White Paper

Digital signatures from the cloud – Basics and Applications

PDF-TOOLS.COM
Premium PDF Technology

Contents

Basics of digital signature

Electronic documents and signature

In business transactions, electronic documents are being increasingly exchanged and archived as a matter of course in the same way it has been done for a long time with their counterparts in paper form. The paper documents are often provided with handwritten signatures, which give the documents a defined probative value in the applicable law. To ensure that electronic documents can also be signed with the same probative value, the law created the electronic signature.

The advantages of electronic signatures in business processes are obvious:

- Improved performance and quality: They enable documents to be signed automatically in the outbox and signatures to be verified automatically in the inbox.
- Legal security: They enable an improvement of the probative value, in particular the non-repudiation of the data sent electronically.

In the legal texts the characteristics of an electronic signature are described. The texts contain no specifications for the technical implementation, however. For the technical realisation the industry has developed a series of standards which define the concept of a digital signature and describe its characteristics.

Electronic signature

The functions of an electronic signature are as follows:

- **Substitute for a handwritten signature:** An electronic signature can fulfil the requirements of a handwritten signature in the same way as a handwritten signature itself if the legal requirements for this are met.
- **Integrity protection:** Electronic signatures have a "sealing effect" for digital documents.
- **Authenticity:** With an electronic signature it can be ensured that the natural or legal person can be identified.
- **Authorisation:** Rights and authorities can be stipulated in the certificate and managed and can therefore be assigned to the person.

According to the Federal law on certification services and other uses of digital certificates in the area of electronic signatures (ZertES) there are two types of signatures:

- An **advanced electronic signature** (integrity protection and identification of the signatory) can be used for natural and also legal persons and is assigned to an "owner". "Owner" can be a person but also a machine (server). It is not equivalent to a handwritten signature and is suitable in particular for signing digital documents where there are no legal formalities.
- A **qualified electronic signature** (fulfilment of form regulations) is an advanced electronic signature which is based on a secure signature creation device and a qualified certificate valid at the time of creation, issued for a specific person. The certificate also has to come from a recognised provider of certification services. The "owner" is always a natural person.

The Ordinance of the Swiss Federal Department of Finance on electronically transmitted data and information (EIDI-V) regulates areas including the technical, organisational and

procedural requirements for an electronic signature to create and verify VAT-compliant invoices. The Company accounts decree (GeBüV) stipulates that electronic signatures and time stamps can be used for storing documents saved on alterable information media.

For qualified electronic signatures with proof of identity there is SuisseID in Switzerland for natural persons.

Digital signature

As mentioned above, a digital signature is a technical implementation of an electronic signature. It consists of data which is assigned to the signed document. To ensure the characteristics demanded in the legal texts can be guaranteed with certainty, cryptographic procedures are used to create and verify digital signatures.

To create a digital signature the following three things are required:

- A certificate, issued to the "owner"
- A corresponding private key which only the "owner" owns and has to keep protected
- The document which is being signed

With the signature software the "owner" can therefore create a digital signature. The recipient of the document can now verify the digital signature. To do this, the recipient needs the following three things:

- The signed document
- The certificate of the "owner". In general this is embedded in the document itself.
- The digital signature. This is also embedded in the document together with the certificate.

This process can be carried out easily by the recipient with the signature software.

According to the law, the "owner" also needs a signature creation device to create qualified signatures. In technical terms it is an electronic device which keeps the private key safe and protects against external access. In practice, smartcards, USB tokens and HSMs (Hardware Security Modules) are used as suitable devices. For practical reasons these devices also contain the "owner" certificate and the certificates of the issuer as well as the private key. Unlike the private key, the certificates do not need to be protected. They may be published because they are needed to verify the digital signature.

Standards for digital documents and signatures

The most important document standards for signed, digital documents are:

- ISO-19005 (PDF/A): ISO Standard 19005 defines a file format based on PDF called PDF/A. The format provides a mechanism which presents electronic documents in such a way that the visual appearance remains over a long time, independent of tools and systems for production, storage and reproduction. For this reason the document has to contain everything which is needed for perfect presentation (fonts, colour profiles, etc.) and may not refer to external sources either directly or indirectly.
- XML: The format was developed for exchanging hierarchically structured data in text form between machines. The specification is published by the W3C (World Wide Web Consortium).

- EDIFACT: This is an international standard covering different sectors for the exchange of electronic data in business transactions. EDIFACT is one of several international EDI Standards. A UN agency is responsible for the EDIFACT Standard.

The ETSI has developed standards for the data structures of digital signatures which meet the requirements for advanced and qualified electronic signatures. These are the standards:

- PAdES (PDF Advanced Electronic Signature Profiles)
- CAdES (CMS Advanced Electronic Signatures)
- XAdES (XML Advanced Electronic Signatures)

Digital signatures are mainly used for the following two applications: document exchange and archiving. For the long-term storage of documents, the digital signature has to fulfil additional requirements.
The first requirement concerns the long-term validity check of the certificate. It is called LTV (long-term validation). On the one hand the ETSI Standards describe measures against attacks on cryptographic procedures which are becoming possible because of the constantly increasing computing power. On the other hand a digital signature with LTV additionally contains the following data:

- Trust chain: The certificate of the issuer including all intermediate certificates which form a trust chain together.
- OCSP response: Data which certify the validity of the certificate through the issuer at the time of the signature.

For the LTV information the OCSP service has to be available at the time the signature is created. For the later verification it is no longer required. This ensures that these signatures can also be verified in the long-term.
For digital signatures without LTV it is the opposite. No service has to be available to create these. The OCSP service has to be accessible for the verification, however.

The second requirement concerns checking the time of the signature. The signature has to additionally contain the following data here:

- TSP response: Data from a time stamp service which certifies the time of the signature.

Without a time stamp, the time of the signature cannot be proven afterwards. The TSP service always has to be available at the time of the signature. No TSP service is required for the verification.

Purpose and uses of the signature service from the cloud

What is the purpose of the service?

The main purpose of a signature service is to create full signature data on account of a signing request of the signature client. The signing request is generated on account of the document which is to be signed on the one hand and the authentication of the client on the other. The service sends the signature data back to the signature client, where they are then connected with the source document for the signed document.

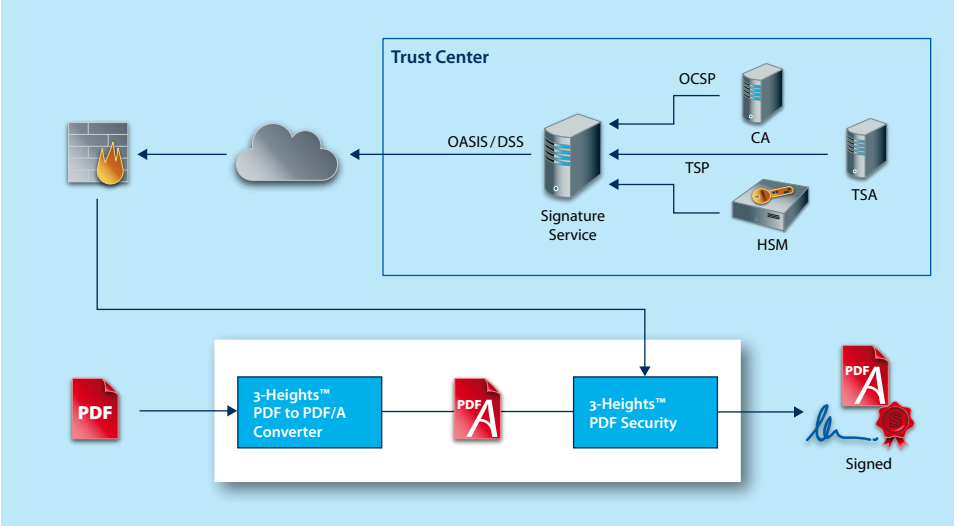


Fig. 1: A central service for creating and verifying digital signatures

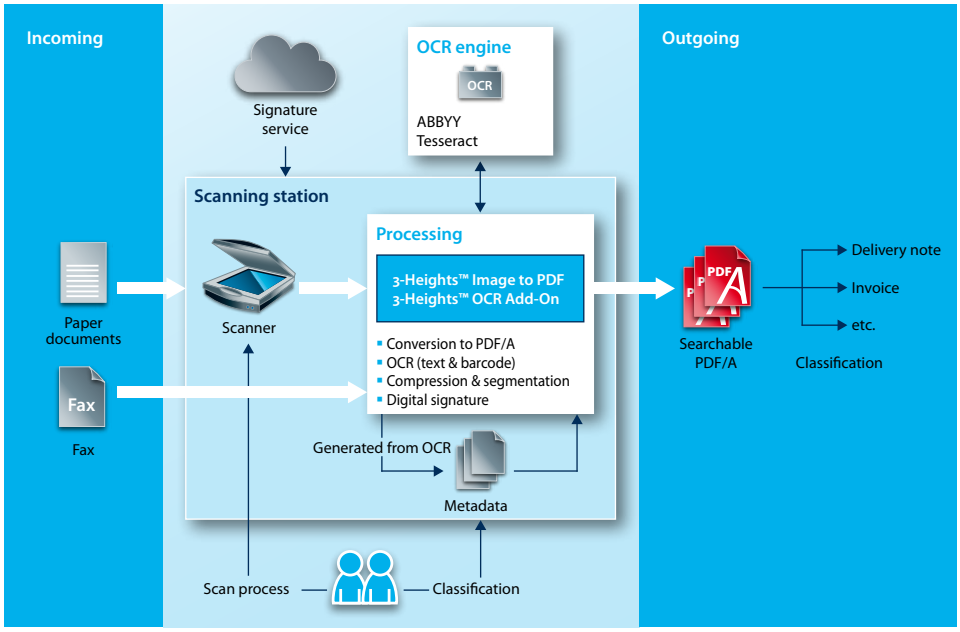
The document itself is not sent to the service but rather a hash value of it (similar to a fingerprint). The content of the document cannot be determined from the hash value. This means the confidentiality of the document remains guaranteed in all conceivable applications such as patient files, banking data, design drawings, etc. The mutual authentication of the client and server and the transaction are via secure connections (TLS). The secure connection is protected by a client certificate and a server certificate. With this measure the service can allocate the signatures clearly to a client.
The service manages the necessary private keys and certificates in a secure and trusted environment for every client. The service therefore creates the individual signatures.
Advanced organisation certificates are supported according to ZertES and ElDI-V and also qualified certificates on the basis of SuisseID. The certificates are renewed automatically by the service when their period of validity expires.
As an option the service can also generate signatures with long-term validity (LTV) and also integrate a time stamp.
High availability is guaranteed by the redundant design of the service. The service is run by an accredited issuer of certificates which guarantees compliance with all relevant regulations.

Where is the service used?

The signature service can be used anywhere in an enterprise where digital signatures are going to be produced or need to be produced. Some typical examples are described in the following.

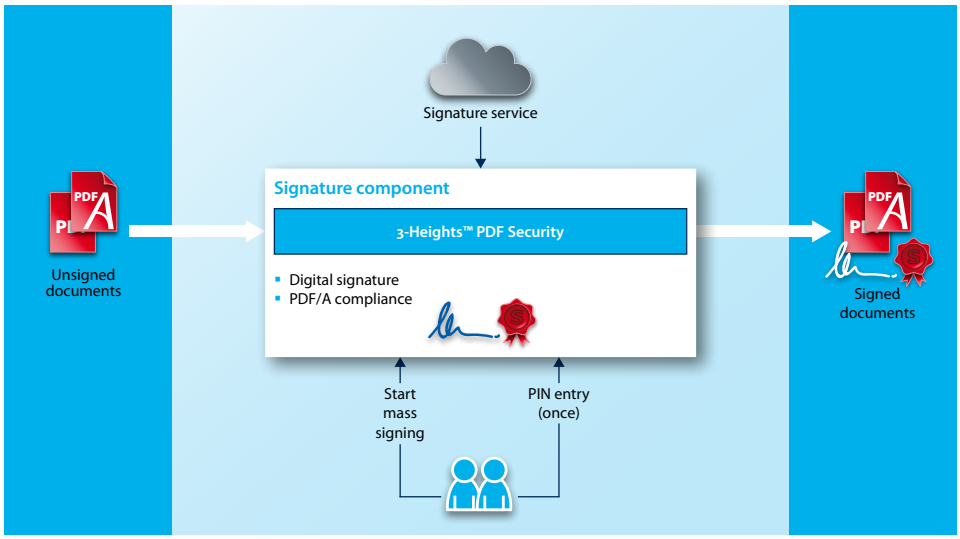
Integrity protection in the inbox

Paper documents which arise in the inbox of an enterprise can be scanned, converted to PDF/A and signed with a time stamp. The same applies for the receipt of the entire FAX communications between the enterprise and its business partners. With this measure the integrity of the received documents is guaranteed in the following processes.



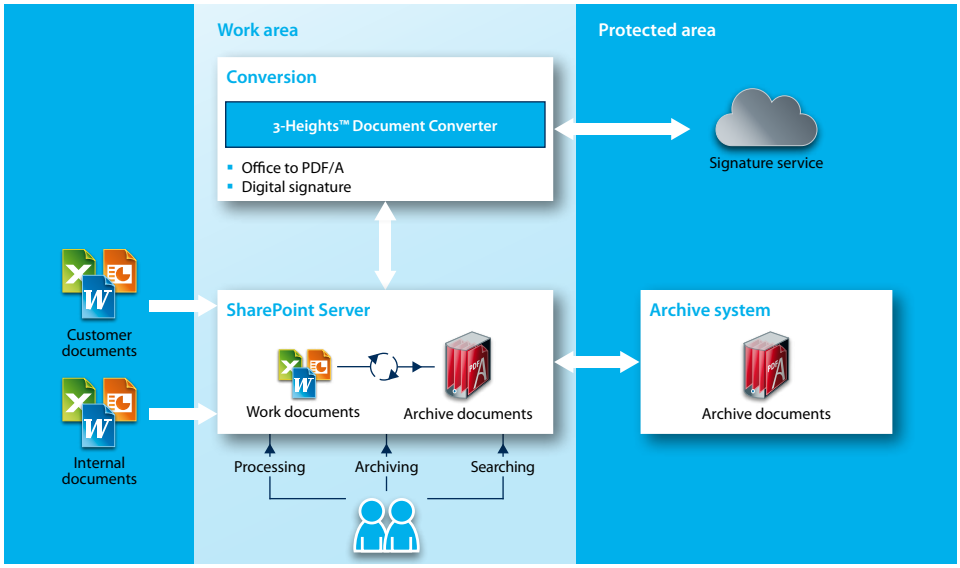
ElDI-V-compliant documents in the outbox

In the outbox, unsigned documents, for example invoices, are converted into PDF/A and provided with an advanced and ElDI-V-compliant signature.



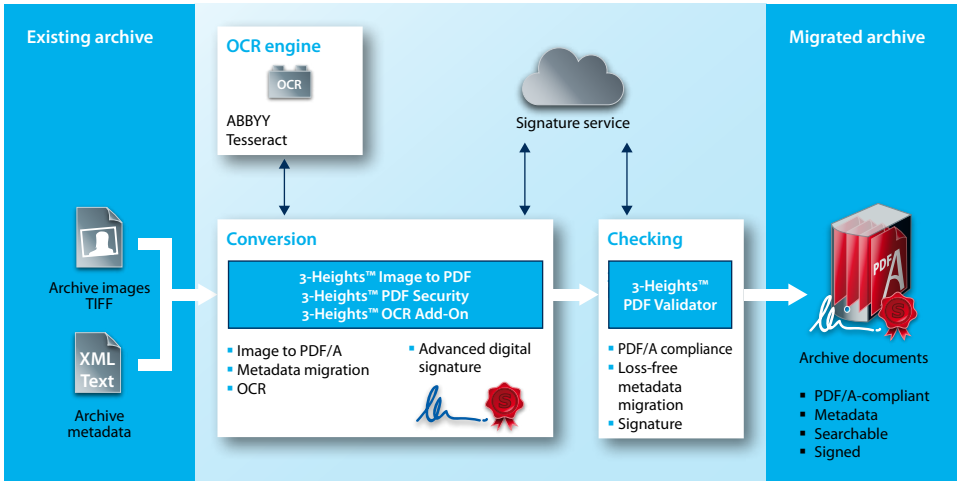
Archiving final work documents

Work documents which have reached the final status in their life cycle and are going to be archived are converted into PDF/A and digitally signed at the same time. The processing of the documents is often supported by a SharePoint Server. With an extension, the conversion into PDF/A and the addition of a digital signature from the cloud can be automated.



Archive migration with traceability

An existing archive with TIFF, JPEG and other images and also separate index data is converted into PDF/A and provided with a signature from the cloud at the same time. The signature guarantees the traceability of the migration.



What are the advantages of a signature service?

The signature service has clear economic and technical advantages over stand-alone solutions. Here is a summary of the most important ones.

Fast implementation time	Setting up a signature infrastructure with server and clients in an enterprise requires know-how, training of staff and time. The use of the signature service considerably reduces this time because it is not necessary to set up a server infrastructure and only the considerably easier signature clients have to be implemented.
Reduction of investment and running costs	Purchases such as HSMs, certificates and tokens for every employee are not required. The costs for running servers and renewing certificates are also not required. Expired certificates can become expensive if they lead to down time.
Ubiquitous presence, independence of location, no tokens	With the signature service, documents and data can be signed everywhere without tokens and card readers having to be available. With the increasing distribution of mobile devices this is often the only possibility of providing electronic signatures. The signatures can be provided via the network, for example from home offices.
Compliance / regulations	The service is run by an accredited issuer of certificates which guarantees compliance with all necessary regulations (ZertES). The service generates both advanced signatures according to EIDI-V and also qualified signatures according to SuisseID.
High availability	With the redundant design of the hardware, the operator of the service guarantees high availability of the service.
High quality, compliance with standards	The provider of the service guarantees the ongoing development and adaptation of the digital signatures to the latest technical industry standards (ISO, ETSI).
Security	The service manages private keys and certificates in a secure and trusted environment. The certificates are renewed automatically by the service when their period of validity expires.
Confidentiality	With the signature service, data and documents with the highest level of confidentiality can be signed because the data never leaves the enterprise for the signature process.
Lower vulnerability	The use of the service increases the robustness of firewall defences as only one single, XML-based protocol is used for the service. Stand-alone solutions need access to several OCSP and TSP protocols which require higher security. The connection between the signature client and the signature service is also protected by mutual TLS authentication.
Scalability	The service can deal with single signing requests up to several million per day.

Table 2: The advantages of a signature service from the cloud

Software for the use of the signature service from the cloud

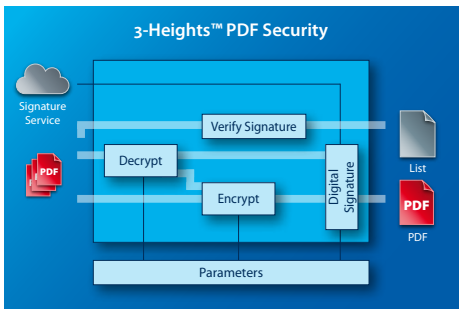
Task of the signature client

The signature client is a software component which can sign data and documents with the help of the signature service from the cloud. The signature client communicates with the service via the OASIS/DSS protocol. It creates correct signing requests, checks the response and integrates the result into the data or document which are to be signed.

The signature client is a component of the products described in the following:

3-Heights™ PDF Security

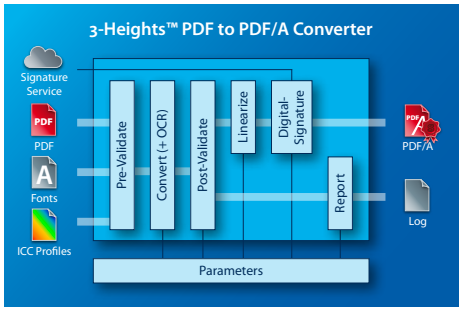
The 3-Heights™ PDF Security component offers two main functions: encryption and digital signature for PDF documents. The "digital signature" part contains:



- PDF and PDF/A-compliant signing (PAdES Part 2)
- Verifying signatures for validity in a PDF document
- User signatures, author signatures (MDP) and time stamp signatures
- Simple, advanced or qualified electronic signature
- Long-term signature (LTV) with embedded trust chain, time stamp and checking information for certificate validity
- Support of signature services from the cloud via OASIS/DSS and mass signature devices (HSMs) via PKCS#11
- Listing and retrieving revisions
- Invisible and visible signatures
- Design of the visible signature

3-Heights™ PDF to PDF/A Converter

The 3-Heights™ PDF to PDF/A Converter is based on the 3-Heights™ PDF Security component and offers the following additional functions:



- Converting PDF documents to PDF/A-1, PDF/A-2 or PDF/A-3
- Validating incoming documents
- Validating outgoing documents
- Automatic and configurable embedding of colour profiles when using device-dependent colour spaces
- Automatic and configurable embedding of fonts: embedding as a subgroup to keep the file size small or embedding entire font to enable the file to be edited later
- Automatic generation of metadata or embedding them from external sources

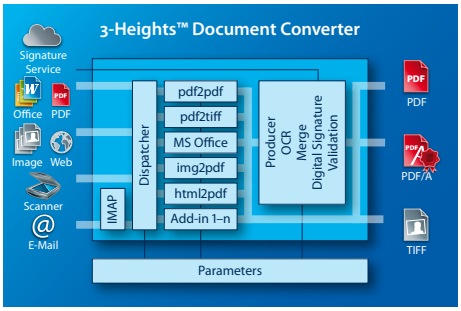
- Connection of an OCR engine (ABBYY or Tesseract) for optical character recognition; optionally saving the recognised text as a text file

3-Heights™ Document Converter

The 3-Heights™ Document Converter is a solution which can be used throughout a company for converting all popular file formats to PDF/A, PDF and TIFF. The most common application is the conversion of Microsoft Office documents to PDF or PDF/A for archiving with optional addition of a signature from the cloud.

Many different requirements in the area of conversion are therefore addressed, in particular:

- Archiving MS Office documents in PDF/A
- Archiving images such as TIFF, JPEG and other image formats
- Archiving websites
- Archiving e-mails
- Standardising the different formats used throughout a company



Interfaces for application integration

A range of interfaces are available for the integration of workstations and server computers that run applications wishing to use the 3-Heights™ products. The most important are:

- **Web service:** The web service allows documents to be signed from the intranet, an application or a mobile device.
- **Application programming interface (API):** This component enables the programmatic integration of the service into applications. It offers interfaces for Java, C, COM and .NET technologies. The component is also available for other platforms, including Linux, Sun OS, AIX, HP-UX, Mac OS/X, etc.
- **Command line tool:** This tool is a stand-alone program that can be run directly from the command line without any other requirements. A command language (shell command) can then be used to automate processes without the need for a development environment. The command line program is also available for other platforms, including Linux, Sun OS, AIX, HP-UX, Mac OS/X, etc.

Glossary

Terms

Hash	A hash value (hash for short) is a number which is calculated from any quantity of data such as documents, certificates, messages, etc. This number is often much shorter than the original data (approx. 20 bytes). The hash value has the characteristic that it is the same for the same data and is almost certainly unique for different data. The original data can also not be determined from the hash value. For the calculation hash algorithms are used such as SHA-1 or SHA-2.
Key	The certificate contains a public key which is used to verify the signature. The public key has to match a private key which is used to create the signature and has to be kept in a safe location.
Signature, signing	Data with which the integrity and authenticity of a document can be ensured. The signature is essentially made as follows: the hash value is formed from the data which is to be signed and this is encrypted with the private key. The signature is packed into a CMS message together with certificates and checking information and as an option is embedded in the signed document.
Token	A "container" (part of the HSM, USB stick, smartcard, etc.) which contains private keys and protects against unauthorised access. For practical reasons the token often also contains corresponding certificates and public keys which do not need to be protected.
Verification, verifying	A signature is verified as follows: the signature is extracted from the document and decrypted with the public key. From this comes the hash value of the data at the time of signature. Afterwards the hash value of the signed data is formed again and compared with the hash value from the signature. If the two values correspond, the data have not been changed and are trusted (integrity check). From the signature message the certificate can also be extracted and the signatory can therefore be identified (identity check). Other checks regarding certificate validity and the time stamp are possible depending on the type of signature.

Encryption	Data are encrypted so that outsiders cannot deduce their meaning. For the communication between sender and recipient, the recipient generates a key pair consisting of a private and a public key. If the sender now encrypts the data with the public key, only the recipient can decrypt the data because the recipient remains the sole owner of the private key. For the encryption, algorithms like RSA with key lengths of currently 2048 bits are used. The usual procedures for digital signatures are based on this technology
Certificate	A certificate is an electronic certification of the identity of a natural or legal person. The certificate also contains a public key for which the person possesses a corresponding private key. With this private key the person can generate digital signatures. Any person can verify this signature with the help of the certificate.

Abbreviations

ASN.1	**Abstract Syntax Notation #1:** Description language for the syntax of digital messages. For the binary encoding of the messages suitable standards are used here (e. g. X.690).
BER	**Basic Encoding Rules:** Easy to handle rules for the binary encoding of digital messages.
CA	**Certification Authority:** Accredited issuer of certificates.
CAdES	**CMS Advanced Electronic Signatures:** An ETSI Standard for the standardisation of CMS-based digital signatures.
CMS	**Cryptographic Message Syntax:** Message format for digital signatures based on the ASN.1 syntax (also often called PKCS#7).
CRL	**Certificate Revocation List:** List of revoked certificates published by the issuer.
DER	**Distinguished Encoding Rules:** Rules for the binary and unique encoding of digital messages based on BER.
EDIFACT	**Electronic Data Interchange For Administration, Commerce and Transport:** An international standard covering different sectors for the exchange of electronic data in business transactions.
EFD	**Swiss Federal Department of Finance:** The Swiss authority informs about structure, tasks and about current financial administration themes.

ETSI	**European Telecommunications Standards Institute:** European organisation for the standardisation of digital signatures etc.
HSM	**Hardware Security Module:** Device for securely saving private keys and also for encryption and decryption.
ISO	**International Standards Organisation:** International organisation for the standardisation of PDF and PDF/A, etc. Switzerland is represented in the ISO by the Swiss Standards Body (SNV).
LTV	**Long-Term Validation:** Enhancement of digital signatures with additional data so that long-term verifiability is possible without online services. The additional data consist of the trust chain of the certificates from the owner certificate up to the root certificate of the issuer and also information which certifies the validity of the certificates at the time of signature.
OASIS/DSS	**Organization for the Advancement of Structured Information Standards / Digital Signing Services:** A standard of the OASIS organisation for signing services based on the XML syntax.
OCSP	**Online Certificate Status Protocol:** Protocol for the online query of the validity status of a specific certificate based on the ASN.1 syntax.
PAdES	**PDF Advanced Electronic Signature Profiles:** An ETSI Standard for the structure of CMS signatures and their embedding in PDF documents.
PDF	**Portable Document Format:** A file format standardised by ISO (ISO-32000) for document exchange. For frequent PDF applications there are special sub-standards such as PDF/A (ISO-19005) for archiving digital documents.
PIN	**Personal Identification Number:** Secret code needed for access to a token.
PKCS	**Public Key Cryptography Standards:** A series of proprietary standards of RSA Security Incorporated. The most common standards are: encryption of signatures (PKCS#1), message format for signatures (PKCS#7), interface to token (PKCS#11) and file format for keys and certificates (PKCS#12).
QES	**Qualified Electronic Signature.**

TLS	**Transport Layer Security:** Further development of Secure Sockets Layer (SSL), a hybrid encryption protocol for secure data transmission on the internet.
TSA	**Time Stamp Authority:** Accredited provider of time stamp services.
TSP	**Time Stamp Protocol:** Protocol for the online retrieval of cryptographic time stamps based on the ASN.1 syntax.
XAdES	**XML Advanced Electronic Signatures:** An ETSI Standard for the creation of signatures and their embedding in XML data.
XML	**Extensible Markup Language:** Format for the exchange of hierarchically structured data in text form between machines.
X.509	ITU-T Standard for a public key infrastructure to create digital certificates based on the ASN.1 syntax.
X.690	ITU-T Standard for encoding digital messages based on the ASN.1 syntax: Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

About PDF Tools AG

PDF Tools AG counts more than 4,000 companies and organizations in 60 countries among its customers, making it one of the world's leading producers of software solutions and programming components for PDF and PDF/A products.

Dr. Hans Bärfuss, founder and CEO of PDF Tools AG, began using PDF technology in customer projects more than 15 years ago. Since then, the PDF and PDF/A format have evolved into a powerful, widely used format and ISO standard that can be used for almost any application. During this time, PDF Tools AG has developed into one of the most important companies on the market for PDF technology, and has played a significant part in developing the PDF/A ISO standard for electronic long-term archiving.

As the Swiss representative on the ISO committee for PDF/A and PDF, the company's knowledge flows directly into product development. The result is high quality, efficient products based on the 3-Heights™ philosophy of the development team, which consists of experienced engineers.

The portfolio of PDF Tools AG ranges from components to services through to solutions. The products support the entire document flow, from raw materials to scanning processes through to signing and storage in a legally compliant long-term archive. An advantage of the components and solutions is the broad range of interfaces, which ensure smooth and easy integration into existing environments.

Due to the growing demands of the market, the products are enhanced and refined continuously. Support is provided by the developers themselves, allowing them to identify trends and customer requirements quickly and use this knowledge when planning enhancements and components.

All development activities are performed in-house at PDF Tools AG in Switzerland. The company does not outsource any programming, so that the entire development process can take place centrally in a single location. This helps to ensure the high standards expected by the company, particularly with regard to the 3-Heights™ technology.

The effectiveness of this approach is confirmed by the success of the products on the market. Our customers include well-known global companies from every industry. That is the greatest compliment of all – and the perfect motivation to continue shaping the world of PDF and PDF/A.

PDF Tools AG | Kasernenstrasse 1 | 8184 Bachenbülach | Switzerland
Tel.: +41 43 411 44 51 | Fax: +41 43 411 44 55
pdfsales@pdf-tools.com | www.pdf-tools.com

PDF-TOOLS.COM
Premium PDF Technology

Whitepaper-Signature_Service-EN-20140630