European Electronic Identification and Trusted Services for Electronic Transactions (eIDAS)

This white paper reviews the legal effectiveness of xyzmo's e-signature solutions, SIGNificant, in relation to the newly adopted EU Regulation 910/2014 on electronic identification and trust services for electronic transactions, especially for the use case of capturing handwritten signatures that are forensically identifiable. SIGNificant supports many other e-signature methods as well, which are not part of this white paper.

The new legislation is a successor to the existing Directive 1999/93/Ec. It provides a clear legal framework at an EU level and breaks down any cross-market barriers to using e-signatures. It will help to increase trust in electronic transactions, promote cross-border use of e-signatures and take Europe a step closer to a single digital market. The directive also requires member states to recognize each other's electronic identification systems. Most provisions will apply from 1 July 2016.

This white paper focuses on (normal) e-signatures and their legal effect under the EU regulation. According to Article 5.2 of the existing e-signatures directive, (normal) e-signatures may not be denied legal effectiveness and admissibility as evidence in legal proceedings. The more trustworthy the technology used, the more trustworthy the signed document. This basic principle has applied for many years. The new e-signatures directive takes this a step further and businesses will no longer be confronted with a patchwork of national legislation. Instead, they will only need to comply with one common and fully harmonized set of rules, significantly reducing the risk of interpretational issues that plagued the old e-signatures directive.

1 What is new?

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using **electronic signature creation data** that the signatory can, **with high level of confidence**, use under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

The new regulation provides, first of all, a new and broader definition for the key concept of e-signatures. That concept has been defined as data in electronic form that is attached or logically associated with other data in electronic form and "which is used by the signatory to sign." This text replaces the former definition in the old directive: "which serve as a method of authentication." This important change in the definition **shifts the focus from the authentication of the signatory to the intention of the signatory** (from "Who placed the e-signature?" to "Did the signatory want to agree to the signed content?").

In addition to unchanged requirements – (1) uniquely linked to the signatory, (2) identifying the signatory and (3) linked to the signed data – an e-signature should be created by the signatory, under his sole control, "with a high level of confidence".

2 How does xyzmo's e-signature solution comply?

A signature captured with xyzmo's e-signature solution, SIGNificant, is much more than just an electronic image of a digitized signature:

- SIGNificant records the handwritten signature of a person using all available parameters, such as speed, acceleration and rhythm. These parameters are unique to every individual and cannot be reproduced by a forger. Thus, a digitized signature is forensically identifiable.
- When someone claims: "I didn't sign that," a forensic expert can perform a deep manual verification of the signature any time afterwards, using the SIGNificant PenAnalyst software, just as they would with a signature on paper. In addition to this service, SIGNificant also provides signature verification that authenticates a signature against a pre-enrolled signature profile database in real time.
- The biometrical signature data are encrypted asymmetrically using a public key directly while the signature is being recorded. Reading the signature for verification purposes is only possible by decrypting it with the corresponding private key, which can be stored either offline, e.g. at a notary, or when required online, for example in a High Security Module (HSM).
- To prevent sniffing of the captured biometric data from the signature tablet, SIGNificant's security mechanisms range from encrypting the communication between the signature pad and the computer to an end-to-end encryption of the signature data on the pad itself.
- Furthermore, the signature is always securely bound to a unique document. The document's fingerprint is encrypted together with the signature data, making copy/paste attacks impossible.
- SIGNificant shows the relevant part of the document as the background image, even on signature pads, to provide the signer a visual link between the signature and the document. On many signature pads, SIGNificant enables signers to browse through the whole document on the signature pad if they want to. Although the displays are typically not very large, this works quite well.

SIGNificant ticks all the legal boxes of the new regulation:

- **"Intention to sign" –** The behavioral, social and commercial significance of the act of signing by hand is deeply embedded in most cultures. As SIGNificant gives an experience link "ink on paper", the signer implicitly understands that they are entering into a binding transaction. With regard to the new emphasis on the intention to sign in the EU directive, the act of signing demonstrates the willingness of the signatory to be bound by legal obligations.
- **"Uniquely linked to the signatory" –** Due to the wealth of data it includes, especially data that are not visible in a printout (e.g. speed, acceleration and rhythm), a biometric signature is virtually impossible to forge.
- **"Capable of identifying the signatory" –** Signatures are forensically identifiable.
- **"Created using electronic signature creation data that the signatory can, with high level of confidence*, use under his sole control" –** Signers have the highest possible confidence from the closest paper/ink replacement technology and process.

- **"Linked to the data to which it relates in such a way that any subsequent change in the data is detectable" –** This is easily proven from the self-contained PDF document sealed with all the embedded audit trail data necessary.

About xyzmo

IconUK brings best-of-breed Customer Communications Management solutions to the UK, combining some of the leading document management products, services and best practices available globally. Together they cover Electronic Signature, Document Creation, Content Integration and Output Management.

This suite is the most cost-effective and flexible software available in this market and when implemented by our 'business-first' consultants produces outstanding ROI, risk management and customer engagement. Contact IconUK (http://www.icon-uk.net) or xyzmo (http://www.xyzmo.com/) to find out more.