Crypto-Sign™ - A White Paper

The Crypto-Sign Solution
Crypto-Sign offers a new approach to electronic signatures to enhance the security of remote, web-based and wireless transactions and to generate significant economic savings. It is a patent-pending technology which combines the benefits of the PIN /Password with those of electronic signature verification to utilize the benefits of, and eliminate the disadvantages of both systems. Its author, Rod Beatson is the founder of Transaction Security and the author of the associated patent application. Crypto-Sign is essentially a non-invasive, low cost, software-based biometric solution to the problem of providing secure access control to remote devices and identifying remote authors of electronic messages and transactions.

Conventional Signature Verification Systems
With the introduction of the Electronic Signatures In Global and National Commerce Act (the "E-sign" Act) an electronic signature is essentially any sign submitted electronically by the author signifying intent. This could be achieved by the submission of a password, which might release a private key to generate a digital signature to "sign" the document. Alternatively the author might submit a biometric sample to be identified by the system and hence generate the electronic signature

In the field of biometrics and particularly that of dynamic signature verification there is a belief that the submission of one's signature on a digitizer, enabling the analysis and comparison of that signature against a previously generated template would provide a secure method of tying an electronic document to the author and give the ensuing transaction a high degree of integrity. Biometrically identified documents and transactions, using dynamic signature verification have been used in a variety of applications from the early 1980's. Applications include cash withdrawals from retail bank branches, change control of engineering drawings, entry control to Safety Deposit boxes, identification of customers using credit or charge cards at retail point-of-sale and a number of others.

Today there are two main forms of dynamic signature verification systems. One system captures and processes pressure and force/acceleration signals sensed by a special pen as it moves over the writing surface.

The other dynamic signature verification system uses a digitizer, Tablet PC or Personal Digital Assistant (PDA) as the capture instrument and works in the following manner:

The capture device is used either with an inkless stylus writing directly on the surface, or with an ink based stylus writing upon paper positioned on the surface. Many digitizer systems today use the inkless stylus. In both systems the pen position is sampled many times a second to generate a stream of sequential X,Y coordinates. Some systems also sample the pen pressure at each coordinate sampling point. From the samples, which are taken at recorded time points, it is possible to define features of the signature, which can be based upon any function of shape, pressure and/or timing data from the signature.

It is possible also to capture the (x,y,t,p) coordinates of the signature key events (for example turning points associated with x, y or p or the points at which the stylus leaves and rejoins the surface) and to use these "event coordinates", standardized against time, in the signature definition.

During enrollment or registration the author submits a number of signatures and a data template, representing the features of the legitimate signature is calculated. Thereafter, as the author submits further signatures, the submitted signature is compared against the template to provide a

statistically based decision regarding it's authenticity and the template is often updated after a successful match to track the signature as it changes gradually over time.

Different systems use different features and different decision-making methods based upon measuring the degree of match (or mismatch) between the submitted signature and the template.

One problem associated with dynamic signature verification is that no two signatures from the same person are ever identical and the accept/reject decision has to consider the inherent variation of the author's signature, which is sometimes large.

Another problem to overcome in dynamic signature verification is that of the angle of the signature as it is written on the digitizer. Typically there will be changes in angle of the signature from one signature to the next and, if these are sufficiently different, the likelihood of a successful match with the signature template is low. Signature systems use different methods to correct for angle before calculating the features or the event coordinates. The result of these problems is that signature verification systems can generate relatively high False Reject Rates (where the authentic individual is denied access to the system) in testing

Another problem with dynamic signature verification is that typically, the author's signature is readily available to a determined impostor and he may also have witnessed the actual signature being submitted. The result of this is that dynamic signature verification systems, based, as they are, upon an open signature can generate relatively high False Accept Rates (where the impostor is mistakenly granted access to the system) in testing

Using dynamic signature verification it is difficult to generate a high performance set of algorithms, effective over a large population, offering powerful discrimination between an authentic signature and an attempted forgery. If the accept/reject threshold level is set too tightly, to reject potential forgeries and generate a low false accept rate (FAR), the effect is often to increase the false reject rate (FRR) to unacceptable levels.

The objective of a biometric system is to minimize both the FRR and FAR (or to maximize both the authentic acceptance rate and the Impostor rejection rate). In any biometric system as one of these rates improves the other deteriorates. One measure of performance of a biometric system is to determine how good these rate combinations are.

The Crypto-Sign Method

Crypto-Sign covers a method of using automatic dynamic ***sign*** verification to verify a secret sign (as opposed to an open signature that anyone might have access to) made on a PDA, Tablet PC or digitizer. This could be used to:

- Grant access to the device.
- Release a valid ID and electronic signature of the individual and attach it to an electronic document or a signature-bearing transaction.
- Release a private key for encrypting a message.
- Release a password, PIN to allow the individual to gain access to a computer file or network.

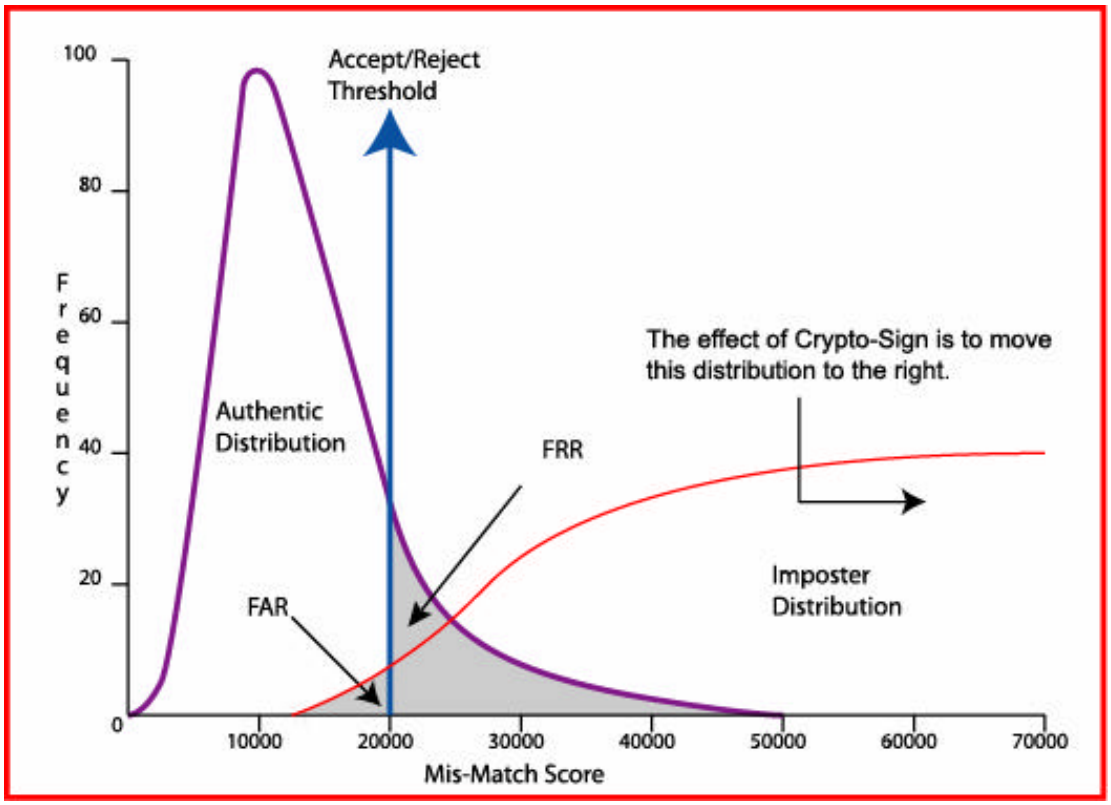
Such a sign, coupled with the attached valid signature would now constitute a secure electronic signature where prior to the E-sign act it would not have been a valid instrument. The secret sign is always submitted with an inkless stylus and is never displayed or printed in its submitted form.

The Crypto-Sign method has a powerful advantage over conventional dynamic signature verification methods in that the sign, which is also tested statistically against a stored template, is

maintained as a secret by the user in the same way a password or a PIN is kept secret. The consequence of this is that an impostor would have to know what the sign looked like, as well as being able to make it in the same manner as the author. This decreases significantly the chance of an impostor gaining access to the system. Hence the accept/reject threshold can be loosened significantly without increasing the FAR. Consequently, the FRR reduces to give high performance.

For the purpose of signing electronic documents the valid signature of the user is also stored in electronic form and is only released to the transaction/document when a verified ***secret sign*** (Crypto-Sign) has been submitted.

Effect Of Crypto-Sign On the FRR/FAR Biometric Performance (Fig. 1)



The frequency distribution of a set of authentic signs or signatures is represented by the Authentic Distribution on the left of Figure 1. The FRR is represented by the area of the shaded portion bounded by the authentic distribution curve, the x-axis and the Accept/Reject Threshold (currently set at a level of 20,000 so that Mis-Match Scores greater than this value will be classified as “rejected”.

The frequency distribution of a set of impostor signs or signatures is represented by the Impostor Distribution on the right of Figure 1. The FAR is represented by the area of the shaded portion bounded by the Impostor Distribution curve, the x-axis and the Accept/Reject Threshold. Values of Mis-Match scores generated from impostor signs or signatures, which are less than 20,000, will be mistakenly accepted as authentic.

It is easily seen that as the Impostor distribution curve moves to the right, that the FAR decreases significantly. **This is the effect of Crypto-Sign** where the impostor has to reproduce a secret sign as opposed to an open signature. Consequently, the Mis-Match Score Accept/Reject Threshold can be increased, which reduces the FRR significantly.

Some Independent Biometric Performance Test Results

Biometric Performance is a key area of product differentiation and the inventor's pre-Crypto-Sign **Signature** verification algorithms were positively evaluated by Sandia National Laboratories – see Figure 2 below. They compare favorably with better-known biometric systems such as fingerprint, facial recognition and voice recognition. With the added secrecy afforded by Crypto-Sign the FAR/FRR performance of the **Sign** verification algorithms have been significantly enhanced above this level.

The Sandia National Laboratories test results on the Sign/On Signature verification algorithms were generated from 3106 authentic attempts to gain access and 6727 impostor attempts to gain access. The user population was some 100 enrolled individuals. Impostor testing was conducted under the assumption that the impostor knew the identity of the target signature (and would therefore have potential access to a sample of the signature, and possibly to the way in which it was signed)

For the ICSA tests of 1998 we do not have access to individual data regarding the different biometrics. However, the tests do support the hypothesis that the biometric signature verification performance of the Sign/On algorithms is slightly superior, on average to the algorithms of Finger, Face and Voice biometrics.

When the Crypto-Sign concept of the secret sign is introduced we can expect that its biometric performance will significantly dominate the earlier Sign/On results as well as those of the other biometrics. An estimate of the new Crypto-Sign algorithms is included.

Crypto-Sign™ Performance (Figure 2)

Biometric Solution	Authentic Acceptance Rate	Imposter Rejection Rate	Comments
Sign/On Biometric Signature Verification Evaluated by Sandia National Laboratories - Spring 1990.	99.4%	99.3%	Based on up to 3 signature attempts Active Forgery
Finger/Face/Voice Biometrics Evaluated by International Computer Security Assoc. - Summer 1998	98.7%	98.7%	Based on up to 3 attempts. Passive impostor Attempts
Estimated Crypto-Sign™ Performance Based on Sign/On performance enhanced by Crypto-Sign™ Secrecy	> 99.9%	> 99.9%	Based on up to 3 sign attempts. Active or Passive Forgery

Benefits of Crypto-Sign Over Other Identification Technologies

It is worth summarizing the pros and cons of different identification technologies and Figure 3 below indicates that, in comparison to Crypto-Sign, which can be used to release a **secure** password:

- The Password/PIN is insecure since, if the impostor knows it, it compromises the system with 100% certainty. It is easily passed on from person to person and simple passwords can be easily guessed.
- Finger Prints can be viewed as invasive, especially to users of remote devices like PDA's. They are certainly more expensive when incorporated on PDA's and Tablet PC's because of the extra fingerprint sensor hardware, which adds proprietariness to products incorporating them.
- Digital Signatures are not biometrics, use insecure passwords to generate the keys and interoperability problems make systems difficult to implement.

Comparison Of Different Identification Technologies (Figure 3)

	Crypto-Sign™	**Passwords/Pins**	**Finger Prints**	**Digital Signatures**
Security & Accuracy	Very Accurate Highly Secure	100% Compromised if Known.	Secure and Accurate	Not A Biometric. Uses Passwords
Privacy	Non-Invasive	Non-Invasive	Invasive	Non-Invasive
Ease of Use	Simple To Use	Simple But Often Forgotten	More Costly Can be Difficult	Difficult to Implement
Audit Trail	Signature Image	None	Print Image?	Digital Certificate

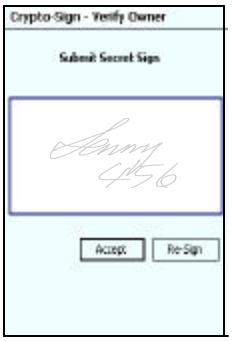
Crypto-Sign Applications:

Crypto-Sign™ Applications range from secure access control to the PDA or tablet PC, which protects stored data from falling into the wrong hands if the device is lost or stolen, through remote access control to networks, web sites, files and electronic documents. Crypto-Sign can be used for secure document signing for proof of authorship and delivery and is ideal for secure storage, access to and retrieval of electronic documents from electronic vaults. With the advent of the Net enabled wireless PDA, it can also be used for conducting secure document-based transactions and M-commerce from these devices. It would be an ideal technology to work in conjunction with an authentication server based service, using wireless PDA's or wired PDA's connected to Workstations or Laptops, where the pen-based hardware means of biometric input is already included.

Crypto-Sign as a secure Access control method for PDA's and Tablet PC's

- Protection of an 8 character, case-sensitive password without the need:
- To enter it or remember it
- Without the fear of someone knowing it
- Without the fear of someone guessing it

Note that the secret sign is not necessarily the signature of the author, although it could be. The secret sign is displayed below (as a watermark) to demonstrate its use. In application the sign is never displayed.



The PDA as a secure Token. The PDA hardened with Crypto-Sign displays all three ingredients of a high security authentication system and can be used to control access to the workstation or Laptop.

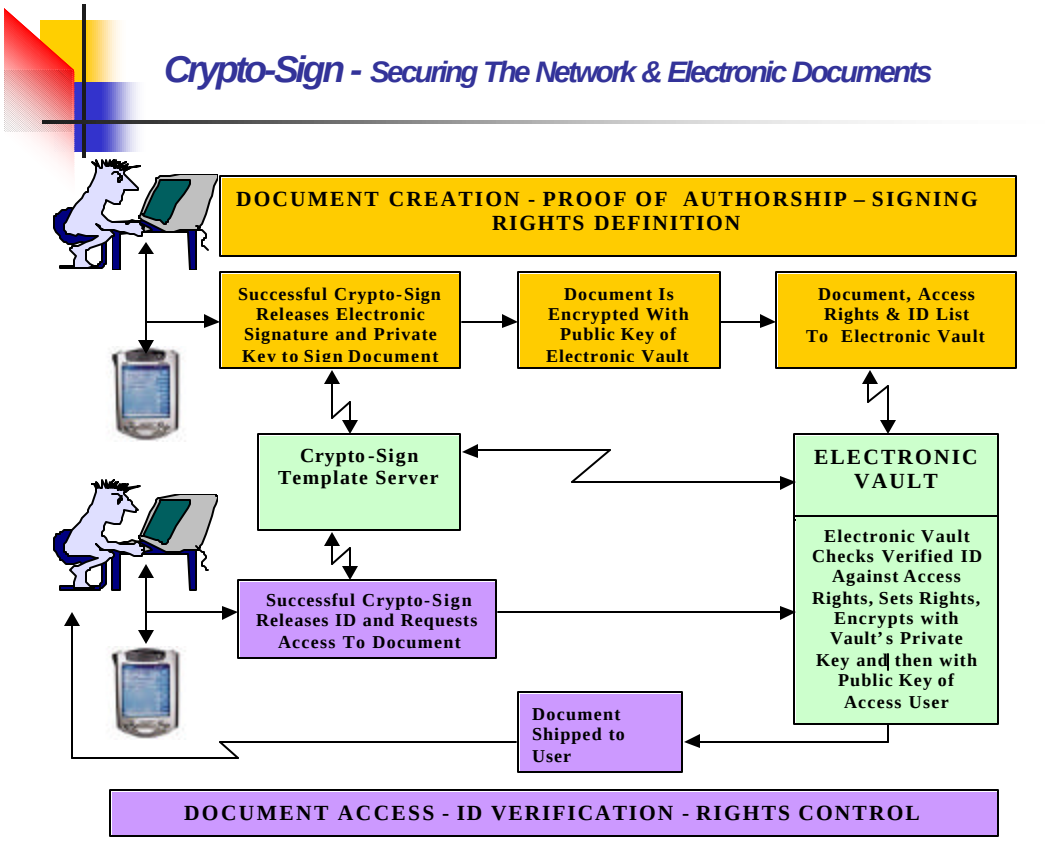
- The “what you own” is the PDA.
- The “what you know” is the Secret Sign.
- The “something about you” is the Biometric data extracted from the way the Secret Sign is submitted by you.

The PDA as a secure key to Intranet sessions.

- PDA presence constantly monitored by the workstation on an encrypted line.
- Removal of the PDA closes down the session.
- Log-On to the Workstation/Network requires a Crypto-Sign enabled PDA.
- Provides strong Remote Authentication capability.

The Crypto-Sign hardened PDA as the source of Electronic Signatures, Encryption Keys and Digital Certificates for secure electronic documents with proof of authorship and an "ink on paper" look.

- Secure Email
- Paper Systems replaced by secure Electronic Documents.
- Huge economic benefits (see Business@ The Speed of Thought)
- Secure On-Line E-commerce from the workstation



The Crypto-Sign hardened PDA as the source of Secure Wireless Transactions.

- Key release for encryption purposes
- Secure Access to Server after authentication by server.
- E-commerce transactions
- B2B
- B2G
- B2C