- DelegationAutomatic
- DelegationManual
- SendSignNotificationToRecipientWithDelegation,
- AutomatedDelegationNotification

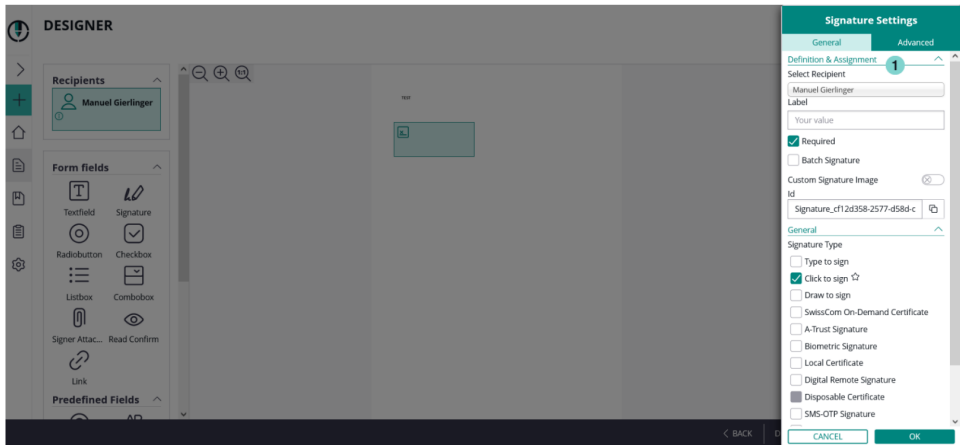# How to define the signature of the recipient (Saw-Viewer)

This tutorial guides you through the process of defining the signature of the recipient. First, the configuration of the definition and assignment has to be made. There you can select the recipient, write a label, select if the signature field is required and if batch signature is allowed.

Definition & Assignment configurations

Setting	Behavior
Recipient	Selection of which recipient has to sign the field
Label	The label of the signature field (displayed)
Required	Define if the recipient has to sign the signature field or if it is optional. If a signature field is required it is highlighted with a red border.
batch signing	If you use this, the recipient is allowed to sign more than one signature field at once. Therefore, you have to select a first signature field and select the "Batch Signature" option.

On the next figure you see where you can find the settings:

Figure	Description
	1. Settings of the field

After this configuration you can decide with which signature type the recipient should sign the envelope.
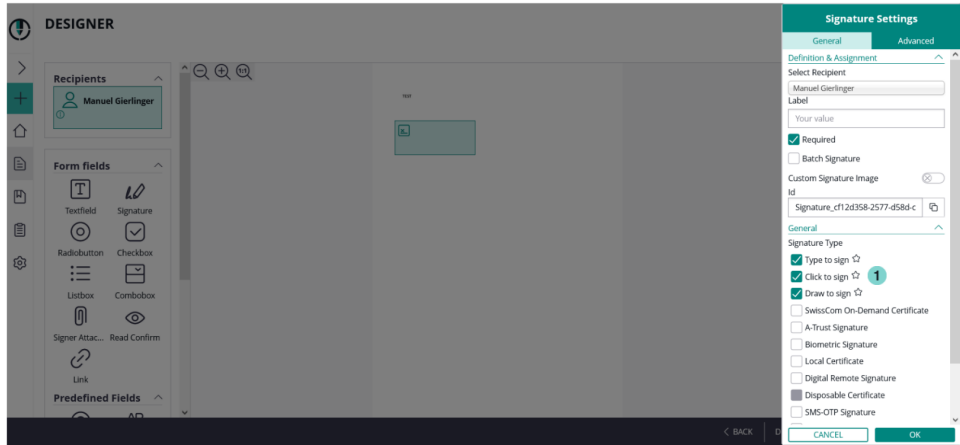
Signature types

You have to select at least one type. You can select more, if you want to give the recipient the option to choose a specific type. You can also define a preselect type (favorite, click on star-icon). Please note, that not all types are available for all customers.

HTML 5 signature types

Click2Sign, Draw2Sign, Type2Sign

For these three signature types you do not have to configure anything. Just place the signature field on the document, select one to more of these types and send the envelope.

Figure	Description
	1. Signature types

As you can see on the last figure, we selected all three signature types, therefore the recipient can choose between these types. With the star-icon on the right sight next to the types you can select the preferred signature types which will be highlighted for the recipient.
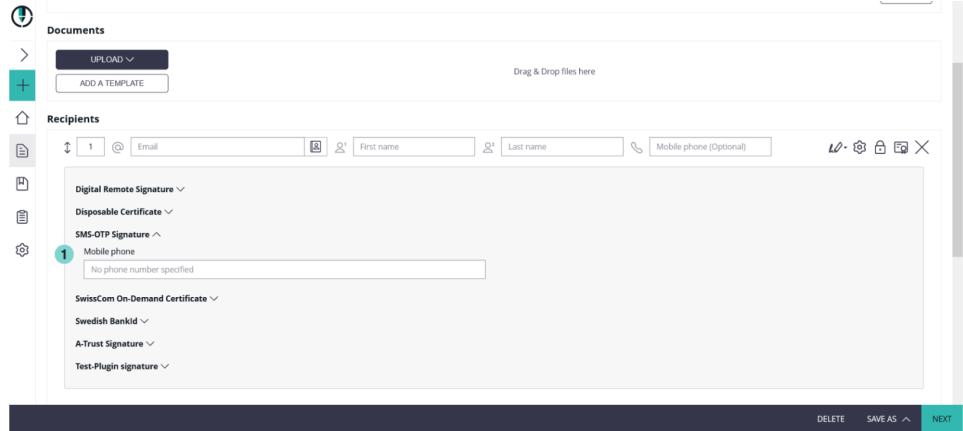
Biometric signature v 3.2

For the biometric signature you can decide between the following three options:

- withinField: the recorded signature must be within the signature field
- onPage: the recorded signature must be on page (can be written outside of the signature field)
- intersectsWithField: the recorded signature must be partly within the signature field (default)

SMS-OTP signature v 3.0

Generally there are two ways to set the phone number. You can either type the number in the SMS-OTP signature field or the recipient type in the number when he/she receives the envelope. First figure shows the first way (sender defines the number), the second one shows if the recipient defines the phone number.

Figure	Description
	1. Settings for SMS-OTP signature
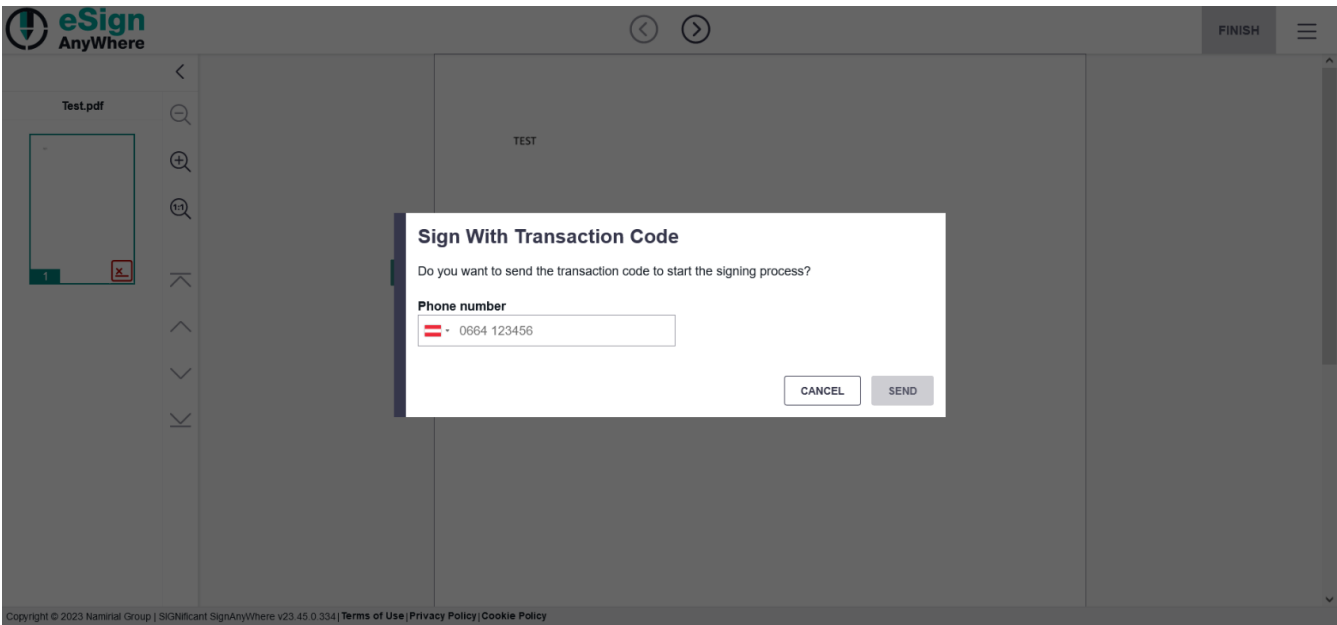
Note: If you place a signature field but you do not enter a phone number you will get a notification like it is shown in the next screenshot:
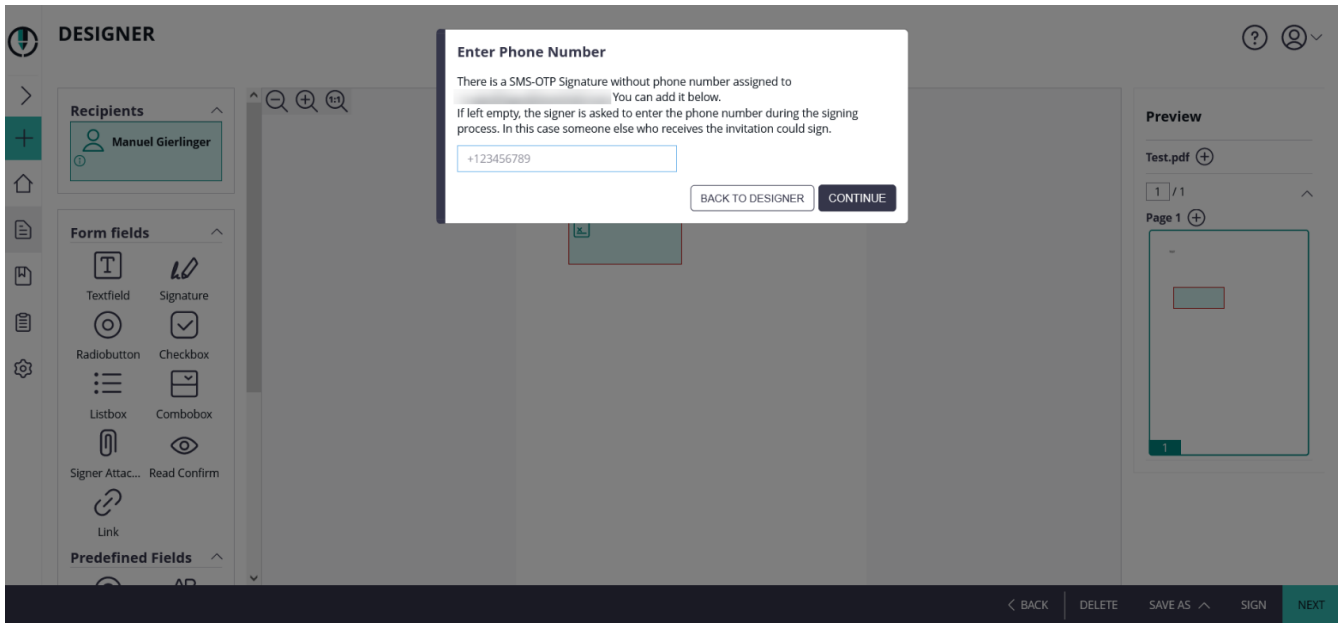
Local certificate, digital certificate v 3.6

With the local certificate the recipient can use a locally on his device installed certificate for signing. For the digital remote the recipient uses a remote certificate for signing.

For the local certificate you can find the settings here:

Figure	Description
	1. Settings for the local certificate

With those settings you can validate the recipient and certificate holder name and the certificate root CA verification with EUTL.

After you configured those settings you just have to select a local certificate. Next screenshot shows the selection:

Figure	Description

	1. Enable local certificate signature type
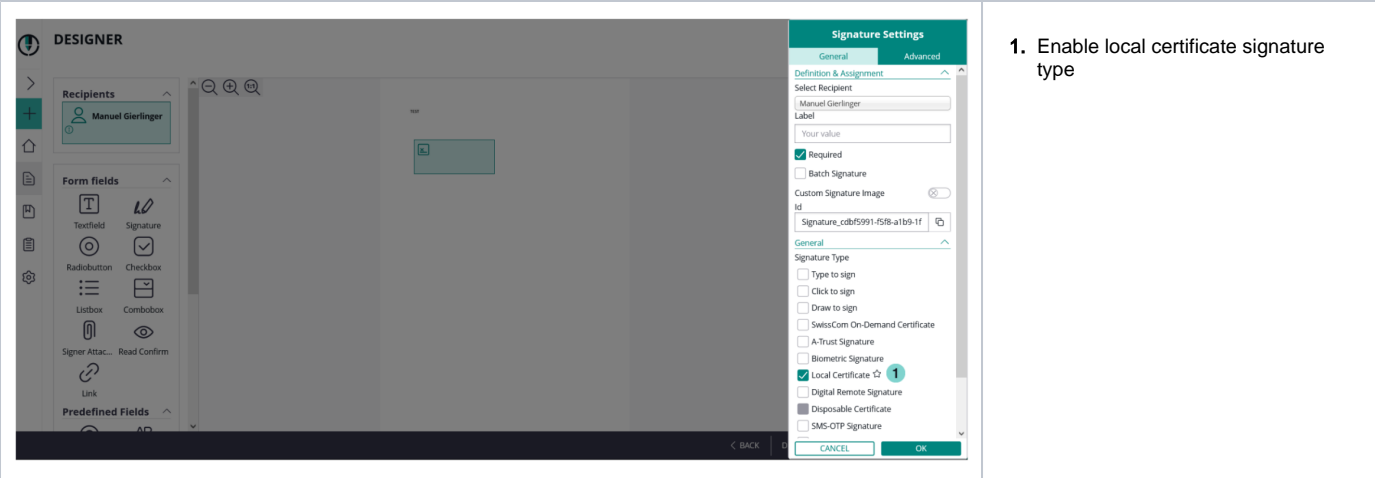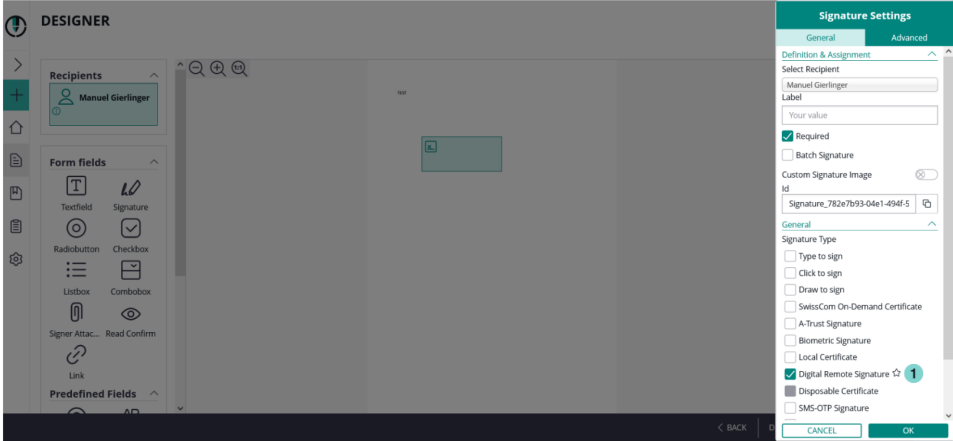
Digital remote certificate

If the user has a long lived certificate you can use the *Digital Remote Signature* option. It is similar to the disposable certificate, but you must not provide so much information, as the user is already registered. It is not required to define the User Id or Device Id, then the signer must enter the data himself.

Figure	Description
	1. Open Settings **2.** Settings for digital remote signature

In the designer you must select the **Digital Remote Signature** for the signature type.

Figure	Description
	1. Select digital remote signature

Figure	Description

1. Signature properties overview

Disposable certificate

Before you can send a disposable certificate you have to fill in some dates. First, in your organization settings and then if you send the envelope. The next figure shows you the configurations which has to be done before sending the envelope.

There are three checkboxes available:

- Use lean disposable (Has to be enabled, except there is a clear reason against it)
  Note: There are differences in the validation rules between "classic" disposable and "lean disposable".
- Show disclaimer before certificate request (to ensure that certificates are issued only with consent of the holder; but might be substituted with other process constraints which address the legal requirement)
- Send disposable disclaimer document emails (might be required in fulfillment of obligations of the LRA contract, unless other delivery methods ensure delivery of the certificate request form)

Figure	Description
	1. Settings for disposable certificate

To use the disposable certificate you just click the settings for the recipient to edit her/his information for the certificate. You need the following information:

- Document type
  - Identity card
  - Driver license
  - Passport
  - Residence permit
  - National electronic identity card
  - Temporary residence permit
  - Embassy/Consulate personnel document
- Document number
- Document issued on
- Document issued by
- Document expiry date
- Identification Issuing Country
- Identification type
  - Tax Code
  - National unique number
  - Passport
  - Identity card
  - Italian tax code
  - Driving license
  - Residence permit
  - Temporary residence permit
  - Embassy/Consulate personnel document
- Identification Number
- Mobile phone
- Country of residence

Figure	Description
	1. Settings for disposable certificate for the recipient

After you filled in the dates you can either validate the dates or reset the data. **v 3.6**

If you validate the dates and the recipient name does not match the holder name for the disposable certificate you will get a warning. The following screenshot shows you the warning:

If you click on the "compare" field the next window appears where you can update the name either to the holder name or to the recipient name:

In the designer you have to select the signature field type as "Disposable Certificate".
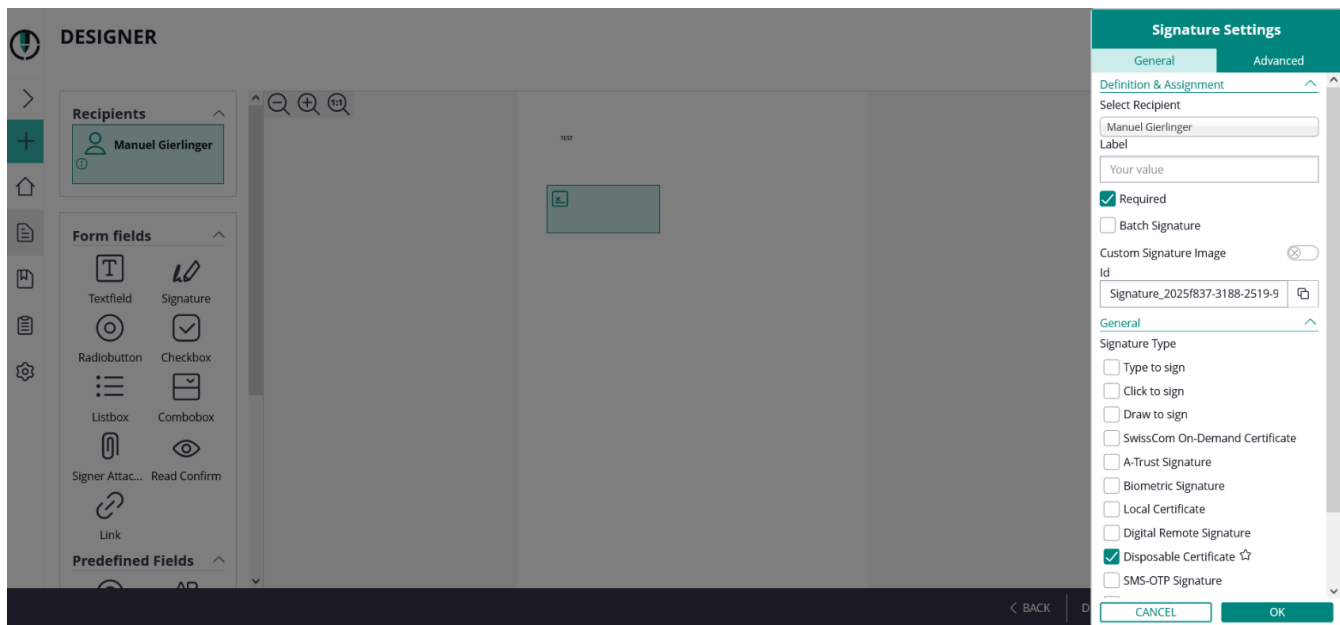
The signer will receive its email as usual and when the signer wants to sign a disposable certificate signature field he will get a one-time-password via SMS. The counter on the disposable certificate starts by signing the first signature.

If "Show disclaimer before certificate request" is enabled in Settings->Organization->Disposable Certificate the signer first receives the disclaimer before the SMS-OTP.

When the document is finished you can validate, for example, the qualified electronic signature in Adobe Reader.

You can also send a disposable signature via api. To do this, you first have to upload a document and then add the signature and the disposable certificate data. Note: You have to add the disposable certificate data in the section "recipient".

After these configurations you can send the envelope with a disposable certificate signature.

Automatic Remote Signatures v 3.2

ⓘ With eSignAnyWhere version 3.2 the automatic remote signatures (automatic remote eSeal) are integrated. So you can setup, as user manager, automatic remote signature profiles for automatic signature.

If you create a workflow, a new type "Add Automatic" recipient is available. The automatic remote signature / eSealing is applied automatically to the document, if it is the automatic recipient turn. The workflow continues automatically with the next recipient after the automatic recipient.

- Automatic Remote Signatures / eSealing are an optional eSignAnyWhere feature
- User Managers can configure the automatic remote signature / eSealing profiles in the Organization settings page, when they have enabled the user option "Allow Automatic eSealing"
- Power use can use the automatic remote signature / eSealing profiles, if they have the user option "Allow Automatic eSealing" enabled

1) Automatic Remote Signature Profiles

The profiles for automatic remote signatures are managed via the organization's settings page (so only by user managers). For creating an automatic remote signature profile you need a description (e.g. name), the username and the password.

Attention: if a power user wants to use the automatic remote signatures, the user must have enabled the user right "*Allow automatic eSealing*" (see "Settings" > "Users").

2) User Settings

User must have enabled the option "Allow automatic eSealing" to use the automatic remote signatures / eSealing within a workflow.

Figure	Description

	1. Enable automatic eSealing for the user

3) Creating a workflow with automatic remote signatures

In the eSAW UI you can add an automatic signer / eSealing via button in the recipient list "Add Automatic". Then the profile must be selected for the automatic signature / eSealing. **Attention**: the power user must have the right "*Allow automatic eSealing*" enabled (see "Settings" > "Users").

Figure	Description
	1. Add automatic

Generic Signing Plugin v 20.42

Note: This feature is not available with basic subscription, so please contact your Namirial sales.

After the configuration of the generic signing plugin in the organization settings you can now use the signature in the envelope. First configure the setting for the recipient. Please see the next figure.

Figure	Description

	1. Configuration of the signing plugin

After the configuration you can select the signature plugin as a signature type in the designer. Please see the next figure:

Figure	Description
	1. Selected signature plugin

Glossary

AATL	Adobe Approved Trust-List
Biometric Signature	A recording of x/y coordinates, pressure and time of a handwritten signature.
CA	Certificate Authority
CRL	Certificate Revoke List
Digital Signature	An electronic signature based on asymmetric cryptographic algorithms.
Electronic Signature	An electronic signature can be from a simple level (SES) to a very high level of signature (QES).
EUTL	European Union Trust-List
PDF	Portable Document Format
PKCS	Public Key Cryptography Standards, e.g. PKCS#7 a high level signature format.
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
QES	Qualified Electronic Signature
OTP	One Time Password

TSP	Trust Service Provider
QTSP	Qualified Trust Service Provider

The information provided on this page is continually revised and adapted to changes in legislation or case law, technology. Hints for clarification, updating and supplementing are always welcome via e-mail. The information on this page does not constitute legal advice. In particular, they can not replace any individual legal advice that takes into account the specifics of the individual case.