



e-Sign documents in your own desktop applications



Using the SIGNificant SDK, you can easily embed a wide range of signature pads to biometrically sign and digitally seal electronic documents in your own custom applications. Simply use a common interface to capture the biometrical data of handwritten signatures with devices from many different manufacturers, enabling you to switch to new available pads from alternative vendors with minimal effort, decoupling you from new developments in the fast changing

hardware market. Edit and prepare PDF documents for e-signing and then sign them according to common standards, enabling reading signed documents with any ISO-compliant PDF reader.

Finally, you may pair the SIGNificant SDK with SIGNificant Server to enable a server-side integration scenario or with SIGNificant Biometric Server to allow for real-time authentication of the captured handwritten signature.

Signature Capturing



Device independence

Use the complete range of signature capturing devices from various manufacturers that xyzmo supports to capture the biometrical data of handwritten signatures.

If necessary, simply switch to new available pads from alternative vendors with minimal effort, decoupling you from new developments on the fast-changing hardware market.



Forensically identifiable handwritten signatures

A handwritten signature captured with SIGNificant is much more than just an electronic image of a digitized signature embedded in a PDF. We record – forensically, identifiably – the handwritten signature of a person using all available parameters, such as acceleration, speed, and pressure. These parameters are unique to every individual and by no means can easily be reproduced by a forger.

An expert tool is available to forensically analyze the biometric characteristics of the captured signature.



Manage your signature pad

- Automatically detect a connected signature pad (plug 'n play).
- Check and initialize communication with your device.
- Show images and buttons on LCD tablets, enabling the tablet to become a fully interactive device.
- Capture the handwritten signature with all its biometrical data.
- Obtain a static image from the signature.



Real-time preview of your signature

Display a real-time preview of the signature to be displayed in your application so that the user can directly watch the signing of the document in real time on the PC screen.



Multi-tablet support

Access a specific tablet when multiple tablets (even of the same model) are connected to the same PC.



Ready for real-time authentication

Use the captured signature to authenticate a signatory in real-time against his or her enrolled biometric signature profile.

PDF Document Processing



Define signature fields

Search for any text markers to automatically define the position at which to put a signature into the PDF document. You also have the option to remove the text marker and turn it into an Adobe signature field.



Open-standard compliant e-signing

Digitally sign a document with a local certificate in accordance with the standard defined in Adobe PDF Reference PDF 32000-1:2008 12.8.3.3 PKCS#7 Signatures (as used in ISO 32000). The used certificate chain of the digital signing process may even be embedded.

The biometric signature data is saved asymmetrically encrypted in the "V"-Dictionary of the signature field and can be exported according to the ISO/IEC 19794-7:2007 standard for biometric signature exchange.











Document binding

When a signature, including all the biometric parameters, is captured locally on the device, it is safely embedded using an asynchronous public key encryption into and uniquely bound to the target PDF document. Copy/paste attacks can thus be easily detected.



Fully secured document

Once a signature, including all the biometric parameters, has been embedded into a document, it is turned into a signed and sealed PDF. You can verify the integrity of your PDF and also extract the used signing certificates for further analysis.

	<p>Biometric signature extraction</p> <p>The biometric signature data of a recorded handwritten signature contained in a document can be extracted and decrypted, e.g. to render the signature image or to extract the location data of the signature. Of course, this requires the appropriate private key.</p>
	<p>Time stamping</p> <p>Digitally time stamp documents using the RFC 3161 timestamp protocol from a trusted timestamp provider.</p>
	<p>Full PDF and PDF/A compatibility</p> <p>The document is Adobe Acrobat compatible, so it can be viewed by any standard PDF viewer. PDF documents are sealed with a digital signature compliant with the ISO standards for PDF and PDF/A. Thus, the validity of the digital signature can be validated with Adobe Reader and many other PDF viewers.</p>
	<p>PDF to image</p> <p>Enable your own custom application to display PDF documents through querying information about the PDF file (number of pages, page size, etc.) and through converting PDF pages to images.</p>
	<p>Add attachments</p> <p>Add any file to the document to be signed as either a new page or a separate file attachment, enabling you to preserve its integrity once you have signed the entire document.</p>
	<p>Annotations</p> <p>Add annotations either as text or as freehand graph anywhere on a PDF document, which is useful for typing on a non-fillable form or outside the fillable areas of a form.</p>
	<p>Fill out and sign PDF forms</p> <p>Complete your PDF AcroForms and static XFA Forms with user input data and allow automated forms data extraction.</p>
	<p>PDF flattening</p> <p>This option permits you to remove any layers (annotations, digital signatures, etc.) that aren't visible by some PDF viewers (e.g. on the iPad or iPhone) and consolidate them into one layer, which is supported by all PDF viewers.</p>

Supported environments:

- Java
- .NET/C#
- COM/C++

Note: Not all features are available upfront in all SDKs.