

## Understanding Electronic Signatures

The recently passed Federal Electronic Signature legislation will now enable true e-business solutions. By giving electronic signatures the same legal weight as wet ink signatures on paper, the legislation enables enterprises to finally realize a fully electronic process flow (even those involving contracts and endorsements).

The Federal Electronic Signature legislation is "technology neutral" and defers to the marketplace for competitive selection of the technology variations. The two main technologies that have emerged in the signature space are Signature Dynamics and Public Key Infrastructure (PKI). If properly deployed, each of these technology approaches meet the basic requirements for a legally acceptable electronic signature. These technologies are dramatically different in their approach but can also be integrated together in a complimentary way. In evaluating which technology is best for a given enterprise, many variables need to be considered not least of which are the specific applications involved. Before comparing and contrasting Signature Dynamics and PKI it will be helpful to take a brief look at the basic elements of an electronic signature.

The Federal Legislation (E-SIGN Bill) effective October 1, 2000 confirms that states must allow the use of electronic signatures if the two parties involved agree to this method of signing. However, each state is empowered to legislate its own electronic signature requirements. For example, in California, the basic elements are:

- It is unique to the person using it.
- It is capable of verification.
- It is under the sole control of the person using it.
- It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

These elements are typical of the other states that have electronic signature legislation that has been passed or is pending. Both Signature Dynamics and PKI can be enabled with the functionality needed to meet these basic requirements. The key point to understand is that the E- Signature law eliminates the Legal Risk, so that it's now all about Business Risk (e.g.- customer acceptance, non-repudiation, etc.).

### What is PKI and how does it work as an Electronic Signature?

PKI technology has been around for almost two decades. It was conceived as a way to transmit electronic information in a secure manner. PKI is based on a key pair system. Each user has a private key or digital certificate and a corresponding public key. The keys are used to seal (encrypt) and un-seal (decrypt). The keys are typically issued and administered by a 3rd party Certification Authority such as VeriSign. The user is responsible for safeguarding his or her private key as this key is used to encrypt and decrypt electronic documents or transmissions. The private keys are typically protected by a password or PIN. The public keys are generally made available to all people within the user's network. The keys can only work as a pair so the CA can reissue keys if it is felt that the security of a user's private key has been compromised.

As originally conceived, if Party A sends a document to Party B then, Party A would use Party B's public key for encryption and Party B would open (decrypt) the document with his private key. This method for using PKI ensures that the document is heavily encrypted and can only be opened by a particular person. To use PKI as a signature the user encrypts (signs) the document with the private key and the recipient opens the document with the user's public key. Authentication of the signatory is assured by the diligence of the CA and the user's safeguarding of the private key.

### What is a Dynamic Signature and how does it work as an Electronic Signature?

Dynamic Signatures are based on biometrics. A biometric is a human body measurement used to positively identify an individual. There are many biometric technologies that have been developed including retinal and iris scans; thumb and palm scans; voice and face recognition; and even DNA analysis. However, for the purposes of applying biometric technology as an electronic signature this discussion will focus on the pen based personal signature.

Pen based electronic signature capture and verification has become the leader in dynamic signatures. The reasons for the wide public acceptance of this biometric are based in culture. Users have been using the pen with ink based personal signature as a way to lend formal accountability to contracts and the like for centuries. Pen based electronic signatures enables this same culturally accepted method to be brought forward into the digital age. The ceremony of the act of signing in itself is a rich tradition that cannot be overlooked. By maintaining the act of signing and gaining all of the benefits of a true electronic signature, the pen based biodynamic signature has become the clear leader for enterprises offering electronic signatures for their customers and business partners.

Beyond the cultural acceptance, robust pen based electronic signature solutions are also among the best biometrics with

respect to accuracy. The stroke dynamics collected in an electronic signature are extremely unique to the individual as well as being highly repeatable. The shape of the signature is captured along with timing elements (speed, acceleration) and sequential stroke pattern (for example, did the "t" get crossed from right to left and did the "i" get dotted at the very end). These "muscle memory" dynamics can yield accuracy results that are comparable to the best alternative biometric technologies (such as thumb and retinal scans). The verification engines for the most sophisticated pen based solutions can be finely tuned to yield the optimal False Acceptance Rates (FAR) and False Rejection Rates (FRR).

In addition to having built-in cultural acceptance and strong biometric authentication, the pen based electronic signature is the most intuitive to use. A typical form, document, or contract using this technology will have pre-designated signature fields that are simply mouse clicked when ready for signing. A signing interface appears that can, if needed, collect supplemental information about the signing event such as the intent or purpose of the signatory and the location of the signing. The signer then simply signs on a high quality cost effective digitizer tablet (such as the ePad by Interlink) or a Palm Pilot and the ink is displayed in real time and with high fidelity in the signature box. Once again, underlying the captured ink are the biometrics of the signatory's signature.

Lastly, in the discussion of pen based electronic signature solutions, it is important to consider the security features and issues. A sophisticated pen based electronic signature solution should not only make the signing process more efficient, but also make it more secure. There are several key areas where security needs to be well executed. The biodynamic signature data that is collected should be secured so that it cannot be lifted from the document and used elsewhere. Different approaches or a combination of approaches can be used such as high encryption and obfuscation. Also, the signature needs to be bound to the document in such a manner as to make it tamper evident, typically done using hashing algorithms. Additionally, if the application in question is using "real-time" signature verification, then the storage of the signature templates needs to be well secured.

### **How can PKI and Signature Dynamics complement each other?**

The main shortcomings of PKI as an electronic signature tool involve the lack of intuitiveness for the user; the cultural acceptance; and the inherent weaknesses of password based security. PKI is based on "Trust" model that can easily be violated, either deliberately or innocently, since the secret (password) can be transferred. By using real time signature verification in lieu of the password for the private key, the main weaknesses of PKI are addressed: the lack of an intuitive interface and the password. In addition, the Signature Dynamics solution is benefited from the high encryption needed for "hacker-proof" transmissions of the document or form. This is an extremely secure model and perhaps the security redundancies would exceed the needs of most e-signature applications. However, this kind of highly secure electronic signature solution is available today (CIC's Sign-It Secure) should the application require it.

### **How are leading-edge organizations moving forward with Electronic Signatures?**

High performing enterprises maintain their edge by quickly seizing upon the opportunity to create worthwhile operating efficiencies while maintaining or ideally enhancing the experience for their customers. Because of the widely known efficiencies gained from e-Commerce and paper eradication, Electronic Signatures is clearly one of these opportunities. In moving forward with electronic signatures these enterprises have thoughtfully considered the following:

- The application and user requirements

Examples:

- B2B, B2C or both
- Brick and mortar location or Internet
- Signing a form, document, or

- The operating environment and system integration

Examples:

- Based on Internet Browser
- Adobe Acrobat PDF form
- Microsoft Word Document
- Custom application
- Win 2000, Unix, Palm OS, or others

- The future need to expand or merge the electronic signature application

- Laws and regulations of applicable states and agencies, since in addition to state laws there may be regulatory bodies within a particular industry that need to be considered.

With this analysis, it becomes easier to focus on the right technology partner.