eInvoicing: Requirements and Fundamentals

Applies to:

EDI (eInvoicing) requirements and fundamentals and SAP NetWeaver Exchange Infrastructure.

Summary

This article examines the legal and technical fundamentals of exchanging electronic bill statements.

Authors: Wolfgang Decker, Marco Freischlag

Company: SAP Systems Integration AG

Created on: 22 June 2007

About the Authors

Wolfgang Decker is a senior consultant in the area of SAP NetWeaver EAI Consulting.

Marco Freischlag is a consultant in the area of SAP NetWeaver EAI Consulting.

Table of Contents

eInvoicing: Exchanging Electronic Invoices

eInvoicing is the procedure for electronically transmitting invoices between business partners. The sender and recipient have to agree a uniform standard for the syntax and semantics of the data they wish to exchange. EDI standards are available for this purpose. Companies can use point to point connections or internet-based technologies to transmit electronic invoices.

According to estimates by the German retail sector, approximately one billion invoices are issued in Germany every year. This brings with it a considerable – and cost-intensive – need for communication between business partners. An efficient invoicing process is therefore very important. Consequently, procedures for electronically transmitting invoices between business partners have now been adopted as best practice methods in many industries. Rapid and secure communication of electronic business data creates potential for rationalization through:

- Reduced handling costs (cost of printing and mailing)
- Faster incoming payments due to shorter delivery times
- Increased process security due to fewer sources of errors (for example, loss of mail)
- Use of EDI standards (Electronic Data Interchange – standardized electronic exchange of messages)

This article will first examine the legal fundamentals of exchanging electronic invoices in Germany and then introduce the EDI standards that are commonly used. It will conclude with an illustration of the implementation of the eInvoicing process, using the consumer products industry as an example.

Legal Regulations

German Sales/Purchases Tax Law (UStG)

The German Sales/Purchases Tax Law (UStG) defines the legal requirements an invoice document must meet so that it can be recognized for tax purposes and be eligible for input tax deduction. The German Sales/Purchases Tax Law was amended on 15 December 2003 and now conforms to the EU Invoice Directive. The regulations for exchanging billing information electronically were amended at the same time. These changes were communicated in a document published by the German Federal Finance Ministry on January 29, 2004 [Schreiben des Bundesministeriums für Finanzen vom 29.01.2004].

The following requirements must now be met when invoices are exchanged electronically:

- The recipient must agree to receive invoices electronically. This agreement does not require a specific format. It can be part of an outline agreement, but tacit approval is also sufficient.
- Within a reasonable period, the tax office must be able to verify the procedure that was used to electronically transmit an invoice (Section 145 of the General Requirements for Accounting and Recording in Germany (AO)). This assumes that the procedure complies with the requirements of the German Principles of Proper Computer-Based Accounting Systems (GoBS).
- When electronically transmitted invoices are checked, the German Principles of Data Access and Verifiability of Digital Documentation (GDPdU) must be observed.
- The authenticity of origin and the integrity of content must be ensured for electronic messages. This can be done in two ways:

  -With a qualified digital signature or with a qualified digital signature from an accredited certification authority in accordance with the German Electronic Signature Act.

  Multiple invoices may be grouped together in one file and sent to the recipient with just one qualified signature.

  -Using EDI with a collective invoice, which is sent electronically and on paper (usually by fax).

  -Since April 1, 2001, the previously most common practice of sending invoices automatically using a fax server has no longer been permissible. Legislation requires that invoicing must involve an explicit act of will. The collective invoice must therefore be transmitted using a standard fax device.

  In order for the invoice to be eligible for input tax deduction, the invoicing party and the invoice recipient must each keep one printout on paper.

  Alternatively, the collective invoice can be sent electronically, as long as it has at least one qualified electronic signature.

German Digital Signature Act (SigG)

In 1997, Germany became the first member state of the European Union (EU) to pass legislation regarding digital signatures (German Digital Signature Act SigG). In December 1999, the European Union issued a directive on general conditions for electronic signatures within the EU. The German Digital Signature Act was then amended in the light of this directive and the amendment took effect on May 1, 2001. The accompanying Signature Ordinance was issued by the German federal government on November 16, 2001.

A digital signature must meet the following requirements to make it a binding professed intention:

- **Authenticity**

  Unequivocal identification of business partners, that is, the specified sender corresponds with the actual sender, who cannot deny this should a legal dispute arise.

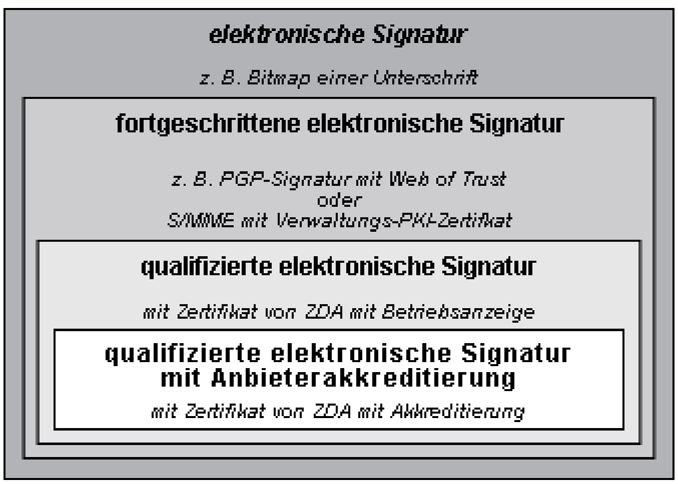
- **Integrity**

  Integrity of the information transmitted, that is, the data that is received corresponds with the data that was sent and was not changed.

- **Indisputability of origin**

  Unambiguous proof that the message was actually sent by the sender

The German Digital Signature Act differentiates between the following, in line with the EU Digital Signature Directive:



Simple Digital Signatures

A simple digital signature serves to authenticate the owner. However, it consists only of electronic data, which is added to other electronic data. It is not possible to explicitly assign the signature to the person who created the document. Its value as proof is therefore minimal. A simple digital signature is suitable for informal contracts only.

Advanced Digital Signatures

While a **simple** digital signature is used for **authentication**, that is, for determining the sender, the advanced digital signature guarantees the **integrity** of a message.

It provides a higher level of security compared to a simple digital signature, as:

- the signature key is allocated exclusively to its owner.
- it enables the identification of the signature key owner.
- the tools for creating it are under the sole control of the signature key owner.
- it is linked to the data it refers to in such a way that any subsequent changes can be detected.

Qualified Digital Signatures

A qualified digital signature is an advanced digital signature based on a certificate that is valid when the signature is created.

Qualified certificates are issued by certification service providers (CSPs). They certify that the signatory is authentic by confirming that the signatory is the owner of the public key. The certificate is issued for a limited validity period and the CSP must make it available on publicly accessible communication connections at all times.

The certificate may only be issued for natural persons. It is possible to authorize one or more natural persons within a company to sign for that company.

A Secure Signature Creation Device (SSCD) is required for the creation of digital signatures. Any technical procedure (e.g. smart card, “Kryptobox”) is permissible, as long as it conforms to the requirements of the German Digital Signature Act. The invoicing party can also sign the invoices using an automated mass process.

It is possible to revoke certificates before they expire (e.g. if the smart card is lost). CSPs publish lists of revoked certificates (CRL = Certificate Revocation Lists) on their websites.

CSPs must conform to the requirements of the German Electronic Signature Act (SigG) and the Ordinance for the German Electronic Signature Act (SigV) in regard to operation, the creation, awarding and revocation of certificates, liability, compulsory cover and data protection.

Qualified Digital Signatures from an Accredited Certification Authority

Qualified digital signatures from an accredited certification authority are provided by CSPs that have (voluntarily) gained accreditation from an accrediting body. The accrediting body in Germany is the Federal Network Agency (Bundesnetzagentur), which also regulates telecommunications and the postal service (RegTP).

Accredited CSPs receive a qualified certificate from the regulating body. It certifies that their software and hardware complies with the required technical safety standards. The authority must make this certificate available at all times on publicly available communication connections.

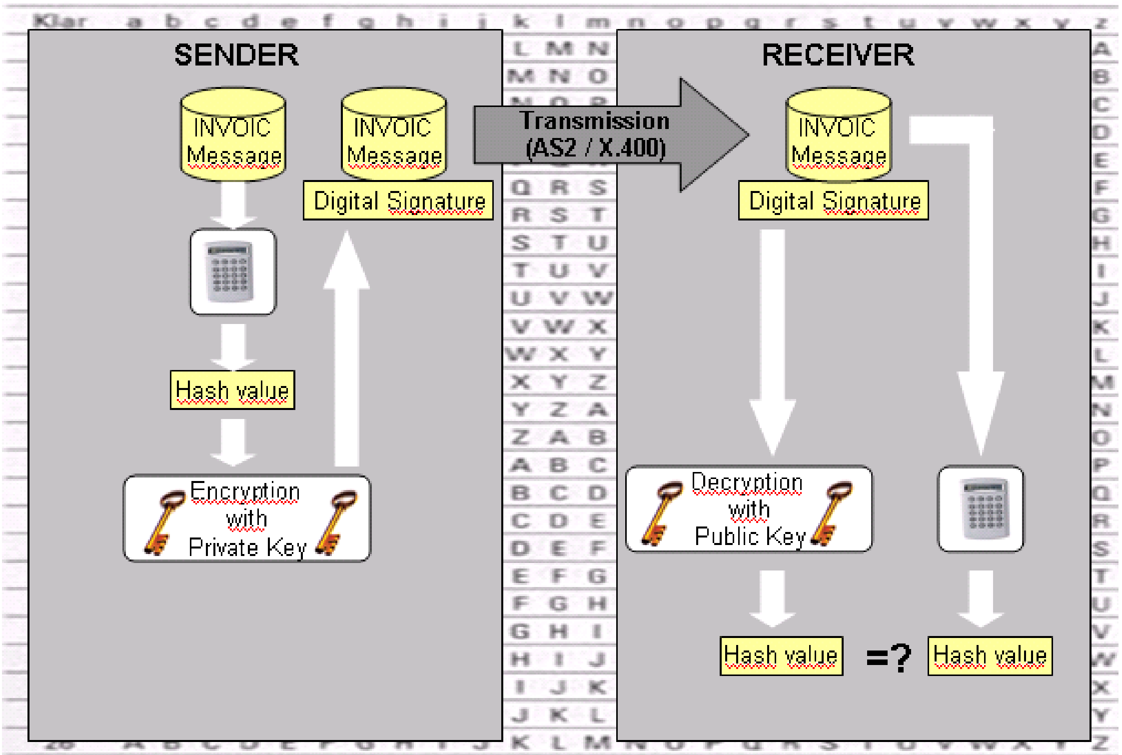
A list of the CSPs currently accredited in Germany is available on the website of the Federal Network Agency (Bundesnetzagentur).

Qualified digital signatures from an accredited certification authority are required in the legal sector, where credibility is especially important.

Digital Signatures: The Technical Process

In Germany, the law permits companies to either create the capacities for using digital signatures themselves, or to transfer this task to a third party. Senders and recipients may use the same service provider.

If the company does not use a service provider, the process is as follows:



Sender's Process

Digital signatures are created using an asymmetric process, which means that public and private keys are used in pairs.

The sender (invoicing party) uses a mathematic compression process (hashing) to create a checksum of the unencrypted INVOIC message. This checksum is encrypted using the sender's private key and then transmitted to the recipient along with the unencrypted data.

The checksum must be created using a Secure Signature Creation Device (SSCD), which is usually a smart card. As qualified digital signatures require a certificate, and this in turn can only be issued by a natural person, that natural person has to release the smart card by entering a PIN.

Recipient's Process

The recipient is provided with the invoicing party's public key. The recipient can authenticate qualified digital signature by using the CSP's certificate before using the public key.

If the signature is a qualified digital signature from an accredited certification authority, the authenticity and credibility of the CSP is certified by an accreditation body. This certificate is also available for verification.

Once the certificate has been verified successfully, the recipient of the invoice applies the sender's public key to the digital signature to decrypt the message.
This results in the checksum determined by the sender. Then the recipient determines another checksum from the unencrypted data.

If the two checksums are the same, this means that the digital signature is valid, which in turn means that the sender is verified as authentic and the transmitted data has not been tampered with.

EDI standards

Standards Enable Electronic Communication

The sender and recipient have to agree a uniform standard for the syntax and semantics of the data they wish to exchange in order to be able to communicate electronically. Existing EDI standards are available for this purpose.

In many industries (automotive, consumer goods), EDI has been the standard procedure for many years. The automotive industry, for example, considers the ability to exchange EDI data as an essential criterion when selecting and assessing suppliers.

For historical reasons, there are many EDI standards, which can apply nationally, internationally, within industries or industry-wide. This has made the interoperability between business partners difficult.

Together with UN/EDIFACT, the United Nations has now published an international industry-wide standard for exchanging structured business data.

Application-Specific Interpretations (Subsets) in Different Industries

The UN/EDIFACT standard messages are highly generic and complex, as they have to meet the process requirements of as many industries as possible. In order to reduce this complexity and adapt the standard messages to individual industry requirements, some industry organizations have developed specific subsets and application descriptions. Subsets are parts and interpretations of the UN/EDIFACT standard.

Examples include the ODETTE subsets for the automotive industry, EDIFICE for the electronics industry and EANCOM® for the consumer products industry.
EANCOM® was developed by GS1, a union of national consumer products industry organizations. EANCOM® 2002 is the 4th release of this subset.

EANCOM® 2002 is based on the EDIFACT syntax version 4 and supports digital signatures. EANCOM® 2002 contains the INVOIC message type for exchanging billing information electronically.

Some well-known retail companies have formed the EDI Retail Team, a union within the GS1 in Germany. This team has developed recommendations for its members on implementing digital signatures.

Digital Signatures in EANCOM®

Like the signed data, the digital signature and the instructions on the mathematical process used to create the signature must be transmitted to the invoice recipient.

Syntax 4 of the UN/EDIFACT standard offers two ways to do this:

- The digital signature is transported separately, with a reference to the INVOIC message (message type **AUTACK** = Secure AUThentification and ACKnowledgement).
- The digital signature is transmitted as part of the INVOIC message, in service segments as a **header/trailer**.
- The KEYMAN (Security key and certificate management message) message can be used to exchange the key pairs. This message exchange however still has the problem of secure transmission. For this reason, GS1 EDI AK retail does not use this message. Instead, it recommends that the invoicing party transmit the certificate to the invoice recipient via e-mail. The UN/EDIFACT Finance Group for the secure exchange of EDIFACT message also recommends exchanging the key pairs by exchanging a form, rather than using the KEYMAN message. For this reason, this article will not deal with the KEYMAN message in more detail.

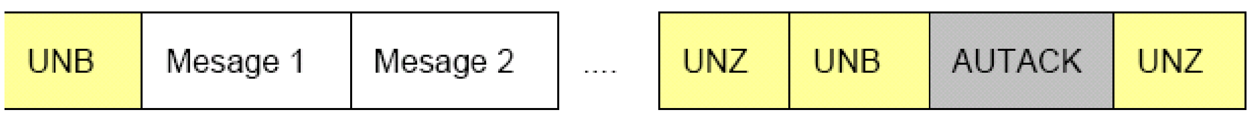
Digital signatures do not affect the choice of transmission protocol (X.400, AS2, etc.).

The AUTACK Message Type (ISO 9735-6)

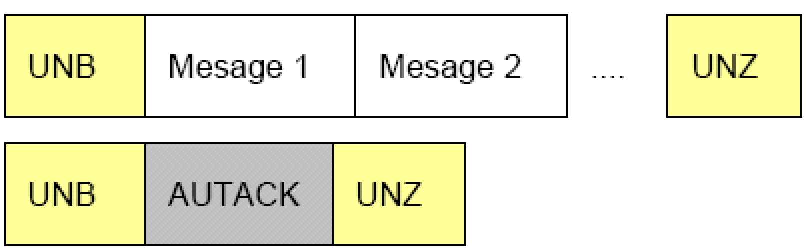
If the AUTACK message is used, two messages are created: the INVOIC message, and an additional message. The structure of the EDIFACT message implies multiple transmission options:

- The AUTACK and INVOIC messages form a shared interchange.

- The AUTACK and INVOIC messages form two separate interchanges within a shared file.



- The AUTACK and EDIFACT messages are transmitted in two separate files.



The invoicing party and the invoice recipient have to agree on a model. GS1 EDI AK retail recommends the transmission in separate files.

This, however, makes the inbound processing by the invoice recipient more complex, as an incoming INVOIC message can only be processed once the corresponding AUTACK message has been received.

The Header/Trailer Approach (ISO 9735-5)

In the header/trailer approach, the digital signature is part of the EDIFACT message. ISO 9735-5 has specified the following service segments:

- USH. Security header segment.
- USA. Reference to the hash function to be used.
- USC. Reference to the certificate that contains the public key.
- USA. Configuration of the encryption algorithm to be used.

- UST. Security trailer.
- USR. Signature.

The signature can refer to the entire interchange or to an individual message.

Segment sequence if the signature applies to an interchange:

UNA	UNB	USH-USA-USC-USA	UNH	Mesage	UNT	UNH	.....	UST-USR	UNZ

Segment sequence if the signature applies to a message:

UNB	UNH	USH-USA-USC-USA	Mesage	UST-USR	UNT	UNH	USH-USA-USC-USA	....	UNZ

Archiving and GDPdU

Auditing methods have been adapted to meet the requirements of the electronic exchange of business data. Since January 01, 2002, the treasury is permitted to audit IT-driven accounting systems by accessing the data. The German Principles of Data Access and Verifiability of Digital Documentation (GDPdU) specify the rules to be observed during data access. They were also communicated in the BMF Statement on Archiving on July 16, 2001 (Schreiben des BMF zur Archivierung vom 16.07.2001).

The retention period is ten years and begins at the end of the calendar year in which the invoice was issued. If the documents are required for taxes, their retention period does not expire until the assessment period for the taxes has expired (Section 147 Para. 3 (3) of the German Fiscal Code (AO)).

According to the German Sales/Purchases Tax Law, a qualified digital signature is part of the electronic settlement. If a company has electronically transmitted invoices, it must provide the invoice as well as proof of the authenticity and integrity of the data (i.e. the qualified electronic signature), even if the validity of this proof has expired in accordance with other regulations.

When a digitally signed electronic invoice is received, the following components have to be archived:

- Encrypted and unencrypted EDI message
- AUTACK message (if used)
- Public Key certificate of the invoicing party
- Result of the signature verification by the recipient
- Source and target file if converted into an INHOUSE format (e.g. SAP Idoc). The source and target file must be maintained in the same index.
- Protocols on transmission, conversion and archiving

Archived electronic documents must be available at all times. It must be possible to evaluate them automatically, and to make them readable immediately. Subsequent changes are not allowed for any reason.

Additional Information

EDI Standards:

GS1: EANCOM 2002®

Empfehlung der GS1 zur Verwendung digitaler Signaturen (Recommendations by GS1 on using digital signatures)

UN/EDIFACT

Legal regulations:

BMF Schreiben vom 29.01.2004 (BMF statement of January 29, 2004)

Bundesnetzagentur als Akkreditierungsstelle (The Federal Network Agency as the accrediting body)

Up-to-date list of voluntarily accredited certification bodies in Germany

GDPdU:

Frage- und Antwortenkatalog zu den GDPdU (Quelle:BMF) (FAQs on the GDPdU (Source: BMF)

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (Principles for Data Access and Verifiability of Digital Documents) BMF statement of July 16, 2001

Abgabenordnung (AO) (German Fiscal Code)

Bundesnetzagentur (Federal Network Agency)

General Information

Signaturrecht (Digital signature legislation)

Copyright