PSA: Security and the Electronic Industrial Order

A White Paper by WonderNet
March 1999

Contents

Introduction

The minute the electronic revolution began to take over our lives, security became the primary issue for concern. While the strides made by computerization decreased infrastructure costs and increased efficiencies, the perceived risk of forgery and fraud have continued to grow. With face-to-face transactions replaced by face-to-screen interaction, how was an electronic solution to verify that the person on one end really was who she claimed she was?

Today, personal authentication remains a major obstacle in the way of a completely electronic industrial order. Electronic commerce, Internet transactions and network security all require a reliable and secure method of authentication to eliminate the threat of forgery and fraud.

Based on biometric or encryption technologies, many authentication methods have evolved over time, but each has presented its own particular disadvantages. This paper explains why Personal Signature Authentication (PSA) offers an ideal solution that can accommodate consumer masses and become the standard for an unlimited number of commercial and network transactions.

Removing the Security Obstacle

Despite today's existing and perceived security threats on-line, e-commerce and the Internet in particular have changed the working and social behaviors of consumers worldwide.

In the December issue of Fortune Magazine, an article entitled, "The E-Corporation," states the following statistics. "In a Spring 1998 study, Jupiter Communications reported that 10 million people in the US had bought something over the Net in 1997, and it expects 17 million to do so this year – up from virtually none a few years ago. Just three years ago only 4% of Americans used the Internet every day. Today the figure is 25%, says the Pew Research Center." Authors Gary Hamel and Jeff Sampler comment, "The trend is clear: this is not a rising tide, it's a tidal wave."

Credit card fraud absorbed by the three major credit card companies reaches approximately $1 billion annually. Removing this burden will finally unleash the full potential of our existing technologies and clear the way for a complete electronic revolution: a revolution that burgeoned in the last decade but whose progress has remained bottlenecked by security and risk issues.

Why Personal Signature Authentication?

The signature has a long-standing history as our personal authorization mark – our personal stamp of approval. Accepted in all areas of commerce, it has been legally and socially accepted as the way to authenticate who we are. Personal Signature Authentication simply takes this age-old tradition and makes it possible to use and verify the signature electronically.

PSA (Personal Signature Authentication) is an enabling technology belonging to the biometric family of products. Biometrics is a technology, which will positively verify a person's identity by identifying and measuring a trait unique to that person. In the case of signature authentication, a person's handwritten signature is the unique trait that is recognized. This replaces or complements a PIN number or password as verification of identity.

The personal signature, by its nature, is an extremely unique 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.

Other Biometric & Encryption Methods

Other biometric methods used for authentication include: fingerprint identification, retinal scan, palm scanning, DNA identification, voice and face matching.

- Besides the fact that fingerprinting has a negative association linked with crime, this method is imprecise, based on heavy and time-consuming scanning and involves high equipment maintenance costs.
- Retinal scanning is an expensive method that requires large quantities of storage space. Limitations include inability to function with contact lenses.
- Although DNA analysis is highly accurate, it is impractical for daily commercial transactions.
- Voice matching is a method that can be easily broken, since background noise can distort the voice data and a voice recording can be used to penetrate the system.

The most widely used authentication method today is the PIN code. The personal identification number is a computer-generated number assigned to individual's accounts. PINs are protected by encryption. These codes can be cracked and present human beings with chains of numbers to remember for each account.

Defining Personal Signature Authentication

Personal signature authentication is a biometric method that measures a person's signature to verify that person's identity. For a personal signature authentication system to be used as a secure method:

1. it must be based on real time tracking
2. it must be able to carefully distinguish between the natural variations of a person's signatures and forges

While several PSA systems have succeeded in fulfilling the first requirement, they have not achieved the second.

Real Time Tracking vs. OSR

Attempted uses of the personal signature as an authentication system have relied on optical signature recognition which treats the signature as a graphic picture. These attempts have proved unsuccessful because a graphical representation of a signature can be copied. The significant differences that exist between the dynamics of each individual's signature can not be detected.

The most important point to remember in using a personal signature for remote authentication is that it is not a picture. The personal signature is a series of movements performed by a writing device over a flat surface.

These signature movements contain unique biometric data, such as personal rhythm, acceleration and pressure flow. The real time tracking method collects and analyzes the biometric data that uniquely binds the signature to an individual. By utilizing this method, the personal signature is an excellent authentication tool.

FRR & FAR vs. Signature Fluctuation

An intrinsic problem to PSA systems is the inverse relationship that exists between the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). The False Rejection Rate is the frequency with which the correct person is incorrectly rejected by the authentication system, while the False Acceptance Rate refers to instances when a forger is accidentally accepted by the system. A higher accuracy in authentication systems results in a higher FRR, while lower accuracy results in a higher FAR.

To balance these error rates, today's PSA systems assign a predefined tolerance level across all signature parameters. In other words, as long as the average of shape, pressure, velocity and acceleration parameters all fall within this tolerance range, then the signature is accepted. However, change is a natural factor within personal signatures and no two signatures can ever be the same. Static tolerance ranges do not account for this natural occurrence - causing the FRR and FAR to remain at unacceptable levels for reliable signature authentication.

In order for a PSA system to neutralize both the FRR and FAR error rates, it must be intelligent enough to incorporate a weighted calculation of parameters according to an individual's unique traits and to update tolerance ranges as they dynamically change. According to the signer's unique propensity to fluctuation, the PSA system must learn to fine tune the individual personal profile as it fluctuates over time.

How does it work?

[Signature image here]

The [x, y, z, t] data streams collected during the signing process are raw data. For the data to be significant, an analysis must take place. Algorithms convert the data into a signature analysis measuring stroke rates, acceleration and pressure flow.
From this analysis the Personal Profile is created, containing all of the data unique to an individual person's signature.

Raw Data + Analysis = Personal Profile

The Personal Profile contains tolerance ranges for signature variations. A person's two signatures are never exactly the same. If 100% match occurs with the Personal Profile, the signature will be rejected. The personal signature authentication system also accounts for drift rate. Over a period of time, a person's signature will drift. Each time a signature is authenticated, it is added to the Personal Profile so that it is constantly updated.

Assuming that a Personal Profile exists for an individual, the following process takes place when the individual requests authentication.

1. New Signature
2. Raw Data is collected
3. Analysis of new signature constructed
4. Analysis of new signature is compared to the existing Personal Profile
5. If the signature is authentic, then it is incorporated into the Personal Profile. If the signature is fake, it is rejected by the system.

For Internet applications:

6. Personal Profile is encrypted for transmission. Each individual Personal Profile contains the time and date when signature took place.

No actual signatures are being sent electronically. Only the Personal Profile is sent, making it extremely difficult to make any changes in the signature itself.
For an unauthorized party to successfully intercept and reuse a signature, the following would have to take place:

- Decrypt the Personal Profile (the analyzed data)
- Make changes to the analyzed data within the Personal Profile, keeping within tolerance (because two signatures can never be the same)
- Reencrypt the Personal Profile

Where does it work? PSA Applications

PSA can be implemented in a broad range of applications, offering added convenience to the worldwide consumer population and enhanced security for commercial business.

Electronic Commerce and Internet

E-Commerce is expected to reach $168 billion by the year 2002, and the number of global Internet users will reach 200 million in 1999 alone and 1 billion by 2004. Since each commercial transaction involves two sides, a PSA system can be easily adopted as the standard for both consumers and corporations including banks, credit card companies and large chain retailers.

Credit card companies especially receive a twofold benefit from PSA, both at the physical retail level via POS as well as over the Internet with on-line shopping.

How does it work?

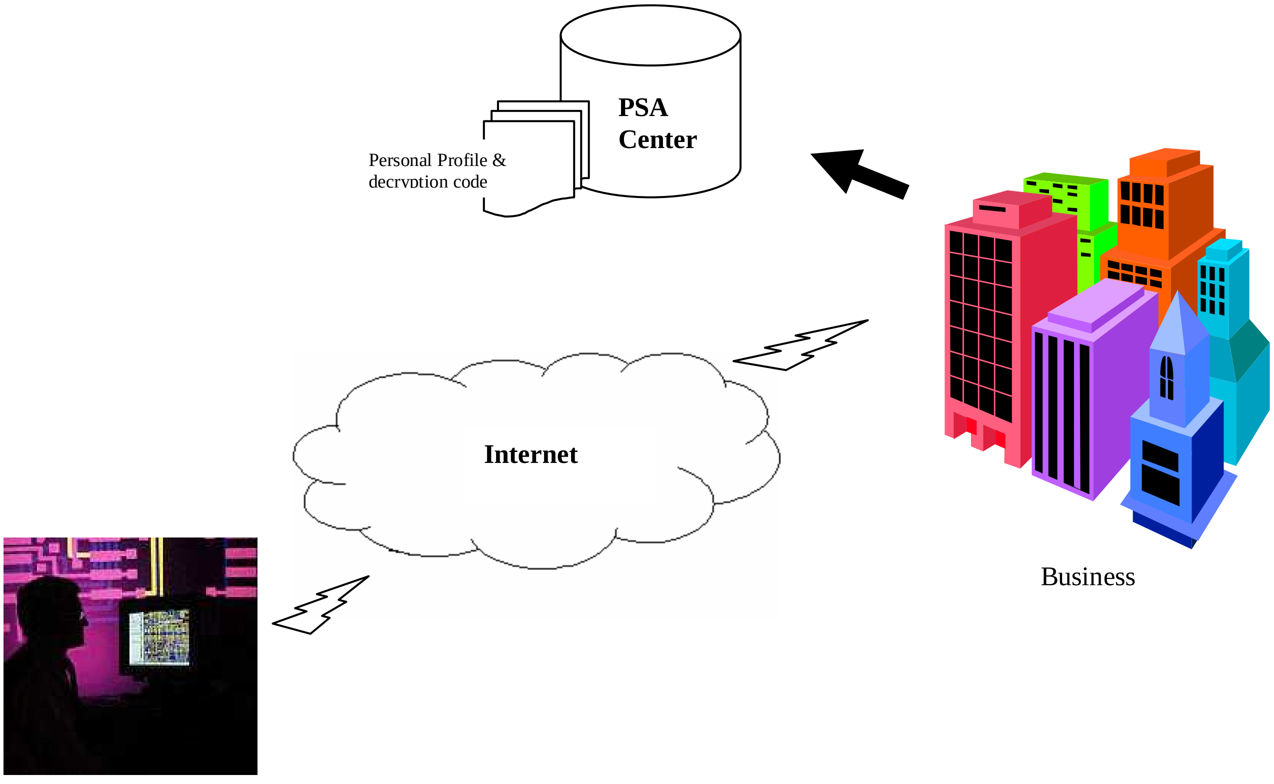
Upon receipt of a signature tablet, consumers will register their signatures with a PSA center. The PSA center collects and stores individual users' Personal Profiles within a comprehensive database. A PSA center can reside within a credit card company, within a commercial organization or within a dedicated third party authentication service.

1. To register with a PSA center, the consumer must submit three signatures so that the PSA system can analyze the characteristics of the signature and create a Personal Profile.
2. The person selects a decryption code and then all the data is compressed into a single record in the PSA center.
3. A personal ID code is assigned to the consumer for reference within the PSA center.

On-line Shopping

To make an on-line purchase today, a consumer completes the company’s on-line order form the necessary credit card information. With a PSA system in place, a consumer only needs to provide the amount of purchase and the personal ID number. The consumer signs the order form using a signature tablet and pen and submits it by hitting the send button.

Transparent to the consumer, the signature is sent to a PSA center which compares the new signature to the consumer’s Personal Profile.



Picture of tablet & signature missing, order form

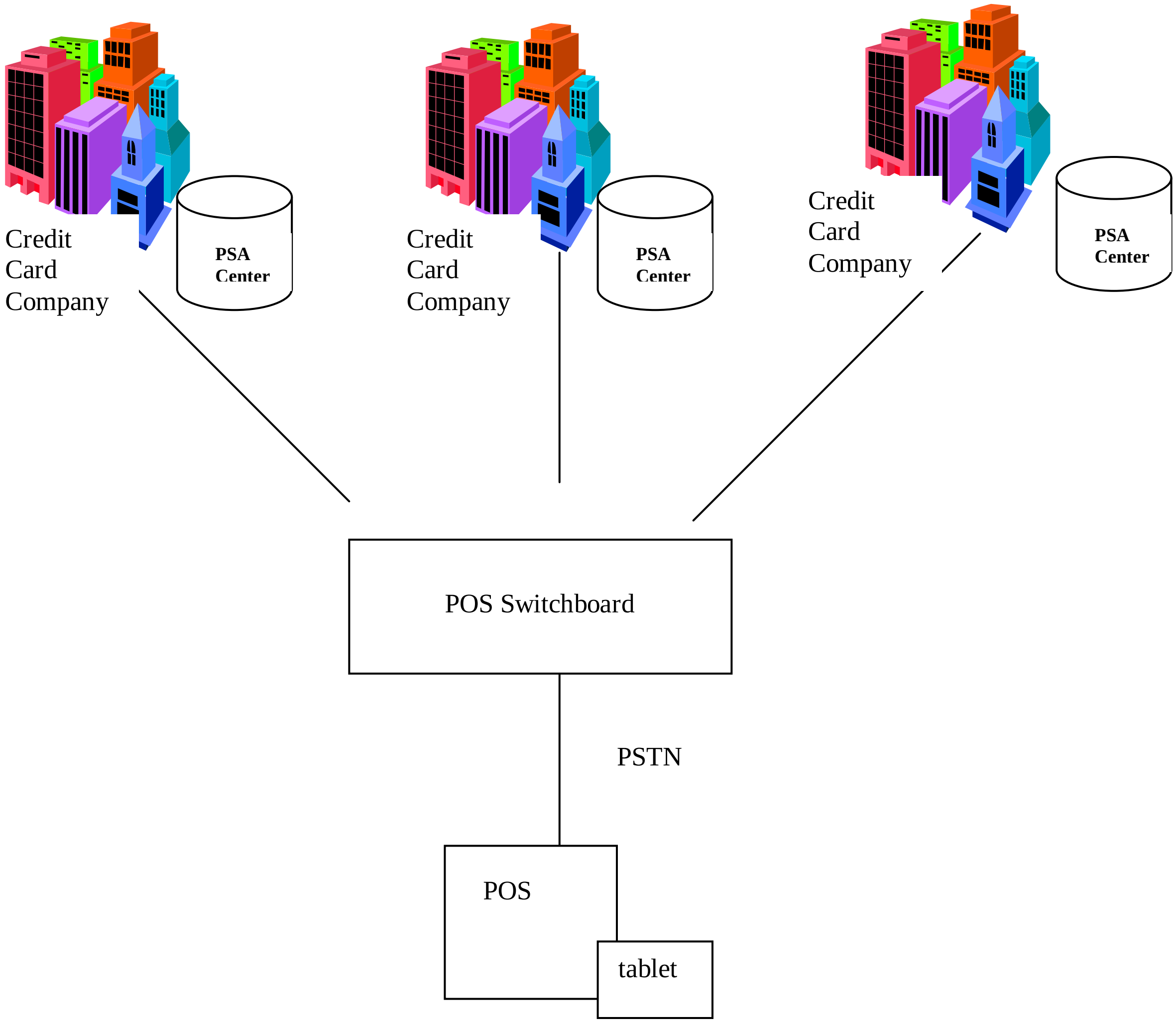
1. The signature data is encrypted and sent (without the encryption code) via Internet to the PSA center.
2. As the encrypted data is received at the PSA center, the appropriate Personal Profile is found, and the decryption code is loaded for data decryption.
3. The Personal Profile parameters are compared to the received data and approval is given if the match is sufficient.

POS

There are two ways in which signatures can be authenticated at the point of sale, alleviating the heavy burden of credit card fraud normally absorbed by vendors.

With today's regular magnetic credit cards, consumers' cards will continue to be checked for validity in the usual manner. The card is swiped and the information is sent via telephone line to the credit card company for approval. Attaching a tablet to the point of sale enables vendors to authenticate, for the first time, that the cardholder is in fact the card's real owner. When cardholders submit their cards, they will sign onto the tablet. When the credit card information is sent, the signature will be sent to the PSA center where the signature will be compared to the Personal Profile.

In the credit card of tomorrow – the internal chip (IC) card - the card itself will contain the Personal Profile. Signing onto the tablet will enable comparison with the profile contained on the chip immediately.



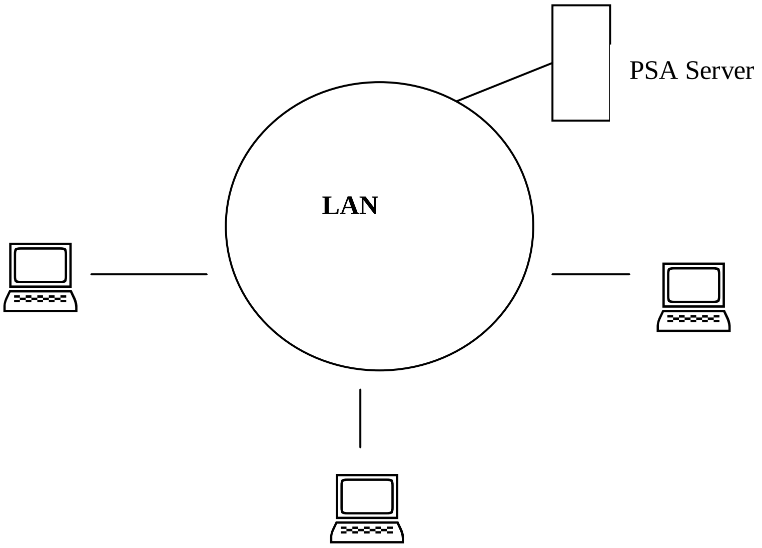
Network Security

PSA used for network authentication enables the minimization of threats and maximization of opportunities in moving crucial business processes to the Internet, intranet and extranet environments.

The total US market for network authentication systems reached $400 million in 1998 and is forecasted to reach $630 million in 1999 and $4.58 billion by the year 2005. Major users of such products and technologies are:

- Banking and financial industries –
  remote access to personal accounts for withdrawal, deposits and electronic checking
- Medical services –
  securing access into patient clinical records
- Government institutions –
  government forms including tax forms
- Large multinational companies
  Secure exchange of information within internal LANs and WANs, and extranets
- technologically oriented companies
  registered software users can access software upgrades

Within all of these organizations, PSA provides an equally critical solution for secured entrance into any building or facility. High security rooms and facilities requiring membership or reservations will have the ability to authenticate the pertinent individuals automatically.



Entrance into today's corporate networks usually requires a login and password key which can be penetrated. The PSA system will require a personal signature in order to access an individual computer as well as enter into a local area network.

The WonderNet Solution

WonderNet is the developer of innovative, quality biometric products, services and total solutions for the security needs of the rapidly expanding information technology market.

With the introduction of its patent pending technology, WonderNet intends to make personal signature authentication (PSA) one of the industry standards for enabling complete and effective electronic commerce.

A strong foundation coupled with powerful technology has enabled WonderNet to offer an unprecedented reliability within its PSA system.

What sets the WonderNet PSA system apart?

- WonderNet's unique patent pending algorithm handles dynamic & static data covering a multiple number of parameters to define an individual's signature.
- Signature parameters are weighted according to the individual's unique traits and propensity to fluctuation.
- Intelligent PSA learns and fine tunes the individual signature profile as it naturally fluctuates over time.
- Accurate method of capturing natural fluctuation rates dramatically reduces false rejection and false acceptance error rates.
- Personal Profiles size require only a few hundred bytes of storage space, allowing Personal Profiles to be stored on IC-cards (smart cards).
- Regardless of tablet positioning or user contact with the tablet, the system captures all hand movements to guarantee the highest level of accuracy and flexibility.
- A strategic partnership with Wacom of Japan, the global leaders in the technology, production and marketing of signature tablets – gives WonderNet the best supply of tablets as well as complementary market expertise.
- The WonderNet management team has extensive experience in global management and marketing. They have proven experience in bringing technological developments to commercial fruition. In 1991, the President and CEO of WonderNet founded GraphiTech Ltd., making it a worldwide leading provider of artistic CAD/CAM solutions.