NamirialGmbh
Digital Transaction Management

Biometric Signature Verification in Real-Time

Secure transactions through authentication signers with their handwritten signature

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

Abstract

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

This whitepaper will help you to understand what biometric signature verification is, and what advantages it offers. Furthermore it is explained how the performance measurement works, including enrolling of the personal profile, threshold, security settings and the results which can be expected. Additionally to that the different features of the SIGNificant Biometric Server are mentioned. Finally the SIGNificant solution is explained in detail and compared with others, to help you to choose the best suited one for your organization.

Table of Contents

1 What is Biometric Signature Verification?

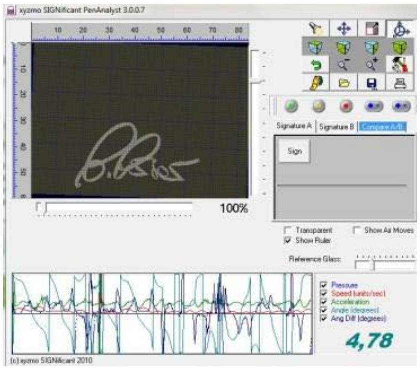
Belonging to the biometric family of products, Biometric Signature Verification authenticates the signers by measuring their handwritten signatures. The signature contains unique biometric data, such as the writing rhythm, acceleration and pressure. Unlike other electronic signature capturing methods, Biometric Signature Verification does not treat the signature as a graphic image. With graphic images, such as the scanned-in signatures we 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, Biometric Signature Verification measures exactly how the signature is signed.

2 Biometric Signature Verification: Two huge advantages

- 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.
- No person ever signs their name exactly the same way twice. Because Biometric Signature Verification can track each person's natural fluctuations over time, it can easily determine forgery.

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, as the movements of the hand (pen) 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). The personal profile has two important characteristics:

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

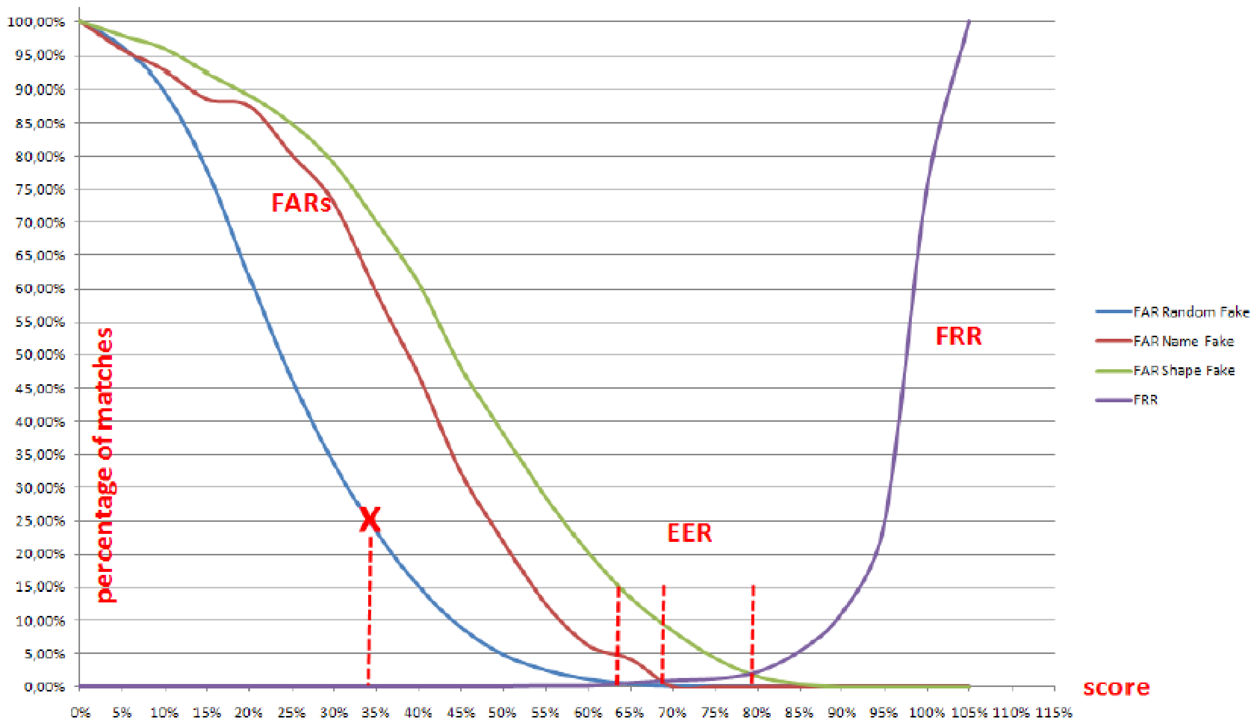


□ Transparent
□ Show Air Moves
☑ Show Ruler

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

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 SIGNificant Biometric Engine is able to adjust the personal profile to adapt to these changes continuously.

3 Performance Measurements



- **FRR** is defined as the 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**). EER marks the point where the same results occur for FAR and FRR.

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 and once hacked, the information can 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 way twice; signatures are bound to be different from one another. 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, so 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.

3.1 The Enrolment of the Personal Profile

The personal signature, by its nature, is a uniquely identifiable trait because it is unique in its 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 enrolment 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 to "simple" signatures.

The typical enrolment 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 enrolment 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.

3.2 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 other's 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.

3.3 The Security Settings

Besides the adjustment of the limitation factors, 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 enrolment process becomes stricter, requiring more users to provide more than 4-6 signatures needed for a standard enrolment.

- **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 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 skilful 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.

3.4 What results can be expected?

We distinguish between three types of fraud:

- **Random fraud**: The forger does not have any idea of how the signer signs. The EER for such fraud is less than 0.01% in the basic security mode.
- **Name fraud**: The forger knows the signers real 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.
- **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%.

4 The Features

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

- **Biometric 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 Limitation factors** – The authentication process is flexible, enabling varying authentication procedures for different environments, allowing organizations 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.

- **Completely Independent from 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 (enrolment, signature verification, suspension of signature profiles) is logged.

5 SIGNificant and Other Signature Verification Solutions

SIGNificant offers the world's most complete, open and accurate real-time signature verification. Since the end of 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 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.

On February 14, 2008 xyzmo shareholders bought the entire IP rights of WonderNet Ltd. (Penflow) including the most prominent technology for electronic biometic signature authentication. By incorporating this technology from WonderNet, 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.

- 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 SIGNificant 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 stept 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 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 wrong profile and “try” to use this for later comparison.

The area of electronic biometric signatrue verification/authentication on a large scale has just started with such high-quality standards as SIGNificant introduces them to the market. There are, meanwhile, early adopters in Europe like www.maquet.com for checking signatures on quality assurance documents, or banks like www.tatrabanka.sk which authenticate all their customers in real-time based on their handwritten electronic biometric signature with our advanced and superior technology as described. This will become a huge market over the next few years, and xyzmo sees itslf clearly in the leading position and far ahead of the competition with the best and most advanced solution available. Self-Learning profiles will be the key!

Trusted by the World’s Most Respected Brands

Deutsche Vermögensberatung
Vermögensaufbau für jeden!
UniCredit
NÜRNBERGER
VERSICHERUNGSGRUPPE
Phone House
GENERALI
+X
BANQUE POPULAIRE
vodafone
INTESA SANPAOLO
Handelsbanken