White Paper:
Security and Legal Issues in VPSign

Challenges in Capturing Electronic Signatures on Existing Devices

This white paper covers these issues:

- *Challenges in existing Electronic Signatures capture devices.*

Legal aspects of electronic signatures

- *Compliance of VPSign's secured signature*
- *Security aspects of using VPadWiz Pro for Android-based tablets*

Previous generation devices for storing electronic signatures created the following compliance gaps:

- Signers use a separate device for signing that creates the signature image and captures its biometric properties, while the target document is stored separately and displayed on the agent's screen.
- An independent signature image and object is created and "glued" later by the client or server software to the target document. This may result in disputes where the customer can rightly claim that the signature was attached to unacceptable paragraphs or documents.
- Document hashing and biometric data cyphering for security reasons, performed on the client or server side, when not fully controlled by the signer, are exposed to external interference and tampering.
- Signed target documents are not presented in real size to the signer for a self-guided review at the signer's pace. Disputes in courts often arise regarding this issue.

Legal Aspects of Electronic Signatures

Global legislators refer to the acceptance of electronic signatures on electronic documents as legal evidence in the same way as traditional paper documents signed in "wet ink". Laws such as the EU Directive on Electronic Signatures in Europe and the US UETA and ESIGN acknowledge and differentiate between a "secured signature" and an "authorized signature" (which is produced by a certification authority), building a strong foundation for utilizing electronic document signatures to replace expensive paper documents.

What you see is what you sign

Teradyon, Misgav 20179
P.O.B. 49
Israel

Tel: +972-54-6447447
Fax: +972-4-9990493
www.VPSign.com

Common basic terminology employed in various laws defines "secured electronic signature" using the following criteria*:

- Is unique to the signer.
- Enables signer identification.
- Is produced by a device that is fully controlled by the signer.
- Enables detection of changes made to the electronic document after signing.

*Some laws do not require the signer to perform a self-review of the signed document, presumably due to its being obvious. However, most early-stage e-signature capturing devices fail to show the actual document text to the signer and create a signature as a separate object, attached to the document by the organization's software, sometimes including it in paragraphs not originally signed by the signer. Such electronic documents have failed court rulings on validation.

Examples

Let's examine some examples of legally acceptable signatures.

Personal graphical signatures

The legality of the signatures stems from compliance with these criteria:

- **Unique identification of signer**: Each signature is different for each individual by its form and its biometric measures (pressure, velocity, line coordinates, pen lifts). These biometric characteristics are widely accepted today as standard for legally accepted signature identification and proof.
- **Validation of signer's identity**: Courts use the expert services of graphologists to authenticate a person's signature by comparing it to signature samples created by that person.
- **Self-controlled device**: The signature is produced by the person holding the pen, who can exercise complete control over the document.

Digital certificate produced by an approved Certification Authority (CA)

- **Signers are unique**: The CA provides each individual with their own unique digital credentials.
- **Signers are identified**: Digital certificates are issued only after the authorities physically identify the subjects, ensuring a high level of security during issuing process, thereby preventing copying or transferring to another person.
- **Self-controlled**: The digital certificate resides on a smart card or other device that is kept by its owner, thus enabling full self-control. The digital certificate is activated by a secret PIN code.

- **Changing audit trail**: Signing with a digital signature adds a signature time stamp to the document. Any later changes to the document are identified.

High Compliance of VPSign's Secured Signature

VPSign's apparatus enables signing electronic documents by graphic signature and or by smart card bearing digital certificates in a way that conforms and excels even above the basic requirements of the law.

Signer-unique:

VPSign pads and software utilizes a means for capturing graphic electronic ink signatures in real-time, signed directly on the electronic document presented on an LCD screen. The biometric data captured by VPSign's VPad is significantly accurate and detailed due to its high sample rate (200 P/S) and wide pressure scale (RSA 2048-bit encryption) that provide a more solid ground for signature validation than any traditional "wet ink" signature on paper, by using computerized authenticating mechanisms, highly superior to the limited eye and magnifier of the graphologist.

Signer identification:

As stated, logging the biometric characteristics of the signature and keeping it as part of the same document enables better signer identification by signature sample comparisons. In addition, VPSign VPad is equipped with more means of identification:

- Smart card reader. Operates in full compliance with ISO7816 (including ISO7816-1, ISO7816-2, ISO7816-3, and 3.3V).
- All APDU commands can be executed by the smart card reader, according to ISO7816-4, T0, or T1. Includes real time ID and authorization verification.
- USB port.
- Optional camera.

Self-controlled by signer:

- VPSign's VPad presents full sized document images, showing original font sizes, for the signers to review and sign with full transparency.
- The signer can browse through the document at a self-determined pace, and then sign, cancel a signature, or approve it in all the required places without the agent's interference.
- Each approved signature is rasterized in real time within the device into the document image, without producing a separate object that can be copied or used elsewhere later on.
- Signature biometric data is cyphered and saved in the document body after approval, in a standard, highly secured cyphering protocol (RSA 2048).

What you see is what you sign

Teradyon, Misgav 20179
P.O.B. 49
Israel

Tel: +972-54-6447447
Fax: +972-4-9990493
www.VPSign.com

- The whole document is digitally hashed upon its approval by the signer with a digital certificate public key (X.509 Standard) issued by a CA. The private key is kept by a trusted third party or by the CA alone for the highest security.
- After locking, the document is automatically transferred in a TIFF or PDF/a format that is sealed and signed into the organizational computer and cannot be tampered with by anyone.
- The device does not keep any trace of the document after its delivery and the signer's session concludes.

Changing audit trail:

Using the VPad for signing documents has many advantages over paper signing:

- In the document body, the device saves the exact time stamp of footprints of each operation performed by the signer.
- Unlike the paper signing process that exposes the signer to post-signature changes to paragraphs by someone else, locking and sealing the electronic document prevents changes altogether.
- Signature time stamps can be compared with the printed dates of the document, ensuring authenticity.
- Recording browsing history can be accessed later as additional proof of the actual signers' behavior during the process in case of disputes over the document content.

Security Aspects of using VPadWiz Pro for Android-based Tablets

VPSign supports using standard Android-based tablet devices as Samsung 10" Note, especially for mobile field agents who need to operate organizational systems remotely via the internet or VPNs.

The security paradigm and apparatus for this software is identical to that implemented in a stationary VPad. However, the VPad has its own sealed firmware that makes hacking or any outside interference with the signing process and data totally impossible,

The Android operating system is considered to be vulnerable. This fact must be kept in mind when choosing the appropriate signing solution, considering the risks of using less secure systems as opposed to the highly secure stationary VPad.