CEN

WORKSHOP

AGREEMENT

CWA 15579

December 2007

ICS 35.240.99

Supersedes CWA 15579:2006

English version

E-invoices and digital signatures

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No.:CWA 15579:2007 D/E/F

Contents

Foreword

This CWA is part of a set of CWAs which has been prepared by the CEN/ISSS Workshop on Interoperability of Electronic Invoices in the European Community, with the view to supporting the effective implementation of the related Council Directive 2001/115/EC of 20 December 2001, with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of Value Added Tax, as well as regulations on electronic signatures and EDI. The set of CWA is as follows:

- Commission Recommendation 1994/820/EC October 1994, proposed revision with the requirements of Directive 2001/115/EC, present day e-Commerce practices and revised definition of EDI Electronic Data Interchange
- The list of invoice content details expressed as UN/CEFACT Core Components
- Recommendation to allow coded identifiers as an alternative to the current unstructured clear text identifications.
- A standardised set of codes with definitions to replace plain text clauses in eInvoice messages.
- Survey of VAT Data Element usage in the Member States and the use of codes for VAT Exemptions.
- eInvoices and digital signatures.
- Storage of Electronic Invoices.
- Guidelines for e-Invoicing service providers.
- eInvoice Reference Model for EU VAT purposes specification

An executive summary of these CWAs is available at:

ftp://ftp.cenorm.be/PUBLIC/e-Invoicing/CWA/Executive_Summary.doc

This CWA summarizes findings and issues identified by the e-Invoicing Focus Group set up by CEN/ISSS regarding electronic invoicing using electronic signatures. Issues surrounding electronic signatures relating to e-Invoicing and VAT in relation to the Council Directive 2001/115/EC are covered, which had to be implemented by Member States by 1st January 2004. Council Directive 2001/115/EC, details the requirements on taxable persons and their service providers to guarantee the integrity and the authenticity of electronic invoices for VAT purposes.

Electronic signatures are a valuable technique to ensure the integrity and authenticity of electronic business data such as invoices. This value, which is based on electronic signatures – under certain conditions – providing integrity and authenticity assurances regardless of time and type of electronic (transport or storage) medium, has been recognized within the EU through the e-Signature Directive, as well as more recently through Council Directive 2001/115/EC where they are one of a limited set of compliance options for sending and storage of electronic invoices.

NOTE: compared to the previous version of this document, a few changes have been brought in section 5.7.1 and 5.7.2 and an annex I.7 has been added. This current version overrides the previous one dated of July 2006.

The final review/endorsement round for this CWA was successfully closed on 6th November 2007.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN : AENOR, AFNOR, ASRO, BDS, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Introduction

According to the Council Directive 2001/115/EC invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed. This could be guaranteed by means of an advanced electronic signature within the meaning of Article 2 (2) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; Member States may ask for the advanced electronic signature to be based on a qualified certificate and created by a secure signature-creation device, within the meaning of Article 2(6) and (10) of the aforementioned Directive.

Although many technologies exist that may be called 'advanced electronic signatures'. In practice, the more widely used Advanced Electronic Signatures in an EU context are typically Public Key Infrastructure (PKI)-based digital signatures using the X.509v3 standard, which have been issued by a Certification Authority using a minimum set of rules and agreements to ensure compliance with the four-part EU definition. At least digital signatures based in X.509v3 certificates should be accepted by all Member States. EESSI standards should be adopted as common technical interpretation, instead of creating new standards, to foster interoperability.

Authenticity and integrity are the sole and clear requirements of the Invoicing Directive for electronic invoices. In addition, Directive 2001/115/EC clearly states “*Member States shall not require invoices to be signed*”, thus excluding giving signatures, even qualified electronic signatures, the meaning of “content commitment”, as per TECHNICAL CORRIGENDUM 3 to ISO 9594-8: 2001. Following this intention it has to be indicated that this requirements can be fulfilled by any electronic invoice, may it be signed by a legal or a physical person. Both scenarios are possible.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the present document are to be interpreted as described in RFC 2119 [10].

1 Scope

Electronic signatures play a major role in electronic invoicing – for transmission of invoice data by EDI or non-EDI - to guarantee authenticity of the origin and integrity of the contents of the invoices. Member States may ask for advanced electronic signature to be based on a qualified certificate.

In this document questions regarding the adoption of electronic signatures for electronic invoicing are discussed. It should help the reader to implement and integrate its software or hardware solutions for signing and verifying its e-invoices regarding the legal requirements.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies."

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[2] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax

[3] ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES)

[4] ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

[5] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8: 2001 – Information technology – Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

[6] ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2001 – Information technology – Open Systems Interconnection – The Directory: Selected attribute types

[7] ITU-T Recommendation X.521 (2005) | ISO/IEC 9594-7:2001 – Information technology – Open Systems Interconnection – The Directory: Selected object classes

[8] ETSI TS 101 862: Qualified Certificates profile V1.3.2 (2004-06)

[9] IETF RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[10] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".

[11] IETF RFC 2104: “HMAC: Keyed-Hashing for Message Authentication”

[12] ETSI TS 102 734: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)

[13] ETSI TS 102 904: Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Advanced electronic signature: an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain 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;

Note: Definition taken from the Directive 1999/93/EC

Authentication: the mechanism that verifies that a person or a process is the stated person or process.

Certificate Policy: certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (ISO/IEC 9594-8:2001) [5] Each CP is assigned a unique Object Identifier – ID by an authorised entity.

Certification authority: a body trusted by all users to create and assign (public key) certificates.

Digital signature: data appended to or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit and protect against forgery (ISO/IEC 7498-2).

Electronic Signature: data in electronic form that are attached to or logically associated with other electronic data and which serve as a method of authentication (Directive 1999/93/EC).

European Telecommunications Standards Institute: an independent, non-profit organization, whose mission is to produce telecommunications standards (www.etsi.org).

Grace period: time period which permits the certificate revocation information to propagate through the revocation process to relying parties (ETSI TS 101 733).

Hardware Security Module: Hardware security module means the cryptographic module used to securely store the private key and generate the advanced signature in electronic invoices. It may generate the key pair itself or it may securely import a private key securely generated in a secure environment, e.g. another HSM.

Internet Engineering Task Force: “The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet”; (http://www.ietf.org/overview.html).

Internet Service Provider: a company who provides users with direct connection to the Internet via either leased or bought direct connections or dialup telephone connections.

Keyed Hashing for Message Authentication: a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key.(RFC 2104).

Private key: in an asymmetric public key cryptosystem, that key of an entity's key pair which is known only by that entity.

Public key: A Public Key is (1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. …..

Qualified Electronic Signature: an advanced electronic signature based on a qualified certificate and created by a secure signature-creation device.

Qualified Certificate: means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II in the Directive 1999/93/EC.

Signature Creation Data: see “Private key”.

Security Policy: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources (RFC 2828).

Static non modifiable document: electronic document drafted in such a way that its content is not modifiable during the access and storage phases, as well as is immutable in the time; to this purpose the electronic document shall not have macro instructions or executable code, capable to activate functions that can modify acts, deeds or data represented in the same document.

Time Stamping Authority: authority which issues time-stamp tokens.

Time Stamp Token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AdES	Advanced digital electronic signatures
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certification Revocation List
ETSI	European Telecommunications Standards Institute
HMAC	Keyed Hashing for Message Authentication
HSM	Hardware Security Module
ISO	International Standardisation Organisation (www.iso.org)
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
IT	Information Technology
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptographic Standards (www.rsa.com/rsalabs/node.asp?id=2124)
QES	Qualified Electronic Signature
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
TSA	Time Stamping Authority
TST	Time Stamp Token
XAdES	XML Advanced Electronic Signature
XAdES-C	XAdES with Complete validation data
XAdES-X	XML Advanced Electronic Signature with eXtended validation data
XAdES-X-L	XAdES-X with complete validation data information provides for long-term validity
CAdES	ASN1 Advanced Electronic Signature
CAdES-C	CAdES with Complete validation data
CAdES-X	ASN1 Advanced Electronic Signature with eXtended validation data
CAdES-X-L	CAdES-X with complete validation data information provides for long-term

3.3 Key words

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "SHALL", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

4 Issuing and receiving electronically signed invoices

This chapter gives an overview about the need for electronic signatures for e-invoicing and its legal environment within the European Union. The basic e-invoicing workflows (receiving and issuing e-invoices) are analysed regarding e-signatures. The major parts and parties involved in these e-invoicing workflows are described in more detail.

4.1 Legal environment

According to the Council Directive 2001/115/EC [2] "*invoices sent by electronic means shall be accepted by Member States provided that the **authenticity of the origin and integrity of the contents** are guaranteed*". *This could be guaranteed "by means of an advanced electronic signature within the meaning of Article 2 (2) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; **Member States may however ask for the advanced electronic signature to be based on a qualified certificate and created by a secure signature creation device**, within the meaning of Article 2(6) and (10) of the aforementioned Directive*".

Authenticity of the origin and integrity of the content has to be guaranteed when using electronic data interchange (EDI) as defined in Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects "*when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data*". However, as per the Directive [2]: "*Member States may, subject to conditions which they lay down, require that an additional summary document on paper is necessary*" to be exchanged, summarising a set of invoices. Where the applicable law allows for it this **summary document could also be exchanged electronically**. It is to be remarked that usage of EDI is subject to meeting the previously italicised wording. To exchange this summary document electronically also electronic signatures can be used to guarantee authenticity of the origin and integrity.

Regarding electronic signatures and electronic invoices focus has to be taken on the companies issuing and receiving electronic invoices:

1. Issuing electronic invoices to customers or other parties replacing paper invoices:
   The issuing party is issuing other parties electronic invoices which are signed with advanced electronic signatures to guarantee authenticity and integrity. Depending on the applicable laws advanced electronic signatures can be or not be based on a qualified certificate and can be issued with or without the use of a secure signature creation device (SSCD). For example in Italy electronic invoices have to be signed with advanced electronic signatures based on a qualified certificate and issued by means of a Secure Signature Creation Device (SSCD).
2. Receiving electronic invoices from sellers or from other parties replacing paper invoices:
   The enterprise is receiving invoices from sellers or from other parties. These invoices are electronically signed. The electronic signatures of the invoices have to be verified. Without signature verification the validity of the invoice cannot be guaranteed, which may have unpleasant consequences upon inspection by any Authority. Depending on applicable laws the verification results have to be documented and archived. For example in Germany all data which is needed for verifying the electronic signatures has to be archived together with the electronic invoices. (GDPdU - Guidelines for companies to enable inspector of taxes to access and verify electronic data). In Italy you do not need to store additional information, but you have to apply every predefined time period (i.e. at most every 15 days) a qualified signature and a timestamp to the set of stored documents and entrusting the QES and the TST to the Tax Authority.

One issue which is relevant for the companies issuing and receiving electronic invoices is the electronic storage of the electronic invoices. Directive [2] states: "*The **authenticity of the origin and integrity** of the content of the invoices, as well as their **readability**, **must be guaranteed throughout the storage period**…. The information they contain must not be altered; it must remain legible throughout the aforementioned period*".

4.2 Basic e-invoicing workflow

Sending and receiving e-invoices includes different sub workflows. This section describes the basic workflows for sending and receiving e-invoices using electronic signatures.

Where the adoption of AdES is chosen to ensure the required guarantee of "authenticity of the origin and integrity", before the electronic invoice is forwarded to the recipient, the invoice has to be electronically signed. From the technical viewpoint the workflow of issuing invoices has the following steps (see Figure 1 Issuing electronically signed invoices):

1. Generation of the electronic invoices;
2. Generation of the electronic signatures for the invoices;
3. Archiving the electronically signed invoices;
4. Transmitting the electronically signed invoices to the customers/suppliers.

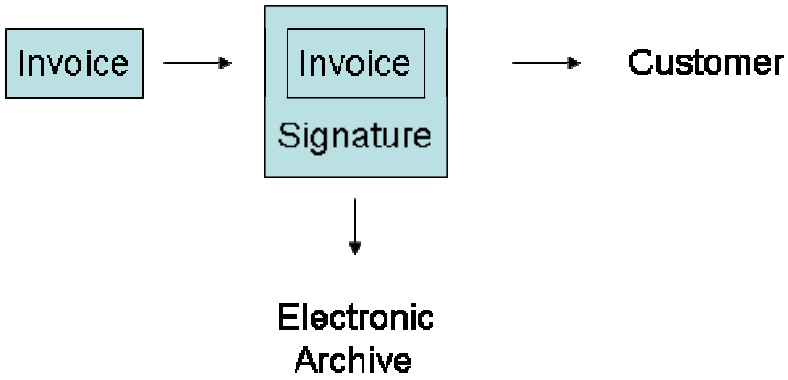

Figure 1 Issuing electronically signed invoices

Where required by force of law or by consolidated practice, items 3 and 4 may be exchanged in order to archive electronic invoices along with their relative shipment details.

On the receiver side before an incoming electronic invoice is processed, the electronic signature of the invoice has to be verified. The Directive [2] states: "*Member States … may also require that when invoices are stored by electronic means, the data guaranteeing the authenticity of the origin and integrity of the content also be stored*". Where this Directive requirement is implemented in the applicable law these data have to be archived together with the electronic invoice.

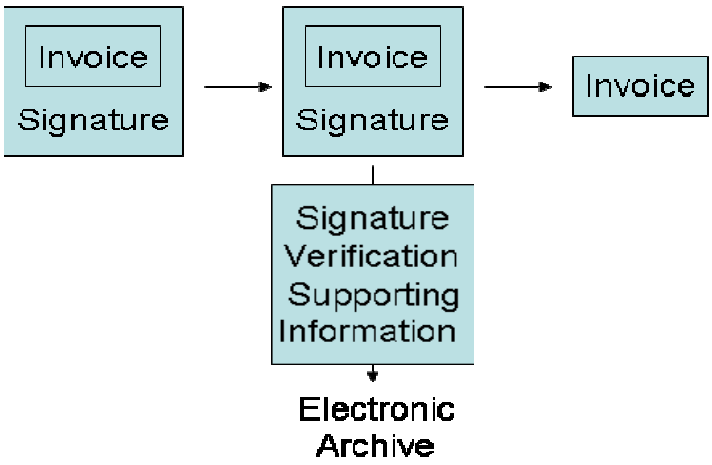

Figure 2 Receiving electronically signed invoices

Signature verification is covered in section "6 Verification and documentation of the integrity and authenticity of an electronic invoice".

After the signature has been applied, we have the original e-invoice. The original e-invoice has to be stored both on the side of the sender and of the receiver. The data before signing and after the verification including storage, we call e-invoice data.

4.3 Basic requirement for electronic signatures for e-invoicing

To implement e-invoicing different requirements have to be fulfilled. Basic requirements for electronic signatures for electronic invoicing from the viewpoint of companies and the legislator can be summarized as follows.

- Generation of the electronic signatures for electronic invoices must be possible also in an automated and reliable process that is law abiding; without the possibility of handling e-invoiced in an automated process large amount of e-invoices can not be handled effectively.
- Service providers should be empowered to sign electronic invoices with their own electronic signatures. The certificate should indicate that the service provider is acting on behalf of a taxable person. This requirement would be easy business for service providers because there would be no need for certificates for every single customer of the service provider.
- Enough information should be provided to ensure long term validity to the electronic signatures of the electronic invoices: "*The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period.*" These requirements are discussed in more detail in the next section.

To fulfil these requirements guidelines for certificates used for electronic invoicing are proposed and specified in "5.5 Guidelines for electronic invoice certificates."

4.4 Major parts and parties in the e-invoicing workflow

The E-Invoicing workflow addresses different parts and parties. This section gives an overview about different topics which have to be addressed when issuing and receiving electronically signed invoices.

4.4.1 Invoice signer

The first question which comes up when issuing electronic invoices is who does/can sign the electronic invoice? For example it might be useful in some cases that a third party signs the invoices on behalf of the seller.

The Directive [2] states: "Every taxable person shall likewise ensure that an invoice is issued, ***either by himself or by his customer or, in his name and on his behalf, by a third party***".

From a technical point of view this implies that each of these three parties - **seller, buyer, third party i.e. service provider** - is **enabled to issue an invoice.** Where the issuer is a customer or a third party on behalf of the seller, it must be explicitly stated that such invoice is issued in the name of the seller. As a direct implication of the quoted stipulation, a third party or a customer is empowered to sign such an invoice with its own certificate, but, where required by the applicable law, it must be clearly stated in the invoice the name of the seller on behalf of which it is issued**.** [1]

In other words, if invoices are issued on behalf of the seller or of the customer (in case of self-billing) and their electronic signatures are generated at a service provider's location, the service provider should be able to sign the invoices using its own signing key pair. In this case a certificate extension should be used, to indicate that the signer is acting as a service provider, as defined in "5.7.2 Certificate Extension for EInvoicing Service Provider.

[1] The term "where required by the applicable law" refers to self billing customer that may be required by some member states legislation to issue the invoice in name and on behalf of the taxable person (i.e. supplier)

4.4.2 The signing process

To guarantee an efficient processing of the electronic signatures it **must be possible to generate the *signatures* for electronic invoicing in a batch process**. The format used for the signature depends on the customers' needs. This signing process can be **run in-house or at an external service provider's** premises. The basic requirements for signing the electronic invoices in a batch process can be found in

"5 Advanced Electronic Signature used for electronic invoices".

4.4.3 Validity of the e-invoice's signature at issuance time

Depending on legal requirements or on organisational procedures or agreements between the parties, data **ensuring the invoice's signature was valid at issuance time** (like CRL or OCSP responses) **can be fetched, sent along with the invoice, and stored**. General Guidelines for Electronic Signature Verification can be found in CWA 14171 (see Bibliography).

As specified in this CWA, it might be good practice to fetch the CRL/OCSP response after what the same CWA calls "Grace period" has elapsed: "time period which permits the certificate revocation information to propagate through the revocation process to relying parties". This can be avoided if CAs issuing certificates for e-invoicing take appropriate measures to apply such technological (e.g. OCSP) and procedural (i.e. short revocation information publication cycles) measures as are required to reduce the grace period needed to a practicable minimum (ideally insignificant). Certain service providers or e-invoicing platforms may accept the business risk of compliance issues arising from non-respect of an applicable grace period.

Note: Technical times are necessary to have the revocation request delivered to the relevant CA and for the CA to process and publish the resulting revocation information. In order to take this into account, the correct CRL to examine, in order to verify an electronic signature, should not be the first issued after the time specified in the TST associated to the signature, but the second one, as specified in Figure 2 Frozen zone.

When checking a certificate revocation using CRLs, the following has to be taken into account.

ISO/IEC 9594-8:2001 TECHNICAL CORRIGENDUM N. 3 amends section 8.6.2.2 by fully replacing it. Its third paragraph states: "After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry."

If the signing certificate had been revoked sometimes before the signing time it has therefore been published in a number of CRLs. As per X.509 it may be removed from the CRL soon after certificate expiration time.

If the revocation request is submitted timely enough to allow for certificate publication in the first next CRL after signing time, and the signing certificate expired in the meantime, the second next CRL may rightfully not list the signing certificate: it had been published before. If the grace period is waited for, this second next CRL might not list the certificate.

If the revocation request is instead submitted too late to be listed in the first next CRL after signing time and the certificate does not expire in the meantime, it will be listed only in the second next CRL.

To prevent the above problem it is recommended that CAs publish certificates revocation information up to the second CRL issued after certificate expiration.

Additional it is recommend not using certificates nearing expiration.

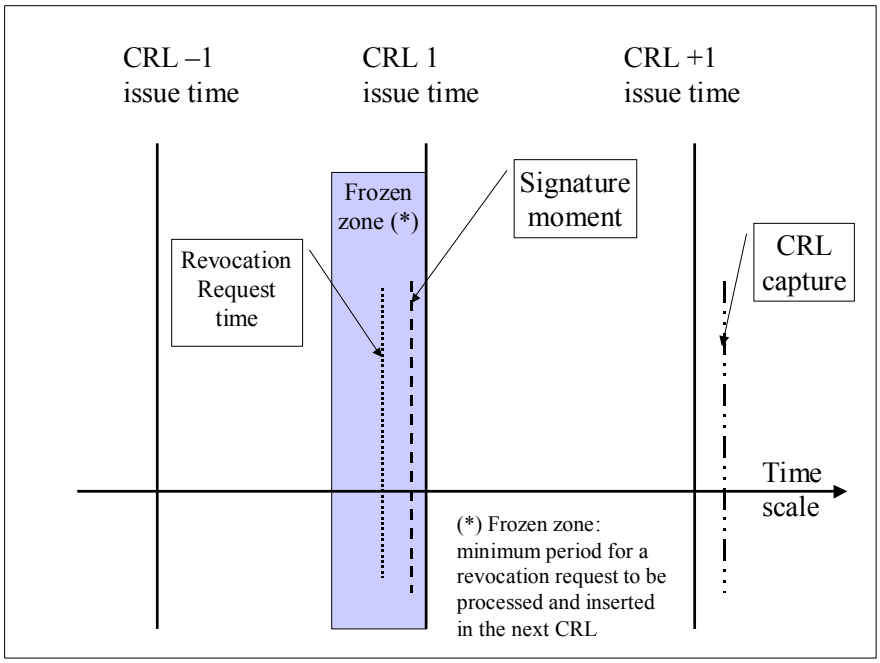

Figure 2 Frozen zone

This topic and recommendation for preserving the validity of an electronically signed invoice can be found in "6 Verification and documentation of the integrity and authenticity of an electronic invoice"

4.4.4 Electronic invoice format

The format of the invoice is **not specified in the Directive** but in certain Member States legal obligations exist that the **electronic invoice has to be machine readable**.

Directive [1] on electronic signature stipulates: "Invoices issued pursuant to point (a) may be sent either on paper or, subject to an acceptance by the customer, by electronic means."

Where mutual agreement is required, any format can be used, provided it meets the applicable law requirements.

As a matter of fact, where, the invoice structure is not mandated by force of law, a simple agreement between the sending and receiving parties is sufficient, and this widely depends on the parties' respective invoice processing systems. e-Invoices may be for example formatted using Extended Markup Language (XML) or Portable Document Format (PDF) and may be encoded using Multipurpose Internet Mail Extensions (MIME) for e-mail or web environments.

Where not forbidden by the applicable legislation, proprietary message formats, such as SAP IDoc (Intermediate Document), can be used. Some of the used formats already support electronic signatures and can be signed within the format used to generate an electronic invoice. For example for signing an electronic invoice defined in XML an XML electronic signature could be used.

Some document formats make it possible to make use of hidden codes. Hidden codes allow a type of programming which can add interactivity and functions to documents. This hidden codes are executed every time the document is opened. These mechanisms can be of great help to him who writes a document, for example by calculating the invoice amount, but they pose a great risk to the invoice system. In fact, the hidden codes mechanism can be used to change the document presentation (i.e. its appearance) while not affecting the document content (i.e. the bytes it is made of). This would cause the presentation to be changed without affecting the electronic signature validity, thus making it possible to perpetrate frauds.

Therefore, it is **highly recommended that static non modifiable document formats are used** that either do not outright support active code, which can dynamically change the presentation, or that allow for disabling these hidden codes mechanisms. As a matter of fact, **some applicable law outright forbids the use of macros and hidden codes mechanisms.**

4.4.5 E-Invoice storage

After the electronic signatures are processed, the signed electronic invoices have to be unalterably archived, where required along with the shipment data and the information needed to subsequently verify the signature integrity and authenticity. The electronic invoices have to be filed for a number of years depending on the applicable legislation. This topic is discussed in more details in chapter “6 Verification and documentation of the integrity and authenticity of an electronic invoice”.

4.5 Facts and recommendations

Basic legal requirements:

- authenticity of the origin and integrity of the contents of electronic invoices have to be guaranteed
- Member States may however ask for the advanced electronic signature to be based on a qualified certificate and created by a secure signature creation device

Signature generation:

- it must be possible to generate the *signatures* for electronic invoicing in a batch process

Storage:

- authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period
- Information should be available to ensure that an invoice signature was valid at issuance time

Service providers:

- Seller, buyer, third party i.e. service provider - are enabled to issue an electronic invoice
- The invoice can be issued by a third party or by a customer and signed by these entities with their own signature, but in some legislation it must be clearly stated in the invoice the name of the seller on behalf of which it is issued
- Service providers should be able to sign the invoices using their own signing key pair.
- Depending on the applicable legislation, certificates MUST, MAY or MUST NOT indicate that the signer is acting as a service provider (See guidelines on 5.4 Responsibility in invoices signing and 5.7 Certificate structure.

Invoice formats:

- Formats of the electronic invoices are not specified in the Directive but in certain Member States legal obligations exist that the electronic invoice has to be machine readable
- It is highly advisable to make use of static non modifiable document formats even where non explicitly requested by the applicable law.
- Some applicable law outright forbids the use of macros and hidden codes

5 Advanced Electronic Signature used for electronic invoices

This chapter provides a more detailed description how to use AdES for electronic invoicing. It deals with aspects of batch signing, e-signature restrictions for e-invoicing.

The purpose of e-invoicing is maximum automation. Natural person certificates always create an additional layer of complexity when the private key must be installed and used in an IT resource.

Advanced Electronic Signatures are used by taxable persons, or their delegates, to ensure over time integrity and authenticity to the electronic invoice. **Using advanced electronic signatures** within the meaning of Article 2 (2) of Directive [1] means that an **electronic signature has to be bound to a person**.

Where applicable law does not expressly prohibit the creation of electronic signatures by legal persons, legal person certificates (technically issued to an IT resource operated under that legal person's control and responsibility) should be used to avoid administrative other and unnecessary complexities relating to the apportioning of responsibility between the natural person and the legal person on whose behalf the former signs.

The next sections deal with these issues in more detail.

5.1 AdES bound to a natural or legal person

It has to be possible that the **electronic signature for an electronic invoice can be the signature of a natural or legal person, where required by the applicable law**. Where legally possible, for a one-man business an electronic signature of a natural person would be functional, in case of an enterprise an electronic signature of a legal person would be useful. In fact, having an invoice signed by a natural person may imply that this very person is responsible of that invoice integrity and authenticity versus the outer world. It is true the opposite: what actually fully bears this responsibility is the company on behalf of which the human being is acting. If he/she misbehaves he/she will be held responsible versus his/her employer that will have its own internal mechanisms/procedures to keep track of who issued what invoices.

Art 2(2) requires an **AdES** to be "**uniquely linked to the signatory**" and to be "capable of identifying the signatory". The definition of "signatory" (Art. 2(3) of the same Directive) is: "a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents". The term "**person" referred to "signatory" is not otherwise qualified**; therefore it **could refer to both a natural or legal person**, which can both act on their own behalf.

The e-invoice signature needs not to be based on a qualified certificate, except where the applicable law explicitly requires a qualified electronic signature. However the certificate used for the signature for electronic signatures has to be bound to a person, be it natural or legal.

In case the electronic signature is an electronic signature of a natural person, **information should be supplemented that the natural person has acted on behalf of the company** issuing the invoices that should be specified in the certificate. For example, the invoice issuing company might be specified in the "organizationName".

5.2 "Electronic seals" versus "electronic signatures"

The decision to use advanced electronic signatures based on a qualified certificate or advanced electronic signatures not based on a qualified certificate rests on the applicable legal requirements for e-invoices.

However, **where qualified signatures are requested by a national legislation, they cannot be given the meaning of commitment to the content of the electronic invoice**, as the Directive clearly states: "Member States shall not require invoices to be signed."

But it is to be noticed that qualified electronic signatures, as per Directive 1999/93/EC: "satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data". Therefore **care must be taken to**

avoid that qualified electronic signatures on electronic invoices are attributed a meaning which is not mandatory by Directive 2001/115/EC. This means that if a qualified electronic signature is used for electronic invoicing it cannot be interpreted as a commitment to the content.

Only the purpose of guaranteeing the invoices authenticity and integrity can be assigned to qualified electronic signatures in this domain.

Directive [1] on electronic signature stipulates: *"Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device … satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data"*. Such Directive does not mandate that what has been called "Qualified Electronic Signature" shall always have this meaning: it simply means that a QES meets these requirements, but, as even a handwritten signature may have different meanings (for example in Common Law countries), similarly a QES may, where appropriate, not have the equivalence of a commitment to content.

To better clarify, and to summarise, the above concepts it may be useful to highlight that, **for the purposes of the Directive 2001/115/EC, the term "electronic signature" would have the meaning of "electronic seal".** This means that a QES used in the invoice domain, does not imply commitment to the signed content, but it only ensures integrity and authenticity to the signed data.

5.3 Batch e-invoice signing

Having clarified that in the electronic invoices domain an electronic signature is to be deemed as an electronic seal, **without the meaning of commitment to the content, it is easier to deal with batch e-invoice signing**.

In some EU Member States it is possible to sign a batch of documents, including e-invoices, without requiring the signer to inspect and explicitly approve each document. This means that the signer has only to wilfully launch the signing process.

Other countries may not allow for the batch signing. In this case, it is to be ascertained if this prohibition blindly applies to any kind of advanced signatures or solely to qualified signatures, and behave accordingly.

5.4 Responsibility in invoices signing

Some laws require these certificates to be issued to natural persons, in which case, this is obviously the way to go.

But in other legal environments, where this provision does not exist, it can be useful to note that issuing a human being an invoice-signing certificate may be arguable. In fact, it is the company, on behalf of which the invoice is issued, that is responsible for any incorrect invoice towards a customer or even towards the law, not the single issuer, let alone a specific human being. This is clearly specified in some country legislation and case law. This natural person is, obviously, responsible towards his/her employer, which is therefore supposed to have in place suitable procedures to trace who signed what invoices.

In conclusion, **it could be a good practice not to issue in the name of a natural person an invoice-signing certificate, again: where the applicable law does not mandate differently.**

A similar comment may apply in general to invoice issuing on behalf of the taxable person, as per the Directive [2]. In some legislation the only person responsible for the issued invoices is the taxable person. Any other actor that issues invoices on behalf of the taxable person is not liable towards the fiscal law for mistakes done in invoice issuing. Nevertheless they have full responsibility towards the taxable person on behalf of which they act, to the extent addressed by the agreements between the parties, as per the applicable law. Obviously, where the fact is an outright fraud, this is a criminal offence to be prosecuted as such, but this falls under another legal domain.

In some case the invoice issuing company would like to hand the signature service to a service provider. Two ways will be found in practise:

1. The Service Provider will sign the invoice data with it's own electronic signature (see section 5.7.4.Certificate Extension for Service Providers)

2. The company will hand its own signature to the service provider. The service provider will sign the invoice data with the signature of the customer. The use of the electronic signature should be restricted by contracts between the service provider and the customer.

5.5 Guidelines for electronic invoice certificates

In addition to the legal requirement set by Directive [2], that the electronic signature must be an advanced electronic signature within the meaning of Article 2 (2) of Directive [1], some guidelines for electronic invoice certificates and signatures are:

1. An electronic invoice can be signed by a natural person or a legal person, under the assumptions of section “5.4 Responsibility in invoices signing”.

2. In some cases it may be recommended, or even required by the applicable law, to specify that a certificate can be used to issue electronic invoices. Examples of possible technical solutions to implement this need are the following ones:

   - the electronic invoice certificate may have a non critical certificate X.509 [5] extension
   - a specific Certificate Policy may be indicated, the OID of which would be written in the certificatePolicies extension
   - some X.500 attribute as specified in X.520 [6] and in X.521 [7] may be used
   - optionally the common name (CN) can include a text that the certificate is used for electronic invoicing.

3. An optional identifier of the person issuing the invoice (e.g. its VAT code) may be specified in the certificate. Where a natural person signs the e-Invoices, it is highly recommended that the name of the taxable person (responsible for the invoice content) is also indicated.

4. An optional statement may be used (i.e. an extension in the X.509 [5] signing certificate) claiming that the private key related to the certified public key resides in a Secure Signature Creation Device (see ETSI TS 101 862 [8], section 5.2.4). Alternatively an assertion could specify this in the relative Certificate Policy, but the previous solution is by and large preferable, since the OID defined in TS 101 862 can automatically be verified by a software application.

5. Depending on organisational measures (i.e. policies, procedures, physical security measures, etc.) taken to preserve the electronic invoices over years there should be archive obligations for certificate authorities issuing certificates for electronic invoicing. Some CAs do not have archive obligation for revocation information. This is the reason why some national laws force businesses to archive this revocation information for the storage period on their own. Where the CAs have this obligation, the businesses would not need to take care about this issue. Where revocation information are required to be stored for certificates for electronic invoicing, they should be archived between 4 and 11 years depending on the national legal requirements for archiving invoices.

6. The Certificate Policy should also address whether certificates issued in its compliance can be used to issue single signatures and/or automated signatures.

Another possible way to represent certain characteristics of the signatory, e.g. business title, type of company or features of the transaction would be to use attribute certificates.

5.6 Signature Creation Data

Council Directive 2001/115/EC, Article 2 (2) makes two electronic signature types usable in the e-Invoicing environment: an Advanced Electronic Signature and a Qualified Electronic Signature. They have different implications on where the signature generation data (usually called “private key”) is generated, kept and used.

AdES do not strictly require private keys to be generated and kept in hardware devices, while QES have this feature as a basic distinction. Where a Member States has adopted one of the two above solutions, the following paragraphs apply.

5.6.1 SCD and AdES

To **generate advanced electronic signatures** and to guarantee high performance the signature creation data (private keys) **not necessarily have to be created, stored and used inside crypto hardware** (HSM or SSCD). The signature creation data could also be stored in a file.

Given the intrinsic insecurity of files, particular external security measures must be implemented in addition to protecting the files themselves from tampering (deletion, modification), e.g. access should be controlled by means of password based encryption (e.g. as specified in PKCS#5) or by means of the Shamir's and Blakley's secret sharing schemes. Literature reference to these methods and schemes can be found in the Bibliography section. In any case, however, suitable organisational policies are to be implemented to support these purely cryptographic means with strong practices to prevent the access secret to become unduly known. Therefore, in this case, the Certificate Policy should require users to adopt more stringent security measures than where crypto hardware is used, to hinder attacks and these measures must be implemented in suitable Security Policies. An example of some suitable policies could be that the related system might not be allowed to be connected to the internet and should only be operated by specific persons authorized to perform the invoices issuing procedure, to which the secret should be given under strict operating procedures.

5.6.2 SCD and QES

Where QES are used, one **basic requirement is that the private key is to be kept and used inside an SSCD**. This makes it easier to implement suitable security measures, because the device itself vouches for key confidentiality and provides a reasonable basis to believe it is used solely by authorised people. Nevertheless, some organisational measures are required as well, to bolster such basics as enforcing the access secret confidentiality and the signing device integrity.

As specified in the previous section "5.6.1 SCD and AdES", an optional statement claiming that the private key related to the certified public key resides in a Secure Signature Creation Device, as provided in ETSI TS 101 862 [8], section 5.2.4, may be used to provide signature verifiers sufficient trust in the correct use of the signing key.

5.7 Certificate structure

Using electronic signatures in a batch process could be risky in that way those also other documents beside e-invoices could be signed without the approval of the signing person. This could have unimaginable negative consequences. To eliminate that risk the certificate policy or the certificate should indicate that the electronic signature can only be used for signing e-invoices.

The invoice issuer should carefully evaluate such risks if it's own needs require certificates that can only be used for e-Invoices signing. In such case the invoice issuer should prefer CAs that issue certificates indicating that they can only be used to this purpose. This can be done by indicating a suitable certificate policy or by specifying a certificate extension (see section 5.7.2) or an Extended Key Usage OID (see section 5.7.1).Especially for the extension "EinvoicingServiceProvider" the following applies: It should be considered whether all applications (on the sender's and the recipient's side) that will be using the certificates recognise/support the extension. If not, the extension should not be marked critical.

To facilitate achieving interoperability it is strongly recommended that the Extended Key Usage OID specified in section 5.7.2 is adopted.

It is highly advisable that one of the following *two possible ways are used to identify a certificate used specifically for eInvoicing:*

a. *a specific CP*
b. *a certificate extension that can be either a new extension or a new value for the extended key usage.*

Is also highly advisable to make use of an extension specifying that the certificate is used by an eInvoicing service provider.

A Certification Authority specifies which rules sets it complies with by indicating in the certificates it issues one or more CP OID,and what certificate types it issues: time stamps signing certificate, authentication certificates, etc.

Where the issuing CA generates only one certificate type under one specific CP, the corresponding OID can be also used to identify that specific certificate type. But where under the same CP a CA issues several different certificate types, the CP OID cannot provide any information on the type of the certificate that exhibits it. In this case something additional is necessary to this purpose, for example a specific certificate extension and/or an extended key usage.

The field subject of the certificate should include the name of the invoice signer in the commonName (CN) and the name of the company issuing the invoice in the organizationName (O). It is suggested to make use of organizationalUnitName (OU) where more Organisation departments independently issue invoices. Optionally the CN field can indicate that the certificate is used for electronic invoicing.

Note: certificates with KeyPurposeId “id-kp-eInvoicing” and/or extension “EinvoicingServiceProvider”, defined in the following subsections, may also be used to issue other types of electronic documents with similar requirements.

5.7.1 Extended key usage “id-kp-eInvoicing”

The extended key usage property indicates the purposes for which the certified public key is used.

In general: specially when using automated e-Invoices signing processes, it would be very wise to use a certificate where it is clearly specified that it is not usable to sign other types of documents, like IOUs, contracts, etc.

RFC 3280 [9], section 4.2.1.13 states:

“This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates. […]
Key purposes may be defined by any organization with a need. Object identifiers used to identify key purposes MUST be assigned in accordance with IANA or ITU-T Recommendation X.660 [X.660].This extension MAY, at the option of the certificate issuer, be either critical or non-critical.

If the extension is present, then the certificate MUST only be used for one of the purposes indicated. If multiple purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present. Certificate using applications MAY require that a particular purpose be indicated in order for the certificate to be acceptable to that application.”

To indicate that the certificate is used for electronic invoicing an extended key usage value should be added. The corresponding certificate SHOULD contain the
extended key usage field extension as defined in RFC 3280 [9] Section
4.2.1.13 with KeyPurposeID having value:

id-kp-eInvoicing.

The following object identifier identifies the KeyPurposeID having
value id-kp-eInvoicing：

id-kp-eInvoicing::= {iso(1) identified-organization(3) cen(162) ceninternal(1) single-part-specification(0) einvoicing-digitalsignature-cwa(15579) extended-key-usage-id-kp-eInvoicing(3)}

This key usage is consistent with, and hence may be used in combination with, KeyUsage digitalSignature and/or nonRepudiation as defined in RFC 3280 [9] section 4.2.1.3.

5.7.2 Certificate extension for “EinvoicingServiceProvider”

To indicate that the **organizations are acting as a service provider** on behalf of companies the **extension EinvoicingServiceProvider should be added**. Certificates with this extension shall only be used by service providers acting on behalf of an organisation.

RFC3280 [9] profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. RFC3280 describes in detail the X.509 v3 certificate, with additional information regarding the format and semantics of Internet name forms and how it has to be used in applications. Additionally to core data like subject or issuer of the certificate X.509 v3 certificates provide the possibility to include additional attributes as certificate extension.

RFC 3280 [9], section 4.2 states:

```
“The extensions defined for X.509 v3 certificates provide methods for
associating additional attributes with users or public keys and for
managing a certification hierarchy. The X.509 v3 certificate format
also allows communities to define private extensions to carry
information unique to those communities. Each extension in a
certificate is designated as either critical or non-critical. A
certificate using system MUST reject the certificate if it encounters
a critical extension it does not recognize; however, a non-critical
extension MAY be ignored if it is not recognized.”
```

The following defines the syntax for this certificate extension using the template defined in X.509.

```
eInvoicingServiceProvider  EXTENSION ::= {
    SYNTAX        EInvoicingServiceProvider
    IDENTIFIED BY id-eInvoicingServiceProvider}

EInvoicingServiceProvider ::= NULL


id-eInvoicingServiceProvider ::= {iso(1) identified-organization(3) cen(162)
ceninternal(1) single-part-specification(0) einvoicing-digitalsignature-
cwa(15579) certificate-extension-einvoicing-service-provider(2)}
```

5.8 Signature formats

Under Mandates M 290 of the European Commission two signature format families have been developed by ETSI: TS 101 733 [4] and TS 101 903 [3].

It would therefore be reasonable to make use of the above signature formats for signing e-Invoices.

However, since in these ETSI Technical Specifications there are many options, the ETSI ESI launched in November 2005 a Task Force to define profiles straightforward enough to suit specific requirements. This CWA defines in section 7 the requirements for various types of electronic signature depending on the presumed signature life. These requirements have been provided to the ETSI ESI to develop suitable profiles. Issuers of electronic invoices based on Advanced Electronic Signatures will therefore be able refer to profiles specified in documents ETSI TS 102 733 and ETSI TS 102 903, to be published by February 2007.

5.9 Facts and recommendations

AdES bound to a person:

- Using advanced electronic signatures within the meaning of Article 2 (2) of Directive [1] means that an electronic signature has to be bound to a person
- Electronic signature for an electronic invoice can be the signature of a natural or legal person, as per the applicable law. If the signatory is a legal person then the signature cannot be a qualified signature.
- In case the electronic signature is an electronic signature of a natural person, information should be supplemented that the natural person has acted on behalf of the organization issuing the invoices that should be specified in the certificate. For example, the invoice issuing organization might be specified in the "organizationName"

Electronic seals:

- Where a qualified electronic signature is used, it can only have the purpose of ensuring authenticity and integrity otherwise any member state requiring qualified electronic signatures would be in conflict with the Directive 2001/115/EC provision ("*Member States shall not require invoices to be signed*").
- Where qualified signatures are requested by an applicable legislation, they cannot be given the meaning of commitment to the content of the electronic invoice,
- Only the purpose of guaranteeing the invoices authenticity and integrity can be assigned to qualified electronic signatures in the domain of e-invoicing
- For the purposes of the Directive 2001/115/EC, the term "electronic signature" has the meaning of "electronic seal".

Batch signing, HSM and SSCD:

- Without the meaning of commitment to the content, it is easier to deal with batch e-invoice signing.
- AdES do not strictly require private keys to be generated and kept in hardware devices, while QES have this feature as a basic distinction

Certificate extensions and Policies

- Service providers should use the certificate extension EinvoicingServiceProvider
- Certificates used for electronic invoicing should use the extended key usage "id-kp-eInvoicing"
- The proposed policy recommendations for electronic invoice certificates should be implemented
- Depending on whether the certificates are qualified or non-qualified (as per the meaning of this term as in Directive 1999/93/EC, art. 2(10)) reference certificate policies could be as in ETSI TS 101 456 or in ETSI TS 102 042, respectively. Where a different certificate policy is adopted it is recommended that it is developed on the basis of IETF RFC 3647.

6 Verification and documentation of the integrity and authenticity of an electronic invoice

In case of electronic invoices, **authentication and integrity have to be guaranteed over the whole storage period of invoices which can be from 5 to 11** (or even longer if data are needed for tax inspection) years depending on the national requirements.

A **problem that arises** when using electronic signatures for electronic invoicing is the method to store the **electronic invoices in a way that the electronic signature stays verifiable over years**. Electronic invoicing storing systems need to take care of this problem. Verifying an electronic signature that has been created several years before could come up against problems. Verifiers may well be able to retrieve the electronic invoice properly including the signature but they may face the following difficulties, even when the electronic signature is cryptographically sound: the signature cannot be relied upon, because the certificate was revoked or the required revocation information is no longer available because the certificate expired and therefore the relevant CA rightfully removed the information on the revoked certificate from the CRL.

Electronic signatures - as defined in the European Directives [1] and [2] - provide basic authentication and integrity protection and may be created without accessing any online services. **However, without the addition of other relevant data, like revocation information and information on "before when" the signature itself was created, the electronic signature could not be verifiable in the future.** The information on the signature creation time is indispensable when the certificate has been revoked or has expired, to ascertain if such event occurred before or after the signature creation.

The present clause identifies formats and procedures to keep e-invoices verifiable over long periods. An e-invoice has to be able to be used for arbitration in case of a dispute between the sender and recipient and the tax authorities.

To ensure that electronic invoices are durable over years, electronic invoices validities have to be extended with additional security elements, or additional organisational measures have to be taken to meet the legal requirements for the storing and verifying them over a certain number of years.

6.1 Long term verification of an electronic signature of an invoice

As said before, to verify the electronic signature of an electronic invoice it is not sufficient to ascertain only the cryptographic correctness of the signature. Additionally the verification of the validity of the used certificate set is necessary. (see CWA 14171 General Guidelines for Electronic Signature Verification).

To validate an electronic signature of an invoice at least these basic data are required:

1. the electronic signature; this includes:
    - the signed invoice;
    - the digital signature;
2. validation data which is the additional (basic) data needed to validate the electronic signature; this includes:
    - certificate set (all certificates needed to generate a path that leads to a point the verifier trusts);
    - certificate status information for all the above certificates;
3. a mechanism to reliably ascertain a moment where the signature existed; this is paramount where one of the involved certificates is revoked or expired, to ascertain if the signature existed before the revocation / expiration time..

In the case of eInvoices, when their implemented storage environment is not sufficiently reliable per se, data indicated in the previous items number 2 and 3 may become necessary:

When involved parties can agree that one audit log may be taken as a reference, then Time-Marking based on that log can replace Time-Stamping. However, in case where the information from that log is challenged, ways to demonstrate that the information really comes from that audit log may not be that simple and may be more costly and time-consuming than time-stamping techniques.

A positive validation of an electronic signature of an invoice has to indicate that the format and digital signature verifications have not failed and there is sufficient information to determine if the electronic signature is valid. **Sufficient information includes that the used certificates and the revocation status information were available at least at storage time, and, where necessary, during the entire storage period.**

A correct electronic signature has to be created within the validity period of the certificate. Additionally it would be unacceptable if the electronic signature gets invalid, should the used certificates be revoked later on. To avoid a signature to become unduly questionable or even rejected in the future, **the point in time when it was issued may need to be provable.**

One way to prove that the signature has been created before a given time, is to **apply a time stamp token relatively shortly after the creation of the signature**.

6.2 Providing long term validity of electronic signatures for electronic invoices

An electronic signature long term validity is based on three issues:

1. reliably defining a point in time where the signature existed;
2. being able to define whether the moment, when each of the certificates the signature is based on (from the signer's up to the end of the certification path) ceased being valid, for revocation or expiration, was before or after the moment the signature existed;
3. keeping the signature sheltered from any possible attack, especially in the case the algorithms or keys have become weak.

Therefore, to achieve confidence on the signature validity:

a. the signature is to be placed in the time,

b. during the whole signature lifetime:

- the information on the involved certificates status at the signature issue moment,

  and

- the signature itself

are to be securely kept beyond reach of any possible attacker, to prevent possibly weakened algorithms/keys from being attacked and certificates/revocation information from being fraudulently changed. Where allowed by suitable organisational measures, certificate status information may not be kept.

Ensuring stored invoices are long term valid, as specified above, **depends on both organisational and technical measures** (see Figure 3 Organisational versus technical measures): the stricter the organisational measures, the less rigid the technical measures can be, as schematised in the following figure.

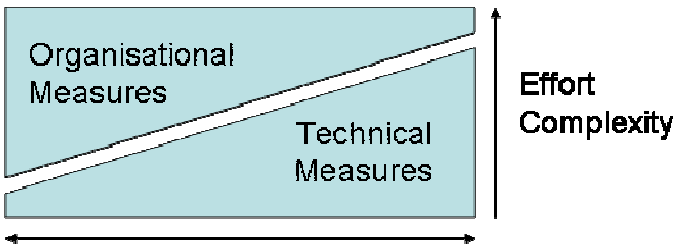

Figure 3 Organisational versus technical measures

For example if a trusted third party like a notary guarantees that the electronic signatures of the electronic invoices were valid at a certain point of time and that they have been securely kept since then, no additional technical measures like archiving the revocation information of the certificates used to issue the invoices signatures are necessary. On the other hand if the notary-like assertion is made electronically and signed with an electronic signature, it may be necessary to time stamp this signed assertion and to keep the certificate paths and the relevant revocation information related to the notary-like certificate and to all the other involved certificates, unless the notary-like organisation is capable to vouch that the signature on such assertion has been kept beyond reach of any possible attacker.

6.3 Proposed organisation types

In this section examples are provided of different organisation types that implement the above concept.

Organisational Type 1 (OL-1)

In addition to implementing all the features required (by force of law or by governing rules) this organisation are officially recognised as meeting the specific requirements for security of electronic invoicing e.g notary, governmental body, person recognised through a national accrediation scheme, depending on the applicable law.

Organisational Type 2 (OL-2)

Organizations which are certified under generally recognised security criteria as meeting the security requirements associated with services operated for electronic invoicing e.g. ISO 17799.

Organisational Type 3 (OL-3)

Organisation with no official recognition for security to counter risk associated with e-invoicing.

Depending on these different security levels suitable technical measures are to be implemented.

More information in the CWA "Storage of Electronic Invoices" section 4.8

7 e-Invoice signature profile requirements

E-Invoicing has special requirements for electronic signatures. Most of these requirements could be fulfilled by using enhanced signature formats as defined in TS 101 903 (XAdES) [3] and TS 101 733 (CAdES) [4]. Since these formats provide for much more features than would be required for electronic invoicing, specific electronic invoicing signature related formats, addressing only the e-invoicing requirement, would be helpful as they would make the handling of e-signatures for e-invoicing easier. This chapter defines the requirements of such e-invoicing profiles.

In February 2007 ETSI ESI, taking also into account the requirements specified in the previous version of this CWA 15579, issued ETSI TS 102 734 [12] and ETSI TS 102 904 [13] that provide profiles of the previously mentioned CAdES and XAdES, respectively. These two new documents can, therefore, be a suitable reference when implementing e-Invoicing related signatures.

7.1 Basic signature

This profile shall fulfill the following requirements, in addition to specifying that the data structure refers to signature and not to other cryptographic processing: i.e. data are signed, not encrypted.

Note: encryption, where required, may be addressed, but it is out of the CWA scope.

The requirements, in addition to the data mandatory for a digital signature, are:

1. an untamperable reference to the signer's certificate must be included among the signed attributes, to prevent forging by certificate substitution;
2. including the signer's certificate in the signature or a reference to it, if the certificate is otherwise securely available to the verifier.
3. storing the signed e-Invoice jointly with the signature.

7.2 Short term signature

This signature profile aims at providing information necessary to later on implement short term verification, i.e. verifications when the signing certificate has not yet expired.

The requirement is to provide the possibility to add to the data, mandatory for a basic signature also a time stamp token and the related data:

1. a time stamp token itself.
2. an untamperable identifier of the certificate supporting the time stamp token signature to be included among the TST signed attributes, to prevent forging by certificate substitution; if the TST policy is that only one certified key with the same attributes is allowed then this is not necessary.

The certificate supporting the time stamp token signature or a reference to it, if the certificate is otherwise securely available to the verifier, can optionally be added to the TST.

7.3 Long term signature

This signature profile aims at providing information necessary to further on implement long term verification, i.e. verifications where the signing certificate has expired.

The requirements are to provide the possibility to add to the data specified above for a short term signature:

1. information on the status of the signer's certificate;
2. a sequence of the following optional data;
    a. the certificate of the CA that issued the signer's certificate and all higher level CA certificates up to the Trust Anchor CA;

b. information on the status of the above certificates;

3. a multiple sequence of the following optional data:
   a. time stamp token; its first instance is already present in the short term signature;
   b. certificate chain supporting the time stamp token signature;[2]
   c. information on the status of the above certificates.

Note: a chain of TST and of the related information is to be possible.

It is to be noted that the implementers must be able to choose between profiles that:

1. include in each single signature all the certificate path and all their related status information, or
2. include only the reference to these certificates and to their related status information, that are stored elsewhere, or
3. include a mix of certificates and their related status information and of the reference to this information types.

Where applicable a storing organisation might apply a single TST to a batch of documents.[3] Which of these data are to be stored internally and which externally is to be left as an option to the implementer.

This is represented in the following table, where shaded cells refer to data that may be held in any place (recipient, TSA, third party service) but must be available for the duration of the invoice lifetime.

	Signature components	**Basic Signature**	**Short term sig.**	**Long term signature**
	Reference to signer's certificate as a signed attribute	✓	✓	✓
	Signer's certificate	✓	✓	✓
	PTR to Signer's certificate CRL/OCSP Response			✓
	Signer's certificate CRL/OCSP Response			✓
Recursive for all CA cert. in the CA chain	PTR to CA certificate			✓
	CA certificate			✓
	PTR to CA certificate CRL/OCSP Response			✓
	CA certificate CRL/OCSP Response			✓
	TST1		✓	✓
	Reference to TST1 certificate as a signed attribute		✓	✓
	TST1 certificate		✓	✓

[2] Note: Where more than one invoice is sent to the same recipient, it would be an unnecessary overhead to include the TSA certificate chain in every time-stamp. In this case, the certificate chain might be stored separately and referenced by every TST issued using it. This store / repository, that can be held by the recipient, by the TSA or by some third party service, must be kept for the duration of the invoice lifetime.

[3] Note: this could be done, for example, by building a file made up with the digests of the involved signed e-Invoices and by applying a timestamp to this.

	Signature components		Basic Signature	Short term sig.	Long term signature
	PTR to TST1 certificate CRL/OCSP Response				✓
	TST1 certificate CRL/OCSP Response				✓
These data may / may not be included in the signature	TST … n				✓
	Reference to TST … n certificate as a signed attribute				✓
	TST … n certificate				✓
	PTR to TST … n certificate CRL/OCSP Response				✓
	TST … n certificate CRL/OCSP Response				✓
	PTR to TSA CA certificate	Recursive for each CA in the TSA chain			✓
	CA certificate				✓
	PTR to TSA CA certificate CRL/OCSP Response				✓
	CA certificate CRL/OCSP Response				✓

Annex I: Informative Annex

I.1 Directive on Electronic Signatures

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Official Journal L 013 , 19/01/2000 P. 0012 - 0020

Art. 2 Definitions

For the purpose of this Directive:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. "advanced electronic signature" means an electronic signature which meets the following requirements:
   - **a) it is uniquely linked to the signatory;**
   - b) it is capable of identifying the signatory;
   - c) it is created using means that the signatory can maintain under his sole control; and
3. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
4. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
5. "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
6. "signature-creation device" means configured software or hardware used to implement the signature-creation data;
7. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;
8. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
9. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;
10. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
11. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;
12. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
13. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
14. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

I.2 Minimizing organizational measures using XAdES/CAdES Formats

TS 101 903 (XAdES) and TS 101 733 (CAdES) define a number of signature formats including some formats providing long term validity of electronic signatures. To ensure that electronic signatures are durable over years, TS 101 903 and TS 101 733 extend the signatures with additional security elements to meet the legal requirements of storing signed documents over a certain number of years.

ETSI TS 101 903 and TS 101 733 define the following seven signature formats. Each additional level adds more security in terms of non-repudiation and long-term validity to the signature. The formats to be chosen would depend on the organizational measurements taken.

- XAdES-BES/CAdES-BES
  fulfils the basic requirements of the advanced electronic signature. If a trusted third party like a notary guarantees through organisational means that certain electronic signatures where valid at a certain point of time XAdES/CAdES should be sufficient.

- XAdES-T/ CAdES-T (Time-stamped)
  XAdES/CAdES with time-stamp on the signature specifies a moment in which the signature exists, to assess if a signature was issued when the related certificate was still valid. If a trusted third party like a notary guarantees that the electronic signatures where valid at a certain point but does not reliably assert the signature time XAdES-T/CAdES-T should be sufficient.

- XAdES-C/ CAdES-C (Complete)
  XAdES-T/ CAdES-T with references to the complete set of validation data provides for long-term validity. If a trusted third party (for example the CA) guarantees to archive for the required time the complete set of validation data (for example CRLs) XAdES-C/ CAdES-C would be sufficient.

- XAdES-X/ CAdES-X (eXtended)
  XAdES-C/ CAdES-C with time-stamp on the validation data references provides for long-term validity

  XAdES-X and CAdES-X may be implemented in two types:

  - Type 1, where the Time Stamp Token applies to the entire XAdES-C/CAdES-C signature

  - Type 2, where the TST applies only to the validation data references

- XAdES-X-L (eXtended Long-term)
  XAdES-X with complete validation data information provides for long-term validity. No additional organisational measurements are necessary to guarantee the validation of the electronic signature.
  The previous time stamped signature formats provide reliability on the signature if the time stamping server's certificate does not expire before the required archival time. If, instead, for example the TSS's certificate expires after three years and the archival time is of four years, information on the TSS's certificate status is to be fetched and kept and the following signature format is required.

- XAdES-A/CAdES-A (Archival)
  XAdES-X-L/CAdES-X-L with one or more archival time-stamps, each applied before expiration of the certificate supporting the preceding TST, provides for long-term validity. Each TST related certificate status information is also required. No additional organizational measurements are necessary to guarantee the validation of the electronic signature.

For achieving an intrinsic long-term validity of an electronic signature all the data used in the validation of the signature should be archived for later arbitration purposes. The data used in the validation process includes the certificate chain from the certificate corresponding to the private key used to sign the signature up to a trust anchor suitable for the verifier and the corresponding revocation information for the used certificates. This certification and revocation data may be stored within the signature or at a different place under the control by the verifier.

If the certification and revocation information is stored outside the signature, references to the used certificates and corresponding revocation information have to be stored with the signature to unambiguously identify the data used in the validation process.

I.3 Time Stamp Token Chain (TST Chain)

It is to be noted that a TST is itself electronically signed by a Time Stamping Authority. If the expiration time of the TSA's signing certificate falls before the end of the invoice's required storage time, the TST applied to the invoice must be re-time stamped before the expiration of the previous TST's certificate, and so on, as indicated in figure 4.

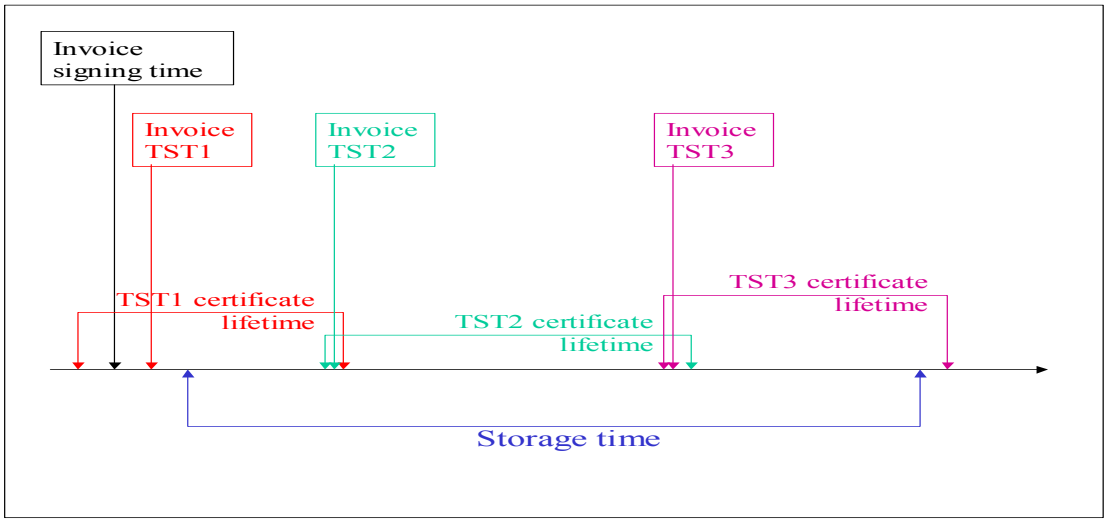

Figure 4 Time Stamp Token Chain

I.4 Short term and long term verification of e-Invoices

Verification of an e-invoice may occur at the following moments:

I soon after it has been issued by the issuer, in order to verify the correctness of the produced binary object; the issuer may want to add a time reference to the signature, by means of a time stamp token or a time mark (time mark: "an audit record kept in a secure audit trail from a trusted third party which attaches [or logically associates ← CWA editor's addition] a date to a signature value" – ETSI TS 102 023);

II upon receipt by the recipient

Note: the recipient may be the final counterpart or an intermediate service provider;

III before the recipient subsequently adds further validity data (countersignature, TST, CRL, etc.);

IV years after the invoice issuance, e.g. by a tax inspector. The inspection may be performed:

a. before expiration of the signing certificate;

b. after expiration of the signing certificate;

c. before expiration of a Time Stamp Token certificate;

d. after expiration of a Time Stamp Token certificate.

Verifications from III onward depend also on the Trust Level of the storage organisation and/or on applicable agreements/legislation.

Case 1 – Basic cryptographic verification

The issuer just performs the "Basic cryptographic verification" by:

1. decrypting the digital signature with the signer's public key included in the supporting certificate, thus obtaining the digest of the document as was calculated when signing;
2. calculating the digest of the signed document with the same hash algorithm used to sign (that is specified in the signature);
3. verifying if both digests are identical.

The issuer may, at this point, apply a time stamp token or a time mark to the signature.

Case 2 – Verification before expiration of the certificate supporting the e-Invoice signature

Short term verification

The e-Invoice recipient performs a "Short term verification" as follows.

1. It is verified if the Certification Authority that issued the certificate supporting the signature is trusted by the verifier.

   Note: how this trust is assessed is outside the present document scope, since it depends on applicable agreements and/or legislation.

2. 2. it is verified if all certificate in the certification path are still valid, i.e. neither expired nor revoked. If any of them is expired then steps in "Long term verification" apply, otherwise the following steps apply.
3. Where anyone of the supporting certificate is not valid:

   a. if there is no time associated to the signature the e-Invoice is to be rejected;

   b. if a time reference is associated to the signature (by means of a TST or a time mark) it is possible to compare it with the revocation time: if the time associated to the signature is before the certificate revocation time the signature was validly issued.

4. If a TST is already associated to the signed e-Invoice, also the TST signature is to be verified in order to trust the time it indicates; this means that items 1 and 2 of this Case 2 are to be performed on the TST signature, and then a “Basic cryptographic verification” as in Case 1 is to be performed on the TST signature.
   Note: verifying a time mark is out of this document scope, as a time mark depends on applicable agreements and/or legislation.

5. If the supporting certificate is valid, performing “Basic cryptographic verification” as in Case 1.

Where applicable, depending on agreements, legislation, storage organisation Trust level, if the signature is verified as valid, a Time Stamp Token or a Time Mark may now be attached/linked to the signature, if not already attached/linked.

After the “Short term verification”

Where applicable, depending on agreements, legislation, storage organisation Trust level, the recipient may choose/be compelled to add certificate status information (e.g. CRL, OCSP Response) to the e-Invoice some time after the “Short term verification”.

In these cases it may be required/advisable to fetch at least the second CRL after signature issuing time, ascertaining if the supporting certificate is not listed as revoked, and then adding/linking this CRL to the signature.

A similar reasoning applies where OCSP Responses are used instead of CRLs.

It may also be required that the CRL or OCSP Response related to the certificate of the CA that issued the signing certificate is to be added/linked to the signature as well.

Before attaching these CRLs/OCSP Responses the “Short term verification” is to be performed.

Where a Time Stamp Token is attached/linked to the signature, and where required by agreements, legislation, storage organisation Trust level, the verifier may apply to the signature also information relative to the validity of the TST supporting certificate, in the same way as above specified.

Case 3 – Long term verification

A verification done after expiration of the signing certificate supporting the e-Invoice signature is a “Long term verification”.

The new cases that arise in this situation are the following:

a. if the verification is performed before expiration of the certificate supporting the first Time Stamp Token and after expiration of the signing certificate;
b. if the verification is performed after expiration of the certificate supporting the latest Time Stamp Token certificate and after expiration of the signing certificate.

Case 3.a – before expiration of the certificate supporting the first TST

1. If the certificate of the CA that issued the signing certificate has expired, it is to be verified if at signing time it was revoked or expired;
2. it is to be verified if at signing time the signing certificate was valid i.e. neither revoked nor expired.

This certificate revocation can be ascertained through the Certificate status information added as specified in section **After the “Short term verification”**.

Case 3.b – after expiration of the certificate supporting the latest TST

As subsequently specified in section **Additional comments**, item 2, a new TST should have been applied before expiration of the certificate supporting the preceding TST certificate, as well as its related certificate status information.

In this case the operations to perform are the following ones.

1. The validity of the most recent TST certificate must be verified: if it is revoked or expired there is no way to ascertain the TST validity and the e-Invoice should be rejected, unless otherwise specified by applicable agreements and/or legislation.
2. If the most recent TST is valid, then the validity of the previous one is to be verified: if its supporting certificate is revoked/expired, then its revocation/expiration time is to be checked against the time indicated in the immediately previous TST; if the time in this TST is before revocation/expiration time of this previous TST certificate, the TST is valid; in the opposite case the e-Invoice should be rejected, unless otherwise specified by applicable agreements and/or legislation.
   The previous operations are to be repeated for each TST in the "TST chain", up to the oldest TST.
3. After having ascertained the validity even of the oldest TST, the signature of the e-Invoice is to be deemed as valid if the time in this TST is before expiration time of the certificate supporting the e-Invoice signature and, obviously, before a possible revocation of such certificate.

Additional comments

1. If the verification is performed before expiration of a Time Stamp Token certificate it technically is a "Short term verification" on such TST and actions as in section "Short term verification" are to be enacted on the TST itself.
2. Before expiration of a TST supporting certificate, a new TST / Time Mark should be applied to the already time stamped signature as well as its related certificate status information (CRL / OCSP Response).
3. In some cases, where required by applicable agreements/ legislation, a recipient, be it the final one (e.g. the customer) or an intermediate one (e.g. a service provider) may want/be required to apply a countersignature to the original e-Invoice. For example: a countersignature may be requested to be applied to a set of e-invoices issued/received within a predefined time frame, regardless of the technical mechanisms to apply such countersignature. In this case the original signatures are automatically "frozen" by the countersignature and their validity is to be assessed as per the applicable agreements/ legislation that may assume they were valid at countersignature time. The countersignature will have to be verified as above specified, consistently with the applicable agreements/legislation.

I.5 Supplying Verification Information – Verification Logging

For verification of an electronic invoice, the validation process will need all the involved certificates and their corresponding status information. In certain member states it is mandatory to supply on the sender as well on the receiver side all necessary information to verify the electronic invoice. Some companies provide this information by generating verification log files. In this verification log files it is logged that the electronic signature was positively verified. Additionally the corresponding status information is included in the log file.

Another way to ensure that the certificates and the corresponding status information are available over the storing period for the relevant tax authorities is to have CAs or other trusted bodies (for example officially recognised providers of storage services) storing the required information according to legal storage obligations.

In this case an electronic signature including references to the complete certificate and related revocation information would be sufficient.

The disadvantage in this case is that only *references* to revocation information that are stored elsewhere are attached. This places these vital data outside the invoice storing organisations' control.

Another possibility to supply the required verification information is to attach already on the issuers side all the relevant validation information to the electronic signatures and the electronic invoice. The verification is less expensive because all the data necessary for the verification is included in the signature and need not to be obtained from a different source. In this case the signature can be verified without accessing any service because everything needed to verify the electronic signature is already included in the format (certificate, CRL, OCSP response). The main advantage is that all relevant data for long-term validity including all relevant certificates and the corresponding status information can be generated already when signing the electronic invoice. This means that the receiver of the electronic invoice has already all relevant data for the verification process. The receiver can store the electronic invoice including without additional information and can guarantee long-term validity without any organizational requirements. On the other side, this signature format has the following disadvantages:

1. the invoice is bloated with additional data; this may be rather heavy where a large number of invoices with the same validation data are issued or received;
2. the invoice issuer has to wait for the "grace period" to elapse before collecting all the relevant certificate status information.

I.6 Examples

I.6.1 Example for a verification log from XiCrypt

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="signature-report.xsl"?>

<report>
  <date day="07" hour="15" minute="42" month="12" second="49"
    type="report" value="2005-12-07 16:42:49 +0100" year="2005"/>
  <isEncrypted value="false"/>
  <isSigned value="true"/>
  <isSignatureOk value="true"/>
  <isSignatureTrusted value="true"/>
  <isOtherError value="false"/>
  <certificate number="0">
    <version value="3"/>
    <serialNumber value="61"/>
    <signatureAlgorithm value="sha1WithRSAEncryption"/>
    <distinguishedName name="issuer">
      <attribute name="countryName" value="AT"/>
      <attribute name="stateOrProvinceName" value="-"/>
      <attribute name="localityName" value="Wien"/>
      <attribute name="organizationName" value="ARGE DATEN - Oesterreichische Gesellschaft fuer Datenschutz"/>
      <attribute name="commonName" value="FREECERT"/>
      <attribute name="emailAddress" value="-"/>
    </distinguishedName>
    <validity>
      <date day="02" hour="00" minute="00" month="12" second="00"
        type="notBefore" value="2005-12-02 01:00:00 +0100" year="2005"/>
      <date day="01" hour="22" minute="30" month="01" second="28"
        type="notAfter" value="2006-01-01 23:30:28 +0100" year="2006"/>
    </validity>
    <distinguishedName name="subject">
      <attribute name="countryName" value="AT"/>
      <attribute name="stateOrProvinceName" value="-"/>
      <attribute name="localityName" value="Graz"/>
      <attribute name="organizationName" value="Testzertifikat"/>
      <attribute name="commonName" value="Dipl. Ing. Markus Wiederkehr,  (Test)"/>
      <attribute name="emailAddress" value="markus.wiederkehr@xicrypt.com"/>
    </distinguishedName>
    <crl>
      <date day="06" hour="19" minute="29" month="12" second="20"
        type="thisUpdate" value="2005-12-06 20:29:20 +0100" year="2005"/>
      <date day="05" hour="19" minute="29" month="01" second="20"
        type="nextUpdate" value="2006-01-05 20:29:20 +0100" year="2006"/>
      <distinguishedName name="issuer">
        <attribute name="countryName" value="AT"/>
        <attribute name="stateOrProvinceName" value="-"/>
        <attribute name="localityName" value="Wien"/>
        <attribute name="organizationName" value="ARGE DATEN - Oesterreichische Gesellschaft fuer Datenschutz"/>
        <attribute name="commonName" value="FREECERT"/>
        <attribute name="emailAddress" value="-"/>
      </distinguishedName>
      <revokedCertificates>
        <serialNumber value="6"/>
        <serialNumber value="37"/>
        <serialNumber value="2"/>
        <serialNumber value="16"/>
        <serialNumber value="19"/>
      </revokedCertificates>
      <derEncoded
        valid="true">MIICTTCCAbYwDQYJKoZIhvcNAQEFBQAwgZMxCzAJBgNVBAYTAkFUMQowCAYDVQQIEwEtMQ0wCwYD
        VQQHEwRXaWVuMUQwQgYDVQQKEztBUkdFIERBVEVOIC0gT2VzdGVycmVpY2hpc2NoZSBHZXNlbGxz
        Y2hhZnQgZnVlciBEYXRlbnNjaHV0ejERMA8GA1UEAxMIRlJFRUNFUlQxEDAOBgkqhkiG9w0BCQEW
        AS0XDTA1MTIwNjE5MjkyMFoXDTA2MDEwNTE5MjkyMFowgfAwEgIBAhcNMDUwOTI5MTUzNzM5WjAS
        AgEGFw0wNTA4MzAxODAxMzRaMBICARAXDTA1MDgzMDE3MDcxMFowEgIBExcNMDUwODMwMjIzMTEz
        WjASAgEYFw0wNTA5MjkxMzM2NThaMBICASUXDTA1MTAwMzE2MTEwMlowEgIBNBcNMDUxMjAxMDgy
        MjE3WjASAgE3Fw0wNTExMjkxNTA5MTNaMBICATgXDTA1MTEzMDE0Mjc0OVowEgIBORcNMDUxMTMw
        MTQ0MzUzWjASAgE6Fw0wNTExMzAxNTMyMjBaMBICATsXDTA1MTIwMTA5NDIwNVowDQYJKoZIhvcN
        AQEFBQADgYEAFeaNFFcQbTQCsgmWLRRHwVBDx2gExY5ZI0PJguDaSgczjwj8Y74QA2Cj3pBTikdX
        dRSjfNUDRrW9Nim2PlQHDyOc/ORlHK38AIefXnLzXa2olBqfNUDqgRK+IWf/GfsjIg63uBCttcKW
39M/NqJ+D/AcY7YQ4DM9U/9AnWyqUJs=</derEncoded>
    </crl>
  </certificate>
  <certificate number="1">
….
  </certificate>
  <certificate number="2">
……
  </certificate>
</report>
```

I.6.2 Example for a verification log from SAP

```
<record name="Message verification" javaclass="com.wm.data.BasicData">
  <value name="verify_status">PKCS#7-Verification completed successfully</value>
  <value name="verify_result">Hash is valid, original message has not been modified. Certificate chain is valid,
message has been signed with corresponding private key</value>
  <value name="verify_timestamp">Thu Oct 07 10:38:45 CEST 2004</value>
  <value name="trust_result">Matching certificate found in trust-dir</value>
- <record name="Signing Certificate Info" javaclass="com.wm.data.BasicData">
  <number name="version" type="com.wm.data.MInteger">3</number>
  <value name="serialNumber">411629918342864242183493444452333 6</value>
  <value name="signature">md5WithRSAEncryption</value>
- <record name="issuer" javaclass="com.wm.data.BasicData">
  <value name="C">DE</value>
  <value name="ST">Hamburg</value>
  <value name="L">Hamburg</value>
  <value name="O">TC TrustCenter for Security in Data Networks GmbH</value>
  <value name="OU">TC TrustCenter Class 0 CA</value>
  <value name="EMAIL">certificate@trustcenter.de</value>
  </record>
- <record name="validity" javaclass="com.wm.data.BasicData">
  <value name="notBefore">25.11.03 15:17</value>
  <value name="notAfter">24.11.04 15:17</value>
  </record>
- <record name="subject" javaclass="com.wm.data.BasicData">
  <value name="C">CH</value>
  <value name="L">Wallisellen</value>
  <value name="O">PayNet (Schweiz) AG</value>
  <value name="OU">TC TrustCenter DEMO</value>
  <value name="CN">Biller Delegation BillingServices (T024)</value>
  <value name="EMAIL">testprofi@paynet.ch</value>
  </record>
  <value name="subjectPublicKeyAlgorithm">RSA</value>
  </record>
  </record>
- <record name="OCSP" javaclass="com.wm.data.BasicData">
  <value name="OCSP_url">https://www.trustcenter.de/cgi-bin/check-rev.cgi/CAF30000000219EEDD4B58B27F48?</value>
  <value name="OCSP_result">OCSP returned: Certificate is valid.</value>
  <value name="OCSP_timestamp">Mi Okt 13 10:23:54 CEST 2004</value>
  </record>
```

I.7 ASN.1 definitions

I.7.1 Extension eInvoicingServiceProvider

```
CWA 15579 ASN1 {  ...  }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL --

IMPORTS

Extension, EXTENSION
   FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 5};

-- Externally defined OIDs
id-eInvoicingServiceProvider OBJECT IDENTIFIER::= {iso(1) identified-organization(3) cen(162) ceninternal(1)
single-part-specification(0) einvoicing-digitalsignature-cwa(15579) certificate-extension-einvoicing-service-
provider(2)}
-- Object Sets
ExtensionSet EXTENSION ::= {
    authorityKeyIdentifier |
    subjectKeyIdentifier |
    keyUsage |
    extendedKeyUsage |
    privateKeyUsagePeriod |
    certificatePolicies |
    policyMappings |
    subjectAltName |
    issuerAltName |
    basicConstraints |
    nameConstraints |
    policyConstraints |
    cRLDistributionPoints |
    subjectDirectoryAttributes |
    authorityInfoAccess |
    eInvoicingServiceProvider, ... }

-- Private extensions
-- eInvoicingServiceProvider info extension

eInvoicingServiceProvider  EXTENSION ::= {
    SYNTAX        EInvoicingServiceProvider
    IDENTIFIED BY id-eInvoicingServiceProvider}

EInvoicingServiceProvider EXTENSION ::= SEQUENCE {
                      extnID = 1.3.0161.00000.15579.001
                      critical = false
extnValue ::= OCTET STRING (CONTAINING EinvoicingServiceProvider)
}

END
```

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- PKCS #5 v2.0: Password-Based Cryptography Standard
- G.R. Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings 48 (1979), 313-317
- A. Shamir, How to share a secret, Communications of the ACM 22 (1979), 612-613
- ETSI TS 101 861 Time stamping profile
- ETSI TS 102 042 Policy requirements for CA issuing PKC
- ETSI TS 102 023 Policy Requirements for Time Stamping Authorities
- ETSI TS 102 231 Provision of harmonized Trust Service Provider status information (TSL)
- ETSI TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
- ETSI TS 102 158 Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
- CEN / ISSS CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- CEN / ISSS CWA 14167-2 Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP
- CEN / ISSS CWA 14167-3 Cryptographic module for CSP key generation services protection profile CMCKG-PP
- CEN / ISSS CWA 14167-4 Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
- CEN / ISSS CWA 14169 Secure signature-creation devices "EAL 4+"
- CEN / ISSS CWA 14170 Security requirements for signature creation applications
- CEN / ISSS CWA 14171 General Guidelines for Electronic Signature Verification
- CEN / ISSS CWA 14172 EESSI Conformity Assessment Guidance (8 parts)
- CEN / ISSS CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices
- CEN / ISSS CWA 14365-1 Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects
- CEN / ISSS CWA 14365-2 Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices
- CEN / ISSS CWA 14890-1 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements
- CEN / ISSS CWA 14890-2 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services