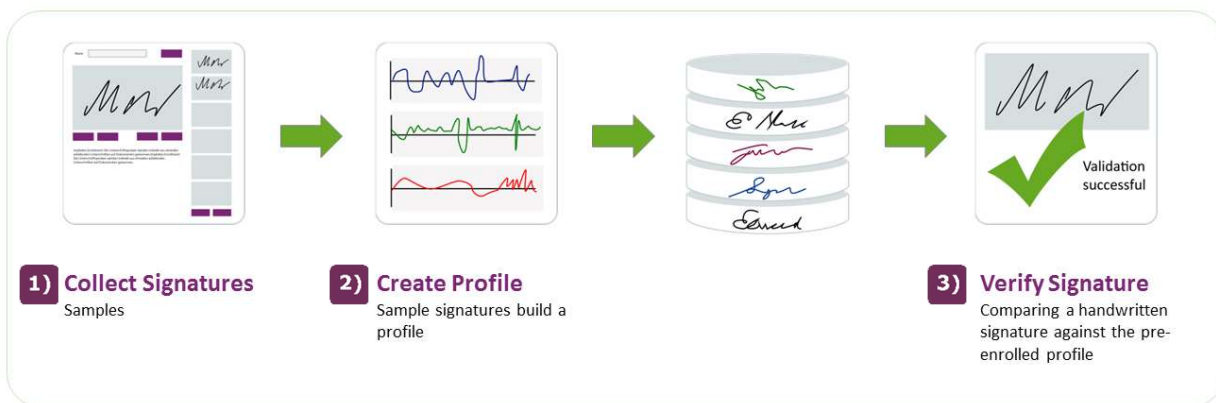




Signature Verification / Signature Authentication

The SIGNificant Suite helps introduce companies to the era of personal electronic signing. The SIGNificant products record the handwritten signature of a person (including measurements of parameters of pressure, acceleration, speed, rhythm, and movements in the air) and embed the signature into an electronic document.

The SIGNificant Signature Verification called SIGNificant Biometric Server takes this ability one step further, enabling real-time biometric verification of a signature to the SIGNificant platform by comparison of the recorded parameters of the handwritten signatures against the pre-enrolled profile. The possibility of a detailed protocol for each signature-relevant action makes it a total solution; documents are only processed if their signers are authenticated and companies can prove who signed which document and when.



How It Works? - Three Easy Steps

1)

Enrollment (Collect Sample Signatures) - The process is initiated by the user's enrollment. The enrollment process requires up to six initial signatures or can be done continually over time. These are collected using a signature pad or a tablet; the user simply signs his personal handwritten signature, exactly as he or she would with a wet-ink pen and ordinary paper.

2)

Signature Profile Creation and Handling - The signatures are stored in profiles. The system can handle numerous profiles per user, allowing, for instance, for one profile for a standard signature and another for signing with initials only. When verifying a signature, the SIGNificant Biometric Server compares the signatures to the relevant profiles.

3)

Signature Verification and Learning - Each time a user accesses the system to verify his signature, the Biometric Server compares the current signature to the signature profiles. With each authentication, the server continues to learn and fine-tune the user's profile. This enables the system to track gradual shifts in the handwritten signature over time.

Security Configuration

The SIGNificant Biometric Engine has three basic security modes that define how complex a personal profile has to be, and how strictly the Biometric Engine should verify the signature. The higher the security, the more likely it is that some customers will have to sign more than once before their signature is accepted. Thus the enrollment process can become stricter, with a tailorable choice of settings and thresholds per business application potentially requiring less or more than the 4–6 signatures needed for a standard enrollment.



Basic – This setting is intended for scenarios where you expect large numbers of customers per day, and where you want to avoid having some users sign multiple times because of false rejections (FR), but still achieve reasonable security in the verification of signatures. Typically, this scenario suits processes where you want to enhance security or where you want to replace the signature comparison presently done by a human. In this case, these settings are a perfect fit for increasing the security dramatically whilst still having very high customer acceptance.



Advanced – This setting is intended for scenarios where you expect large numbers of customers and skillful fraud attempts. Typically, this scenario suits processes where the signature has an important business impact (e.g. withdrawal of cash, signing important contracts etc.). Because of the importance of the signatures, you are willing to accept that some customers will have to sign more than once before the document is processed, to achieve better security against fraud.



High – This setting is intended for scenarios where you expect very high security with medium to small numbers of customers. The security parameters allow for a near-zero percentage False Acceptance Rate; therefore this is suitable for even the most critical environments.

Key Features






Clear, Fast Verification Results - The verification is performed in a transparent manner. The server compares the signature to the updated personal profile in the database and enables or rejects the entry within milliseconds.



Automatic Detection of Variations - The server automatically detects variations between signatures to make the personal profile as secure as possible. While some users sign in a very consistent way, others display a greater variance between signatures; the system recognizes and records this variance to calibrate the profile for future authentications.



Versatile Threshold Factor - The authentication process is flexible, enabling a varying authentication process for different environments, allowing organizations to easily adjust the balance between customer acceptance and security.

	<p>Constant Profile Enriching - A dynamic mechanism recognizes the fluctuation rate in each of the signature parameters in real time, thus nourishing the authentication engine with added parameters and enhancing the profile every time a signature is authenticated.</p>
	<p>Audit Trail – A detailed protocol of users’ security-relevant actions (enrollment, signature verification, suspension of signature profiles) is recorded.</p>
<p>ISO</p>	<p>Fully support of the ISO/IEC 19794-7 Biometric data interchange format standard</p>
	<p>Signatures are the only biometrics that vary over time - Every biometric system, such as iris scan, fingerprints etc., may be hacked. Once hacked, the information may be used again and again because eyes, fingerprints etc. do not change (they are static). By contrast, a signature, even if hacked, is not reusable with SIGNificant Biometric Server since no-one can ever sign the same signature in exactly the same manner twice; an exact match would be rejected. Also, the user can always change their signature and create a new personal profile.</p>

What results can be expected from online signature verification?

All electronic signature verification solutions participating in the 2011 IDCAR conference (International Conference on Document Analysis and Recognition) were evaluated by forensic experts using different testing sets. The task was to determine whether a particular signature had been written by the author of the reference signatures or if it had been forged by another writer. In each test, twelve known reference signatures were presented to the systems.

IDCAR evaluated the systems according to several measurements. They generated ROC-curves to see at which point an equal error rate was reached: i.e. the point where the false acceptance rate (forged signature being accepted as genuine) equals the false rejection rate (genuine signature being rejected). At this specific point they also measured the accuracy, i.e. the percentage of correct decisions with respect to all queried signatures. The winner was the xyzmo solution, with an accuracy of 96.27%, a false acceptance rate (FAR) of 3.70% and a false rejection rate (FRR) of 3.76%. In comparison, the second best system had false acceptance and false rejection rates above 7%! The rest of the dozen-plus systems tested thus had much inferior results! And, xyzmo settings can be set higher still.

xyzmo compared to other signature verification solutions?

The major advantage over other solutions on the market today is that our technology is able to compare a signature against a profile which is self-learning over time. Only this approach guarantees appropriate results for signature verification and authentication, respectively, because it is human nature never to sign twice in exactly the same way, and also to alter the signature constantly over a life-time.

A comparison with only one sample signature is mathematically much easier to handle, and thus some companies offer essentially inaccurate solutions. These “low level” solutions merely pick one random signature as a basis for the comparison. This approach only works for people who always sign in exactly the same way. Most human beings do

not behave like that, and thus this approach is simply not feasible for a broader usage of that technology. Test this by asking 10 random people to sign 6 times in a row in order to see how different most of these signatures are.

A more sophisticated but still not satisfactory approach is to build a solution which takes several signatures – a profile – into consideration at the time of real-time comparison, but still using a static profile which is not self-learning. This will deliver, at the start, better results than a comparison with just one signature, but the comparison will get less and less accurate over time. This will happen for nearly 100% of human subjects.

To summarize: only the xyzmo SIGNificant dynamic approach – based on self-learning profiles – really works in the long run with sufficient accuracy. The SIGNificant Biometric Server takes the ability of self-learning profiles one step further, by using a sophisticated algorithm when building a signature profile, initially by recognizing if such a profile is of sufficient quality or not. In particular, when people sign for the first time on a signature pad they change their signing behavior a little bit, and adjust it after they get used to this new technology, or find a new way of signing on a signature tablet, until it becomes the “usual” way. Thus it is business-critical to take more than 2 or 3 samples for each profile and to check by intelligent algorithms if these profiles are a robust base for the later verification. It is much better to reject improper signatures out of this profile creation stage and ask a customer to sign one additional time, instead of generating a wrong profile and “try” to use this for later comparison.

About xyzmo SIGNificant

xyzmo’s enterprise e-signature platform allows contracts, agreements, NDAs, forms, or any document that requires a signature, to be signed electronically on signature pads, payment terminals, the iPad, Android devices, with digital certificates or online via ‘click-to-sign’. It could not be easier or more secure. xyzmo is a private company based in Ansfelden, Austria with international offices in the United States and Romania. xyzmo and its predecessors have a combined history of more than 10 years of digital signature expertise. Our solutions have processed millions of electronic signatures to-date around the globe including for organizations such as:



About icon^{uk}

icon^{uk} brings best-of-breed Customer Communications Management solutions to the UK, combining some of the leading document management products, services and best practices available globally. Together they cover Electronic Signature and Enterprise Document Creation, Content Integration and Output Management. These solutions are ideal for any UK based enterprise, or public sector organisation, whose business processes rely on a high proportion of document exchange with Customers, Suppliers and Partners.

SIGNificant Signature Solutions and xyzmo technologies are distributed in the UK by Icon^{uk} and our selected Value Add Resellers. This suite is the most cost-effective and flexible software available in this market - and when implemented by our ‘business-first’ consultants produces outstanding ROI, risk management and customer engagement.

Consistently deliver great documents and reduce paper. Contact us to find out more.