Signature Verification: Why xyzmo offers the leading solution

Dynamic (Biometric) Signature Verification

The signature is the last remnant of the hand-written document in a digital world, and is considered an acceptable and trustworthy means of authenticating all written documents and business approvals. Dynamic Signature Verification is the most natural solution to the problem of authenticating documents digitally. Because the personal signature has always been strongly ingrained in our social, legal and commercial lives, Dynamic (or Biometric) Signature Verification applies this universally accepted authentication method to the electronic age. With Dynamic Signature Verification, we can now interact more quickly, freely and effectively than ever before. It's as easy as signing on the dotted line.

What is Dynamic Signature Verification?

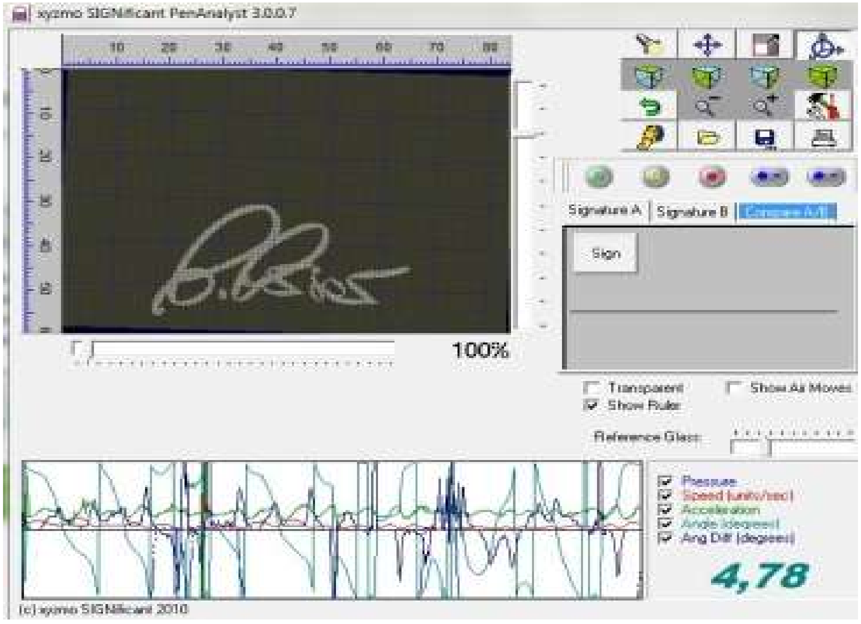
Belonging to the biometric family of products, Dynamic Signature Verification authenticates the identity of individuals by measuring their handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration and pressure. Unlike "electronic signature" captures that are often used today, Dynamic Signature Verification does not treat the signature as a graphic image. With graphic images, such as the scanned-in signatures we may often attach to our documents, it is not possible to detect the dynamics within each individual's signature and hence the signatures can easily be copied.

By contrast, Dynamic Signature Verification measures exactly how the signature is signed.

Dynamic Signature Verification has two huge advantages:

1. **Social Acceptance:** As soon as we learn how to write, we learn how to sign our names. It is second nature to us. The signature is a personal identification mark for verifying identity and authorizing transactions throughout the world. Its significance as an act of affirmation or commitment is well understood and accepted.
2. **Dynamic profile evolution:** No person ever signs their name in exactly the same way twice. Because Dynamic Signature Verification can track each person's natural fluctuations over time, it can easily determine forgery and better accept genuine signatures.

The biometric engine included in the SIGNificant Biometric Server is called the SIGNificant Biometric Engine. The basic idea behind the SIGNificant Biometric Engine is the transformation of natural hand fluctuations into a mathematical structure called a Personal Profile. This transformation is one-way only, hence the hand (pen) movements can be transformed into a personal profile but the reverse operation is virtually impossible. Pen movements are measured in up to five ways (horizontal and vertical, movement, pressure, angle, tilt).



☐ Transparent
☑ Show Ruler
☐ Show Air Moves

☑ Pressure
☑ Speed (units/sec)
☑ Acceleration
☑ Angle (degrees)
☑ Ang Diff (degrees)

The personal profile has two important characteristics:

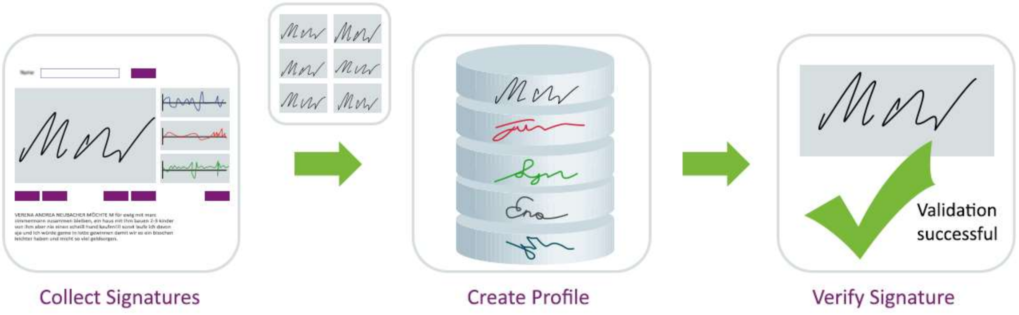
1. It is very stable (and comparable)
2. It occupies just a few hundred bytes, regardless of the signature size and complexity.

The personal profile is updated each time the user signs, and the profile's record of the signature is highly flexible. As time passes, each person's signature tends to change, and the SIGNificant Biometric Engine is able to adjust the personal profile to adapt to these changes continuously.

SIGNificant Biometric Engine was developed in a way that makes it more robust, relative to other biometrics (such as fingerprints, iris scan, etc.), because of the unique characteristics of a signature: signatures are the only biometrics that vary over time. The assumption is that 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 since no-one can ever sign the same signature twice in exactly the same manner; signatures are bound to be slightly different from one another. So an exact match is automatically caught. Also, the user can always change signature and create a new personal profile.

SIGNificant Biometric Engine does not use a universal test for everyone. Since some people sign in a very consistent (stable) way, their signatures will be almost alike. Other people sign with much greater differentiation between their signatures. SIGNificant Biometric Engine automatically detects these variations and builds as strong a personal profile as possible without producing False Rejection errors.



The Enrollment of the Personal Profile

The personal signature, by its nature, is a uniquely identifiable trait because it is unique in its variations. The subtle variations that occur each time an individual signs are unique to that individual. The natural variation is instinctual and reflects the individual's propensity to fluctuation, so that two signatures by one person can never be the same. By accumulating a series of signatures for an individual, a very accurate personal profile for authentication can be created over time. The enrollment of the personal profile is an important aspect of the security of the system. The quality of the profile greatly influences the results of the verification. The goal is to avoid inconsistent profiles and too "simple" signatures.

The typical enrollment process asks the user for 4–6 signatures. If one or more signatures are not consistent with the others, or they are too simple according to the configured security settings, the user is asked for more signatures to complete his/her profile. The enrollment process can also be done "continuously" over time. This means that you can collect the signatures from your signature processes and the Biometric Engine builds a profile over time. As soon as the profile has a defined number of consistent signatures, you can start using the profile for verification.

The Threshold Factor

The SIGNificant Biometric Engine has a threshold factor that makes the authentication process more "strict" for specific applications. In many environments, the chance that the forger will imitate the true signature without knowing what it looks like is very low. Therefore, the threshold and the various security settings may be set lower to achieve high customer satisfaction. However, in a closed environment where each person knows what others' signatures look like, the forger may have a better chance of imitating other persons' signatures, and the SIGNificant Biometric Engine threshold has to be set to a higher level.

The Security Settings

Besides the adjustment of the threshold factor, 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.

1. **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, 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.

2. **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.

3. **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.

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 becomes stricter, requiring more users to provide more than the 4–6 signatures needed for a standard enrollment.

Performance Measurements

When deciding on the optimum security settings and thresholds per application and use type, consideration may be given to false acceptances and false rejections in a similar manner to such considerations for any other technology of paper based process. Some metrics to examine are:

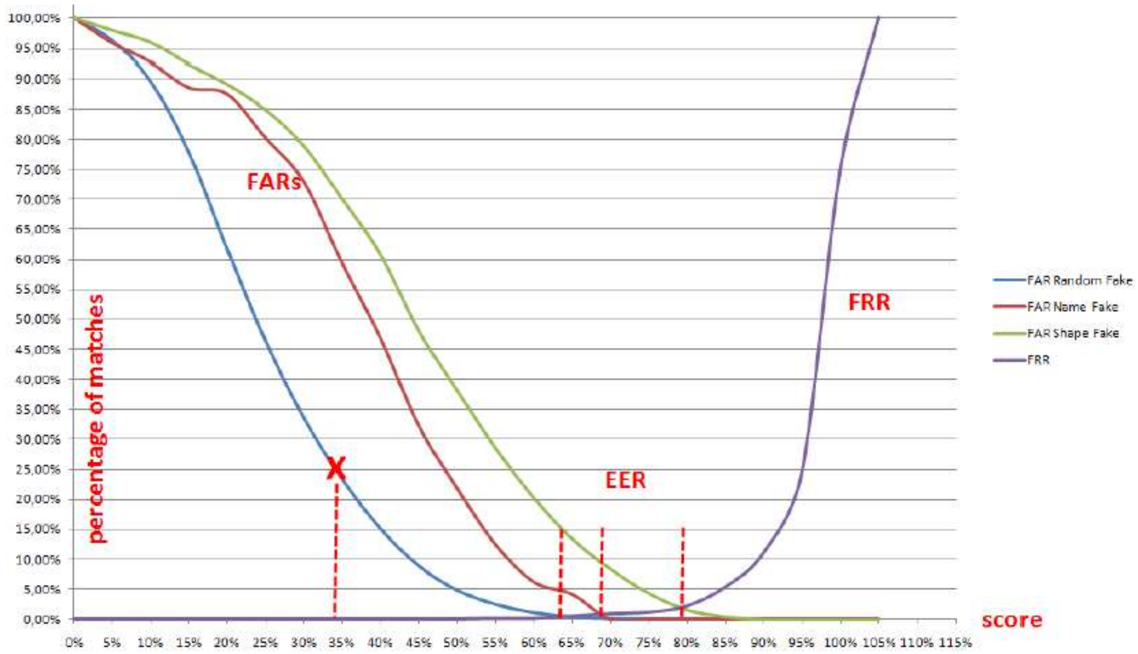
- **FRR** is defined as the rate or number of False Rejections ("embarrassing the real person").
- **FAR** is defined as the number of False Acceptances ("faking the person's signature").
- The point where these two graphs meet is called the Equal Error Rate point (**EER**). ERR marks the point where the same results occurs for FAR and FRR.

What results can be expected?

We distinguish between three types of fraud and apply these different FARs in the analysis:

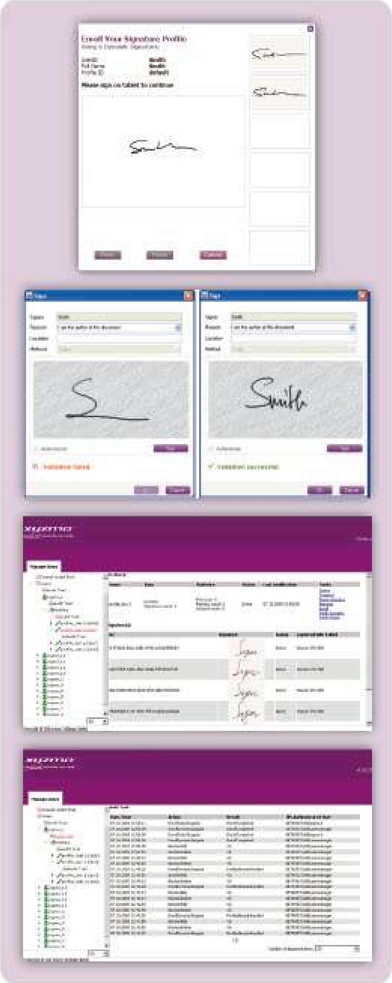
1. **Random fraud**: The forger does not have any idea of how the signatory signs. The EER for such fraud is **less than 0.01% in the basic security mode**. The FRR is also extremely low.
2. **Name fraud**: The forger knows the real signatory's name. The EER can vary depending on the type of signature, because complex signatures are very hard to imitate dynamically while simple signatures are easier. The EER for such fraud is typically **less than 0.5% in the basic security mode**.
3. **Shape fraud:** The forger knows what the signature looks like (e.g. from viewing it in print). The EER for such fraud is **less than 2.5% in the basic security mode** of the Biometric Engine and **less than 0.5% in the advanced security mode**. In the **high security mode, it is less than 0.01%.**

These are illustrated by the 3 different EER (FAR-FAR intersections) points below:



The Features

The SIGNificant Biometric Server is an extremely reliable product due to the following factors:



Enroll Your Signature Profile

Please sign on tablet to continue

- **Dynamic Signature Verification** – The system utilizes distinctive aspects of the handwritten signature, such as rhythm, speed, pressure, acceleration and movement, by measuring the physical activity of signing.

- **High-Security Concept** – The system provides secure storage and communication of captured biometric signatures.

- **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 varying authentication procedures for different environments, allowing organizations to easily adjust the balance between customer acceptance and security.

- **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 accepts or rejects the entry within milliseconds.

- **Constant Profile Enriching** – A dynamic mechanism recognizes the fluctuation rate in each of the signature parameters in real time, thus enriching the authentication engine with additional parameters and enhancing the profile every time a signature is authenticated.

- **Independent of Signature Pads** – SIGNificant is a device-independent solution, meaning that it enables the use of a broad range of signature-capturing devices from various manufacturers. As some companies require basic signature pads, while others require more advanced devices, a signature pad-independent solution offers the necessary flexibility and leads to improved satisfaction rates due to the fact that each customer, integrating this solution, can choose the signature pad that best fits their needs.

- **Audit Trail** – A detailed record of users' security-related actions (enrollment, signature verification, suspension of signature profiles) is logged.

xyzmo SIGNificant and Other Signature Verification Solutions

Development History

Since the end of the 1990s WonderNet has been the market leader in personal digital signature capturing and identification based on electronic biometric signature data. Together with Prof. Michael Werman and Dr. Yoram Singer from the Hebrew University in Jerusalem, WonderNet investigated the nature of the human signature and developed mathematical methods to compare such electronic biometric signatures against pre-enrolled signature profiles. Bank Hapoalim, Israel's largest bank and financial group, and WACOM Co. Ltd. Japan, were both investors in WonderNet at that time.

Early adopters helped to improve this technology:

- The Israeli Air force uses this technology; for example, to check signatures on airplane maintenance protocols.
- Ono Academic College (OAC), a leading Israeli institution of higher education, facilitates contract signing with SIGNificant. Lecturer recruiting became easy to manage administratively, with controlled budget approvals which are biometrically authenticated in real-time, in order to secure the process.
- Sao Paulo's Electric Energy Company, using this technology, signs and verifies more than 250,000 signatures annually, the equivalent of 26 full days of signing by old manual methods.
- …and many more, including Bank Hapoalim as mentioned above.

xyzmo offers the world's most complete, open and accurate real-time signature verification.

On February 14, 2008 xyzmo shareholders bought the entire IP rights of WonderNet Ltd. (Penflow) including the most prominent technology for electronic biometric signature authentication. By incorporating this technology from WonderNet with its own, xyzmo SIGNificant Group became a major international company in its field, with offices in Austria, the US and Germany, and represented by many Value-Added Resellers worldwide.

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.

Alternatives may be viewed in two approach types:

- 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. Anyone can easily prove this by asking 10 random people to sign 6 times in a row, on a blank sheet of paper, 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 approach – based on self-learning dynamic 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, on top of that, 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 a profile at this stage, namely, at the time of creating such a profile, and ask a customer to sign one additional time, instead of generating a wrong profile and "try" to use this for later comparison. This dynamic signature verification technology has won recent global competitions for electronic signatures, with accuracy and security aspects scoring highest of any vendor.

The area of electronic biometric signature verification/authentication on a large scale has just started with such high-quality standards as xyzmo introduces to the market. There are, meanwhile, early adopters in Europe like Maquet Getinge Group (a leading global medical technology company http://www.maquet.com/) who use SIGNificant for checking signatures on quality assurance documents, and innovative banks like Tatra Banka (http://www.tatrabanka.sk/) which authenticate all their customers in real-time based on their handwritten electronic biometric signature with our advanced and superior technology. This will become a huge market over the next few years as the ROI case to replace wet ink on paper signing is undeniable for most organisations, and xyzmo sees itself clearly in the leading position far ahead of the competition with the best and most advanced solution available. Self-Learning dynamic profiles will be the key!

Now UK clients can benefit from xyzmo through 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, Document Creation, Content Integration and Output Management.

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. Contact Icon^UK (http://www.icon-uk.net) or xyzmo (http://www.xyzmo.com/) to find out more.