Secure &
Authenticated
Document Manage-
ment:
Not a New Problem

Anno Dominici 808, Karolus Magnus (Charlemagne) rules what is now known as Europe. After having consolidated and pacified the different regions of the empire, Charlemagne needs to strengthen the administration of the empire. Such a large territory requires specific and improved ways of communication, a law system that spans all the territory and a solid and undisputed documentation process.

Charlemagne creates a "central" imperial data repository for official documents in Aachen, designs a unique font to be used for all imperial communication (Karolina) and invents the monogram flanked by a unique header, introducing the first handwritten biometric authentication, guaranteed by a seal (wax).

Since 808 no major changes in official document processing in Europe until October 28, 2008 when French justice signs the first gouvernement backed e-document.
Unique Font.
Through the invention of a "typical" handwritten font, the clerics of Karolus Magnus follow two objectives: firstly ease of reading and clarity, secondly authentication of the document source.

Document Management by Carolus Magnus:
1. Customized and unique document header
2. Customized and unique font system
3. Unique monogram
4. Unique seal

Key elements of document authentication
In the early European Middle Age Carolus Magnus sets the stage for document management:
- handwritten signature, monogram, font and unique seal.
In order to authenticate an imperial document, only one seal is available and travels through Europe. It is safe but very slow.
The most valuable asset an organization has is its information or knowledge base. The sharing and access to information and knowledge is critical. Facilitating the exchange of information and knowledge between and within departments is an essential step to integrating an organization's knowledge base.

The successful delivery of Electronic Document Management (EDM) is a primary objective of modern e-management and its successful introduction depends on the users trusting these services and the privacy of the personal data.

The need to share information throughout the enterprise has created an inefficient and costly workflow. At each step, a department takes information from a form and then physically amends that information or data into a new and unique system creating a new entry containing the same information that was originally entered. These redundancies create productivity, time and cost inefficiencies at each level of the enterprise.

The measurable cost inefficiencies are staggering, the Bureau of Labor Statistics of the USA estimates that it costs an organization an average of USD 20 an hour just to process data. Reason for doing these redundant tasks may be summarized as follows:

1) Legal signatures that are needed for authentication.
2) Privacy and security concern.
3) Data and document integrity.
4) Each entity establishing its control and identity.

Assumptions (USA Bureau of Labor)

1. Cost of data entry is $1.50 per entry, (this is a labor cost).
2. Cost to fill forms is $1.50 per form, (this is a labor cost).
3. Cost is $20 per form or case copied, (this includes labor and material costs).
4. The cost to scan and/or archive each form is $1.00 this includes labor and material costs.
5. Sending costs is $50 per each form sent, (handling and actual shipping costs).
ASDE allows departments to work together effectively. The gap between islands can be effectively reduced with efficient Authenticated Secure Document Exchange (ASDE) resulting in significant intangible returns on productivity, collaboration and innovation. These types of returns have no real measurement in the immediate (short) term, but in the long term and through the life cycle of the system, these types of returns can be measured by decreased retraining time, reduction in turnover costs and significant productivity gains.


These situations exist when time is lost due to printing, sending, and data entry resulting in monetary and productivity losses. Bridging temporary islands of information is crucial to the short and near term operations of an enterprise.

When making a decision about knowledge management an organization must look at four elements: cost, longevity, effectiveness, and ROI.

Authenticated Secure Document Exchange is the most simplified and cost effective document workflow management solution that can be used by an organization to bridge their islands of information and manage their cost effectively.

StepOver supports these efforts through three combined unique approaches:

- The signature pad authentication device
- The signature software and
- The patented data encryption protocols
Better than Wet Ink!

The signature captured by the signature pad and embedded with the StepOver signature software components basically is identical to a wet ink signature.

The data sensed by the signature pad contains more than image info, speed, pattern and pressure are also capture at high resolution and frequency. This data constitutes a biometric set unique to every individual that cannot be reproduced by a forger.

Managing the Workflow

Four out of five IT professionals say that document management is part of an effective IT strategy, but many haven’t found the right mix of technology and services to capitalize on potential savings or boost worker productivity, according to the survey.

IT departments are spending as much as 40 percent of their time and budget administering document technology, but one-third of those surveyed said their company doesn’t have a handle on the costs associated with it and lacks the tools to minimize spending while meeting the needs of end-users.

Implementing content management software to organize information and help employees collaborate online is top priority.

Document management, electronic records management, imaging capabilities and digital document archiving and storage in secure repositories are methods by which organizations can save time and money.

Staggering Costs of Documents (*)

Four trillion documents are stored in US files. Paper files are doubling every 3.5 years. Average document is copied 19 times each day. One billion photocopies are made. Half of an office workers time is spent handling paper or data entry.

* Source: AIIM, Forrester, Star Securities
** Source Xerox & ICR 2007
User friendly approach

Unlike other biometric technologies such as fingerprints, facial or iris scan, the handwritten e-signature is easier to handle.

Users are less hesitant to sign electronically for completing business transactions rather than using other biometric technologies since signing has already been an accepted form of authentication and authorization since Carolus Magnus.

Data Security

In addition to advantages such as the cultural acceptance of signatures, dynamic signatures also offer some of the best biometrics with respect to uniqueness and repeatability thus sealing transactions in a secure manner and removing any question as to the identity of the signer.
A document processed with StepOver software components is secured better than on paper. Once a dynamic signature has been inserted into a document, the signature data is encrypted and combined with the unique identifier of the signature pad.

The hash created with the document data and the signature features is encrypted and cannot be separated anymore. Attempts to modify the signed document (e.g., PDF or TIFF file) will result in breaking the seal. Sealed documents can no longer be altered without first removing the authorizing signature. In this way, security against post-signing alteration is guaranteed.

The StepOver biometrical signature consists not only of X- and Y-axis components, but of 4-dimensional biometric data by also incorporating the individual pressure and velocity parameters of every signature.
Long Term Protection

Documents which are electronically signed by using StepOver software components are still standard confirmed documents after signing, e.g. a PDF/a document stays a PDF/a document.

In order to ensure long term data readability, StepOver only uses well known and secure industry standard encryption algorithms such as RSA and AES, as well as secure open standard hash functions like SHA512. Source codes of the StepOver software components and method descriptions are usually deposited by a notary for the safety of our users.

All electronic documents which are signed using StepOver software components can be resigned e.g. using a digital mass-signature for long term archive purposes. This works by the Matryoshka principle: There a new signature surrounds the already signed document. The Matryoshka principle allows to over-sign an existing document with a longer or stronger encryption algorithm for future security at a time when the originally used algorithm is still expected to be secure. The need for this procedure results from the fact that the vulnerability of an electronic seal, based on older encryption algorithms raises with the increasing computing power available to a potential attacker. Therefore the Matryoshka principle is the only legal method to extend the validity of an electronic signature beyond the period in which the original seal of the signature is expected to be secure.
The StepOver Signature Pads

Form follows function – something implicit for StepOver – as the pads are designed for the unique purpose of signature. Compared to other devices on the market the StepOver signature pads attracts with a slim and flat design, perfectly fitting different industrial application.

Key Product Benefits

From the first the user feels that surface allows a natural way of signing – like on paper.

Users are signing just as usual. The signature image is displayed promptly throughout the signing process – fast, precise and sharp.

The sensor area signature pad is equipped with an end-to-end sensor offering enough space to cater for long names (such as compound names).

The ball of the thumb can rest on the signature pad surface throughout the signing process.

The writing surface is non reflective and highly resistant to scratches.

Customization

Individual device colors – matching a corporate design – and integrating logos of a company or product are an option for larger orders.
StepOver

Software Components

As the only manufacturer worldwide, StepOver GmbH develops, manufactures and sells both hardware products as well as complete software products for handwritten electronic signature.

Therefore we are in a position to offer signature solutions where the hardware (signature pads) and the software are matched 100% and thus allow “Plug&Sign” in every sense of the word.

In the development of software products for electronic signature it is our goal to provide our customers with software tools as well as complete applications which can be integrated into the existing electronic workflow with a minimum amount of effort.

The software portfolio covers almost all application areas of electronic signature. StepOver provides:

Converters for the creation of tamper proof Tiff and PDF documents from any Windows application with a printing feature.

Simple tools for embedding the signature image of an electronic signature into customer applications.

Programming interfaces to facilitate secure integration of the electronic signature into the customer application.

Plug&Sign eSignatureOffice solution where every possible customer requirement is satisfied, right through to a signature template for recurrent forms.

Adobe PDF-Plugin to support SAP-Interactive Forms and Adobe Live-Cycle Server documents.

StepOver

1st Class Service & Support

Our products are characterised by the highest quality and lowest failure rates – simply “Made in Germany”.

Since we are that convinced of the value of our products, StepOver offers you “real” support instead of impersonal telephone assistance. Our support offer is established in such a way that the demands of major customers and large companies can be fulfilled at all times. In addition to the highest variety of support tools of all manufacturers of handwritten e-signature products, we offer you e.g. direct support of in-house computer operators and developers.

StepOver Information Network

The free StepOver Information Network offers:

All software products for download: StepOver software products can be freely downloaded for testing and integration purposes.

Documentation: All API descriptions, examples and technical/legal aspects.

All information you need: In the Information Network you will find all news and information on StepOver GmbH. You can perform specific searches applying the filters „Software“, „Hardware“ and „General“, and you can register your e-mail address to receive the latest news in the selected categories.
The Company

StepOver GmbH is a company founded in 2001 with head office in Stuttgart and branches in London, Madrid, Minsk and Frankfurt.

It is the leading European manufacturer of hardware and software for handwritten electronic signature. Numerous insurance corporations, banks, industrial, trading and health care companies are conducting paperless business with third parties using StepOver GmbH products.

StepOver’s Unique Position

Features:

As the leading experts for secure signature recording hardware (signature pads) and software, StepOver offers not only ergonomic and high-quality products “Made in Germany”, but also signature devices with the highest possible proof security in the world.

Customer Reference:

More than 100,000 StepOver signature pads are already in use by:

Allianz  
SiXT  
Debeka  
AXIMA  
Versicherungen  
Dräger  
Siemens  
Debeka  
Dräger  
Siemens  
Debeka  
Dräger  
Siemens  
Debeka  
Siegfried  
Gottlieb  
Bosch  
Mühlbauer  
Wüstenrot

Headquarters:
StepOver GmbH
Otto-Hirsch-Brücken 17
70329 Stuttgart - Germany

Info-Hotline:
+49 (0) 711 120 269 30

Our website:
www.StepOver.com