



European Forum of Official Gazettes

4th meeting

Helsinki - Tallinn,

14th – 15th June, 2007

Electronic publishing of legislation - towards authenticity

Final report of the working group

presented by

Aki Hietanen

Ministry of Justice

Finland

Electronic publishing of legislation - towards authenticity

1. Introduction

2. On the key concepts

3. Legislative issues on Legal Gazettes - on the relation of the electronic version to the paper version

3.1. On the legal status of the electronic Legal Gazette

3.2. On the specific legal issues of electronic publishing

3.2.1 Simultaneous publishing – is there any need to regulate the publishing order of the paper and electronic version (which is published first)

3.2.2. Is the entry- into-force of the act dependent on the paper version or the electronic version

3.2.3. Is there any reference to electronic signatures in legislative acts on Legal Gazette

3.2.4. Are there acts or decrees or secondary legislation which are published only in electronic form

3.2.5. Is there any force majeure clause if the electronic version is not available

4. On the use of electronic signatures

5. Workflow and chain of confidence

6. On the use of secure servers and certificates in the delivery of electronic Legal Gazettes

7. Other measures of authentication

8. Good practices in the authentication of legal gazettes: a preliminary inventory

8.1. General principles

8.2. Steps towards authenticity – a checklist

Annex List of useful standards and de facto standards

1. Introduction

The Working Group on Authenticity was one of the working groups established by the European Forum of Official Gazettes in September 2004 in Vienna.

Since 2004, there has been clearly a need for the work on this issue. The use of electronic legal gazettes has been growing rapidly. At the same, the number of paper copies of Legal Gazettes and the number of subscribers has been decreasing. Thereby the printing the paper copies has become less cost-efficient.

The working group has analyzed the general context of the authenticity in the electronic publishing of legislation. The authenticity of electronic legislative documents cannot be seen as an isolated issue, but rather as a part of the complicated process of publishing legislation in paper and electronic form.

Since the Forum meeting in Copenhagen in September 2005, there has been ongoing discussion on the authenticity of the electronic Legal Gazettes in most countries. In the majority of countries the paper version of law is still the only authentic one. The approach of the working group has been very pragmatic, based on the experiences of the participating countries. In the participating countries there have been different approaches to solve the dilemma of authenticity of Legal Gazettes.

The methods of authentication of the texts in legal electronic gazettes have been discussed in the working group by delegates from Austria, Belgium, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Portugal and Spain. The group has been chaired by Aki Hietanen (Finland) and the secretary of the group has been Maria Manuela Cruz (the Office for Official Publications of the European Communities).

During the work of the working group, a number of significant changes have taken place:

- Electronic signatures have been introduced in electronic legal gazettes
- Secure servers have been established in the delivery of electronic gazettes
- Certificates have been used with secure servers
- Legislative reforms have been implemented concerning the status of electronic Legal Gazette
- Authentic and consolidated law in electronic form has been made available
- The number of paper copies of Legal Gazette has been cut down

Historically, there are national milestones in the development of electronic legal gazettes:

- **Estonia:** 23.1.2001: the paper and electronic versions are equal; from 1.1.2007: electronic version the only authentic one
- **Belgium** 1.1.2003: electronic version is not authentic, but it is the only version widely available (five paper copies are authentic); in addition a helpdesk with free of charge access described in the law and a summary of legal gazette available at

each court

- **Austria** 1.1.2004: only an electronic version, which is authentic, is available. In addition, non-authentic electronic versions (html/pdf) and five paper copies for archiving
- **France** 1.7.2004: the paper and electronic versions are equally authentic
- **Hungary** 1.1.2006: the electronic version of the legal gazette has been made authentic
- **Portugal:** 1.7.2006 the electronic version became the authentic Official Journal. The acts only become official after their publication on the Electronic Journal at www.dre.pt. The paper version of the Official Journal has not been published after 31.12.2006.
- **Slovenia** 1.1.2007: the paper and electronic versions are equally authentic, in case of conflict, the electronic version prevails.
- **Denmark** 1.1.2008: the electronic version is the only authentic one

The national reports, meeting reports and other documents of the working group are available at the Forum website.

The work of the working group has focused on the following questions:

- 1) What is the relation of the electronic version to the paper version of the legal gazette
- 2) What kind of technical tools are available for the authentication of electronic legal gazettes
- 3) What kind of reliable processes are necessary in the production and distribution of electronic legal gazettes
- 4) What is the quality control in the production chain
- 5) Which tools and methods of authentication are generic and could be used also in other countries
- 6) What level of reliability and authenticity is sufficient
- 7) What kind of guidelines and good practices can be spread within the European Forum of Official Gazettes

The authenticity of electronic legal documents has to be analyzed in the framework of information security and general security attributes of electronic documents.

The relevant **security attributes** of electronic legal documents are

- * Integrity
- * Authenticity
- * Availability
- * Utility (usefulness)
- * Control

These attributes of information are non-overlapping and they refer to unique aspects of information. Any information security breach can be described as affecting one or more of these fundamental attributes of information.

Integrity refers to being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity. For example, data stored on server are expected to be stable – they are not supposed to be changed at random by problems with the operating system. Similarly, application programs are supposed to record information correctly. One additional attribute of integrity could be traceability – the possibility to trace any amendments made to the original texts, in order to guarantee the origin and integrity of the text.

Availability means having timely access to information. For example, a disk crash or denial-of service attacks both cause a breach of availability. Any delay that exceeds the expected service levels for a system can be described as a breach of availability.

Utility equals usefulness. For example, if someone encrypted data on server or disk to prevent unauthorized access or undetected modifications – and then lost the decryption key: that would be a breach of utility. The data would be integral, authentic, and available – they just wouldn't be useful in that form. Similarly, the storage of data in a format inappropriate for a specific computer architecture; e.g., SGML instead of XML, EBCDIC instead of ASCII or DVD-ROM instead of 1.44 Mb diskette.

Control of information usually refers to the ownership of data and to the different possibilities to modify or delete data. The access control to databases with the “original versions” of Legal Gazettes is a typical challenge to the this aspect of security.

As regards **authenticity**, a distinction has to be made between

- a) authenticity of electronic documents
- b) authentication of production processes of electronic documents
- c) authentication of printing and delivery of electronic documents

In the question of authenticity and authentication, some principles are essential.

- 1) The authentication processes should be **effective, efficient, reliable and easy-to-use**.
- 2) The choice of technology, services and technical solutions should emphasize **compliance with standards**.
- 3) **Proportionality** should be stressed: the scope and intensity of the practical measures in the authentication should be in **proportion to the degree of benefits** that the institutions and citizens are expected to have.

Often authenticity equals with reliability. A reliable document or an authentic document is a document endowed with trustworthiness. Specifically, trustworthiness is conferred to a document by its **degree of completeness** and the **degree of control** on its **creation procedure** and/or its **author's reliability**. The author's reliability means in practice for example that a legislative Act is sufficiently authenticated if it is signed by the president or the prime minister.

ISO standard on record management (ISO 15489) defines **authenticity, reliability, integrity and useability** in the following terms:

- An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported.
- A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
- The integrity of a record refers to its being complete and unaltered.
- A useable record is one that can be located, retrieved, presented and interpreted.

In the discussion concerning the quality requirements or criteria for electronic legal gazettes, the Office for Official Publications of the European Communities has analyzed, in addition to availability and authenticity, the following criteria: Accessibility, certification, durability and traceability.

The most suitable means for choosing the type of authentication could be a **cost-benefit analysis, risk analysis or SWOT analysis** defining the strength, weaknesses, opportunities and threats of different methods. This analysis would specify the needs of different target functions. Each need would be evaluated with the four main security criteria : integrity, availability, authenticity and usability. The target of the analysis would be to identify what you may win and what you may lose (confidence, trusted process, etc.) and what is the impact of the choices.

As an example, here is the SWOT analysis

SWOT ANALYSIS OF AUTHENTICATION METHODS
USE OF ELECTRONIC SIGNATURES

<p>Strengths</p> <ul style="list-style-type: none"> - Efficient and reliable methods for authentication - Several techniques and standards available, also open source signatures 	<p>Weaknesses</p> <ul style="list-style-type: none"> - Not necessary if workflow and secure servers are used - Difficulty to choose the most suitable electronic signature - Difficulties in transferring the signature to new document formats
<p>Opportunities</p> <ul style="list-style-type: none"> - Electronic signature is applicable to all legislative documents - Essential part of electronic commerce 	<p>Threats</p> <ul style="list-style-type: none"> - The archiving of documents with electronic signature is problematic - The electronic signature has to be renewed (re-signed) frequently

In a similar manner, the SWOT analysis of the use of secure servers and protocols can be made:

SWOT ANALYSIS OF AUTHENTICATION METHODS

USE OF SECURE SERVERS AND CERTIFICATES

<p>Strengths</p> <ul style="list-style-type: none"> - Efficient method for ensuring the data transfer -Several techniques and standards available, -also open source --Data encryption is used 	<p>Weaknesses</p> <ul style="list-style-type: none"> -Does not guarantee the authenticity of documents -Difficulty to choose the most suitable combination of SSL and protocols -Progress in data encryption outdates the old one (40-bit encryption etc.) -> Risk of intrusion and hacking
<p>Opportunities</p> <ul style="list-style-type: none"> - Experience found in all countries, well-known techniques -Secure server easy to establish and maintain 	<p>Threats</p> <ul style="list-style-type: none"> -The standards and protocols develop constantly

The countries planning to develop the electronic version of the Legal Gazette, have several possibilities and options. Here are some examples:

No specific authentication of Legal Gazette

If the producer of paper and electronic version is the same authority, the electronic version may be deemed to be authentic on the basis of the competence of the authority

Use of electronic signatures with Legal Gazettes

If there is no workflow or if there are different processes for paper and electronic versions, it may be useful to attach electronic signatures to the electronic documents

Use of secure servers in the delivery of electronic Legal Gazettes

If there is a secure workflow in the production of the legal gazette, it may be sufficient to use secure servers with certificates

Use of workflow in the production of electronic Legal Gazettes

If the production of legal gazettes is decentralized and there is no secure workflow in the production of the legal gazette, it may be necessary to establish a secure workflow for the whole process or for the printing process

Examples of different approaches

Methods	Country	Remarks
No specification	Belgium United Kingdom Portugal Norway	- legislative changes - no technical projects concerning authenticity of OJ
Use of workflow	Austria Denmark France Portugal Germany Finland	- the scope of workflow varies: - only the publishing - the whole lawmaking process
Use of secure servers and certificates	Estonia France Greece Portugal	- mostly servers with secure https protocol -also open source products
Use of electronic signatures	Austria France Greece Hungary Slovenia	Different signatures: - server signatures -XML-signatures -XaDES-signatures -PDF-signatures

2. On the key concepts

The working group has noticed that there is a plethora of concepts used in the discussion on electronic publishing of legislation. To clarify the differences between the key concepts, the working group has drawn up a list of key concepts with short descriptions or definitions.

The key concepts in the electronic publishing of legislation are:

- Authenticity / Authentication of electronic documents
- Chain of confidence
- Digital or electronic signature / Advanced or qualified electronic signature

- Electronic document
- Official electronic version

Authenticity

Authenticity is referring to the quality and credibility of the electronic document (in this case the electronic act or the electronic legal gazette). It has something in common with genuineness, legitimacy, undisputed credibility, believability. Authentic implies being fully trustworthy as according with fact and with regard to documents in law, authenticity (Greek: αυθεντικός, from 'authentēs'='author') is the truthfulness of origins, attributions, commitments, sincerity, and intentions; not a copy or forgery. As regards electronic legal text, authenticity means that text published is **provided by the competent authority**, that the text has **not undergone any substantial modification** and that the text read today is **strictly identical to text** first released perhaps 50 years ago.

Webster's 1913 dictionary defines authenticity as *the quality of being authentic or of established authority for truth and correctness*. It also refers to genuineness; the quality of being genuine or not corrupted from the original. In the electronic world and digital materials, authenticity means that the digital material is what it purports to be. In the case of electronic documents, such as electronic Legal Gazettes, it refers to the trustworthiness of the electronic document as a document. The authentic version could be described as the complete digital image of the paper version. In the case of originally digital ("born digital") or digitised materials, it refers to the fact that whatever is being cited is the same as it was when it was first created unless the accompanying metadata (e.g. on the amendments or the consolidation of the law) indicates any changes.

On 15 September 2001, the International Organization for Standardization (ISO) published the standard ISO 15489-1, **Information and documentation—Records Management**. This standard, in clause 7.2.2 defines authenticity:

“An authentic record is one that can be proven

- a) to be what it purports to be,
- b) to have been created or sent by the person purported to have created or sent it, and
- c) to have been created or sent at the time purported.

To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.”

Authentication can be defined as the process of verifying that a document or message is authentic and that it has not been altered in route from the producer of the document to the recipient(s). Authentication systems have become an essential part of electronic commerce and e-government via the Internet. Based on a range of encryption techniques, digital signature systems allow organizations and individuals to electronically certify the authenticity of an electronic document. Authentication has also another meaning – the authorization of a person to access an electronic system.

Chain of confidence

A chain of confidence (chaîne de confiance) is a reliable process of producing electronic documents, which can be authentic and official. Usually the chain of confidence utilizes certification and digital signatures. It is important that there are methods for the diagnosis and verification of the integrity of the process and of the different phases.

Digital or electronic signature

A electronic signature is used to authenticate the identity of the sender of a message or of the signer of a document (e.g. act of parliament). It can also be used to ensure the integrity of the original content of a document or message. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped.

In the UNCITRAL Model Law on Electronic Signatures (2001), electronic signature means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

The European directive on a Community framework for electronic signatures (1999/93/EC) defines an electronic signature as: "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication". The directive addresses three forms of electronic signatures. The first one is the simplest form of the "electronic signature" and is given a wide meaning. It serves to identify and authenticate data. It can be as simple as signing an e-mail message with a person's name or using a PIN-code. To be a signature the authentication must relate to data and not be used as a method or technology only for entity authentication.

Advanced and qualified electronic signature

An advanced or secure electronic signature connects the signature more closely with the signatory. A secure electronic signature is defined as "an electronic signature that results from the application of a technology or process prescribed by regulations."

In the European directive 1999/93/EC, the second form of electronic signature defined is the "advanced electronic signature". This form of signature has to meet the requirements defined in Article 2.2 of the Directive. In this article, advanced electronic signature is 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

The European directive is technology neutral but in practice, this definition refers mainly to electronic signatures based on a public key infrastructure (PKI). This technology uses encryption technology to sign data, which requires a public and a private key.

In addition, there is a third form of electronic signature mentioned in Article 5.1, which

the directive did not give a term of its own, but which for the purposes of this report will can be called “qualified electronic signature”. This consists of an advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device and needs to comply with the requirements in Annex I, II and III of the European directive.

An example of the use of qualified electronic signature is in the Austrian database of authentic legislation (BGBl Authentisch), where there are four formats available: html, pdf, word and authentic XML text. In the Austrian service, the digital signature can be viewed and verified separately.

Electronic Document

An electronic document is defined as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."

Official electronic version is a version of the law published in electronic form and being recognized by the national authorities as an official electronic document. The official electronic version may have a similar status as the paper version of law. The status of the electronic version can be based on a specific act, administrative procedure or other authorization. The official electronic version can be equal to the paper version of the legal gazette or (as in some countries) the electronic version can be the only official version.

3. Legislative issues on Legal Gazettes - on the relation of the electronic version to the paper version

3.1. On the legal status of the electronic Legal Gazette

Among the member states of the European Forum of Official Gazettes, there are different approaches to the legal status of the electronic Legal Gazette.

1) *The traditional approach*

The traditional approach in the definition of the legal status has been that the paper version is the only authentic and legally valid version of the Legal Gazette. In addition, it has been possible to publish unofficial, unauthentic electronic versions of the Legal Gazette, mostly for information purposes and for easier access to the materials of the Legal Gazette. Usually these electronic gazettes are available in html or pdf formats. Nowadays the traditional approach is still valid in a large number of European countries.

2) *The balanced approach*

The balanced approach in the definition of the legal status made progress in the late 1990s in a number of countries. In the balanced approach the paper version and the electronic version have the equal legal status. However, in case there is a difference in the content of the paper version and the electronic version, the paper version is usually the only authentic one.

In **France**, since 1.6.2004, with the authenticated Official Journal, the electronic publication has acquired an equivalent status with the paper version of the Official Journal and, by coming out at the same time as the paper version, constitutes the official publication of legal acts. The electronic Official Journal is not identical with the paper journal, due to the question of anonymising regulatory acts relating to the status of individuals. Name changes or naturalisation are sensitive issues and therefore the notices or act including information on name changes or naturalization are not published digitally.

Another example of this balanced approach is the **Estonian** act on the Legal Gazette (Riigi Teataja) in 1999. According to the act (§ 1),

(1) The *Riigi Teataja* is the official publication of the Republic of Estonia. The *Riigi Teataja* shall be published on paper as printed matter and electronically on the Internet.

(2) Legislation, notices and other documents published in the *Riigi Teataja* which is on paper and in electronic form have equal legal force, unless this Act provides otherwise.

NB: In Estonia the Riigi Teataja Act has been amended in such a way, that the electronic version is the only authentic one from 1.1.2007 onwards and there will be only five paper copies for archiving.

Another balanced and efficient approach to authenticity can be defined as declaratory authenticity. In declaratory authenticity, the authenticity of electronic version is defined either by

- 1) national law, for example with the definition that "the electronic version has the same legal status as the paper version" or the "the electronic version is the only authentic version"
- 2) or by declaration, tradition or administrative principle:
the declaration can be based on the competence and authority of the publisher or on general reliability of the source. This is the case for example in the United Kingdom and Norway.

3) The information society approach

The information society approach in the definition of the legal status is a fairly recent one. During the last four years there has been - in a number of countries - new legislation on the paper and electronic versions of the Legal Gazette. These new legislative acts define the electronic version as the primary authentic version. In comparison to the traditional approach, the situation is upside down: it is possible to publish unofficial, unauthentic paper versions of the Legal Gazette, mostly for information purposes and for the archiving of the materials of the Legal Gazette. In some countries, the number of these paper copies has been limited to 4-6 copies.

Belgium was among the first countries to reduce the number of printed copies. The situation in Belgium is now as follows: the distribution to the public has been carried out exclusively online since 1.1.2003. Only five paper copies of each legal gazette are produced (for the Ministry of Justice, Moniteur belge, National Library and National Archive and one for microfilming) for different purposes: archiving, accessibility, and continuity of the principle of publication. The only way for individuals to consult the official journal is in Pdf format on the secure site of the Federal Ministry of Justice www.moniteur.be. A free-of-charge helpdesk for facilitating access to the online version was created on 1 August 2005, and since 15 October 2005 almost every courthouse has been obliged by law to make paper summaries of the legal gazette available for the public.

In **Austria**, from 1.1.2004 the publishing of the Legal Gazette was reformed. The legally binding Austrian Federal Law Gazette, with electronic signature, is only published in the Austrian Legal Information System. According to the Federal Act on the Federal Law Gazette (Bundesgesetzblattgesetz BLBlG, 2003:100, § 7) "legislation to be published in the Federal Law Gazette shall be available for access on the internet at the address www.ris.bka.gv.at. Each issue of the Federal Law Gazette shall make reference to this address." The unofficial paper copies still exist for archiving purposes (§8): "At least three backup copies and four certified printouts shall be made of each document. One backup copy and certified printout each shall be delivered to the Austrian National Archive and to the Austrian National Library to be filed there. One certified printout shall be forwarded to the Library of Parliament."

In **Slovenia**, a reform was carried out in 2005. In the Slovenian Official Gazette Act of 2005, the new approach is clear (articles 1 and 4): “The Official Gazette shall be published in electronic form and in printed version. Electronic edition of the Official Gazette shall be safely electronically signed and published on the website of the public company Uradni list Republike Slovenije.” “The electronic edition and printed version of the Official Gazette shall be published on the same day. When both editions are not published on the same day or do not contain the same text, *the electronic edition shall apply.*”

In **Portugal**, on 1.7.2006 a new Act on the Official Journal entered in force, changing the organization, the entry in force and the distribution of the Official Journal.

The official journal Diário da República was reduced from three to two series. The first series used to be divided in two parts, which now were incorporated into one. The third series, the content of which dealt with societies was discontinued. The acts of establishing and modification of the societies, which represented 80% of the 3rd series, were moved to another website.

Since the 1st of July 2006 the electronic version became the authentic Official Journal. The acts only become official after their publication on the Electronic Journal at the website www.dre.pt

The paper version of the Official Journal was discontinued on the 31st of December 2006. It will be possible to have the paper version of the 1st series, but only for the private societies and general public, at real prices and only for informational purposes. It is forbidden the distribution of the paper version to the government and to the local and regional administration.

3.2. On the specific legal issues of electronic publishing

In the electronic publishing of legal gazettes, there is a number of specific issues which have to be analyzed.

3.2.1 Simultaneous publishing – is there any need to regulate the publishing order of the paper and electronic version (which is published first):

In most European countries, the paper and electronic versions are published simultaneously, although in practice the electronic version is naturally available earlier than the paper version.

3.2.2. Is the entry- into-force of the act dependent on the paper version or the electronic version

Traditionally, the acts have entered into force on the day when the paper version is

available or some days (“one day after the publication date of the legal gazette” or “within five days” etc.). The electronic publishing has changed this situation. Today, in a number of countries (e.g. Austria and France), the act enters into force on the day it is published in electronic form. According to the Austria legislation (BGBIG § 11), “Unless therein or by law specified differently, publications in the Federal Law Gazette whose contents are binding shall be effective as of expiry of the day of release for access. Each issue of the Federal Law Gazette shall contain this date.

Similar changes are being prepared e.g. in Estonia.

3.2.3. Is there any reference to electronic signatures in legislative acts on Legal Gazette

The use of electronic signatures in the authentication of legislative acts is reflected also in the legislation. Only in few countries, there is direct reference to the use of electronic signatures. In the Austrian Federal Act on the Federal Law Gazette (§8), it is stated that .

- (1) Documents containing a legislation to be published must have a format warranting upward compatibility. They must have been produced in a reliable process and carry an electronic signature.
- (2) After having been provided with the signature, the documents must not be modified any more and also not be deleted any more after having been released for access.

Similar reference to electronic signature is found in the Slovenia legislation.

3.2.4. Are there acts or decrees or secondary legislation which are published only in electronic form

The lower costs of electronic publishing has contributed to the recent development that in some countries a number of decrees or secondary legislation is published only in electronic form. This kind of electronic-only publishing has been used e.g. in France, Finland and Slovenia (in Slovenia: “*Other instruments, the publication of which is stipulated by law or other regulation, shall be published only in the electronic edition unless otherwise provided by law or other regulation.*”)

In France, Decree No 2004-617 of 29 June 2004 states that certain texts are to be published in digital form only. The texts in question are:

1. Regulatory acts, other than orders, which concern the administrative organisation of the State, in particular decrees relating to the organisation of central administrations, acts relating to the organisation of the decentralised services of the State, and those delegating signature authority within the State's services and its public institutions.
2. Regulatory acts, other than orders, which concern public officials and other staff, judges and servicemen.
3. Regulatory acts, other than orders, which concern the State budget, in particular decrees allocating, opening, cancelling or transferring appropriations, those which concern support funds, account headings of the State Treasury and imprest accounts; and also budgetary and accounting directives.

4. Individual decisions taken by the Economic Affairs Minister in the field of competition.
5. Regulatory acts of independent administrative authorities and independent public authorities having legal personality, other than those concerning the general public.

Furthermore, in France the decree no 2004-459 of 28 May 2004, adopted pursuant to Article 4 of the Order of 20 February 2004, specifies the individual acts which may not be published in electronic form:

The decrees in question are those concerning:

- changes of name
- acquisition, recovery, loss or forfeiture of French nationality
- naturalisation
- gallicisation of forename or surname or assignment of forename

3.2.5. Is there any force majeure clause if the electronic version is not available

The modern view on electronic publishing of legislation is based on the fact that the Internet works and no hacking disturbs the access to law. The possible problems have been taken into account in the legislation of some Forum member states. In Austria, the Federal Act on Federal Law Gazette includes a force majeure clause in §7): “ If and as long as making or keeping legislation to be published in the Federal Law Gazette available for access on the internet is not only temporarily impossible, such publication shall take place in a different manner complying with the requirement of art 49 para 3 B-VG.”

4. On the use of electronic signatures

The electronic signature (as “data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication”) can be related to a person or to an institution (corporate signature, server signature). Today there are a large number of standards or de facto standards of electronic signatures. The electronic signatures can be used as server based signatures or as signatures contained in the electronic documents.

XAdES – a European ETSI standard of electronic signatures

An electronic signature produced in accordance with XAdES standard provides evidence that can be processed to get confidence that some commitment has been explicitly endorsed under a signature policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role. The signature policy specifies the technical and procedural requirements on signature creation and validation in order to meet a particular need.

XAdES extends the original XML Signature Specification with additional syntax and processing necessary to satisfy the European Directive on a Community Framework for Electronic Signatures as well as other use-cases requiring long-term validity. XAdES itself contains several modules that permit varying levels of security such as non-repudiation with time-stamps, certification data and certification archives.

The European **ETSI standard TS 101 733** of XAdES defines formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive and incorporate additional useful information in common use cases (like indication of the commitment got by the signature production).

Electronic signatures of PDF documents

The Adobe Acrobat software supports a number of standards of electronic signatures, especially the so-called PKCS de facto standards.

The best way to find out that a PDF document is authentic and genuine is to check whether the digital signatures (if any) within it are authentic. A PDF document can have two kinds of digital signatures:

- A certification signature, which can be applied by the document’s author. Adobe Reader or Acrobat automatically checks the authenticity of this signature when you open the document, and then displays a window that indicates whether the signature is valid (that is, authentic and current). The certification signature can be described as the “author’s digital signature”.

- A standard signature, which can be applied by anyone who has permission to digitally sign the document. Adobe Reader or Acrobat can automatically check the authenticity of standard signatures when you open the document, or you can check them manually from within the application.

Note: Adobe Reader or Acrobat must have access to the Internet to check digital signatures.

Checking the certification signature of PDF documents

Immediately after a certified Adobe PDF document is opened, Adobe Reader or Acrobat automatically checks for unauthorized modifications to the document and checks the authenticity of the certification

signature. The software then opens a Document Status window that shows one of three results,
• Certification Valid, with a blue ribbon / Validation Of Author Not Confirmed, with a blue question mark next to a person / Certification Invalid, with a red X. A result of *Valid* can provide strong assurance that the document has not been modified and that the document is genuine.

Challenges in the use of electronic signatures

There are several challenges in the use of electronic signatures. The first challenge is in the choice of the most suitable signature. There are several alternatives and each of them have different procedures for the utilization and.

The second challenge is the fact that electronic signatures are aging. The increasing computing power, the possibility of networking, and progress of cryptography contribute to the “weakening” of electronic signatures, i. e. electronically signed documents may lose their probative value over the years. The electronic signatures usually have a limited time of validity. The challenge of renewal of signatures will be significant in the coming years.

The third challenge is related to reform and data transfer. Electronic signatures break when changing the document format. The technological development, harmonization attempts, and also new legal guidelines cause changes of user data and signature formats over the years. With electronically signed documents format changes are problematical, since changing the format breaks the original signature. A similar problem arises during the digitalization of paper documents. If, for instance, a document signed by hand is digitized, the signature loses its validity. The legal authenticity of the transformed document is at least doubtful.

Practices

France

In **France**, there are two types of electronic signatures being used in the chain of confidence. XAdES is used in most cases with higher level of authentication, as a non-intrusive signature and PDF (#PKCS7) as an intrusive signature.

A Time Stamp for the XAdES texts to extend the certificate period of validity (beyond the initial 2 years), in accordance with the RFC 1305 Network Time Protocol; and the specific time stamp protocol ((RFC 3161 Internet X509 PKI Time Stamp Protocol (TSP)). In France the software choice for managing the time stamp has been nCipher Appliance. It includes a new tool to “re-sign” the texts at the certificate's end of validity.

A Crypto Box is being used to keep secure the private keys for the publication's signature. (these keys are not personal keys but these with the name of the official gazette).

Austria

In Austria, an XML based digital signature has been used since 2004. The documents leaving the secure workflow will be signed electronically on an XML basis, using XML-DSIG. It is a server based electronic signature by the Federal Chancellery.

Nachfolgend finden Sie das Ergebnis der Prüfung der eingereichten elektronischen Signatur.

Unterzeichner

Name	Christian Wregar
Organisationseinheit	Verfassungsdienst
Organisation	Bundeskanzleramt
Staat	AT

Aussteller des Zertifikats

Name	a-sign-corporate-light
Organisationseinheit	a-sign-corporate-light
Organisation	A-Trust Ges. f. Sicherung des Verkehrs
Staat	AT

logo

signing person (function)

Informationen zum Zertifikat

Seriennummer	176454
Qualität	gewöhnliche Zertifikat

Prüfungen

Signatur	Die Überprüfung der Hash-Werte und des Werts der Signatur konnte erfolgreich durchgeführt werden.
----------	---

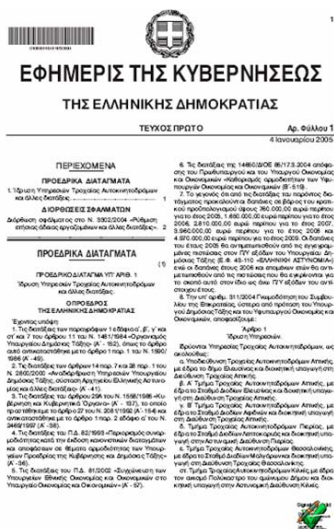
CA and serial number

validity hint

Electronic Document

Greece

In Greece, PDF signature is used in the electronic version of Greek Legal Gazette.



The PDF signature includes a link to the Document Status window or verification page, where it is possible to check the signature data and the validity of the document.

Η υπογραφή είναι ΕΓΚΥΡΗ, υπογεγραμμένη από τον Theodoros Moutouris <tmumu@et.gr>.

Σύνοψη | Έγγραφο | Υπογράφων | Ημερομηνία/Ωρα | Δικαιώματα

Υπογράφηκε από: Theodoros Moutouris <tmumu@et.gr> Εμφάνιση πιστοποιητικού...

Αρτία: Signed PDF (embedded)

Ημερομηνία: 2006/04/18 18:35:04 +03'00' Θέση: Athens, Ethniko Typografic

Σύνοψη επικύρωσης:

- ✓ Το Έγγραφο έγγραφο δεν έχει τροποποιηθεί μετά την υπογραφή του.
- ✓ Η ταυτότητα του υπογράφοντος είναι έγκυρη.
- ⚠ Η ημερομηνία/ώρα της υπογραφής προέρχονται από το ρολόι του υπολογιστή του Υπογράφοντος.

Η υπογραφή δημιουργήθηκε με τη χρήση του Adobe Acrobat.

The Signature is valid

Who signed the pdf

The Date that pdf was signed

The file has no changes

In France, the user of the authentic version of the Journal Officiel can check the validity of the electronic signature and view the certificate.

joe_20070605_0128_0018.pdf

Signature valide

Édition n°128 : Le texte n°18 est valide conformément à son certificat. Cliquez sur le bouton ci-dessous pour afficher le contenu du certificat.

© 2004 Dictao. Tous droits réservés

Voir le Certificat

Fermer

5. Workflow and chain of confidence

Workflow solutions provide organizations with a means of automating and streamlining content-centric processes and managing the lifecycles of those processes efficiently. Workflow solutions are used to develop and optimize multiple types of process automation applications – including processes that involve both systems and people.

Workflow is commonly associated with the electronic processes of managing documents. Workflow handles approvals and prioritizes the order documents are presented. Authenticity by workflow is generally a very demanding effort. In the workflow, the integrity of the electronic act is secured in a work process from the first draft to the final text published in the Legal Gazette. The workflow can consist of capturing the data from source and transferring the data within one work-flow or between separate work-flows (ministries-parliament)

The chain of confidence is a reliable process of producing electronic documents, which can be authentic and official. Usually the chain of confidence utilizes certification and digital signatures. It is important that there are methods for the diagnosis and verification of the integrity of the process and of the different phases.

The chain of confidence may cover only a part of the production process, for example the final steps of preparing the publication from the materials received from the ministries and the parliament. At the moment, there are very few experiences of either workflow or chain of confidence.

Practices

Austria

In Austria the project e-Recht has prepared a separate workflow for the ministries and for the parliament. The basic ideas of the e-Recht (e-Law) project were:

- replace printed legal texts by digitally signed electronic documents
- provide an electronic workflow for producing legal texts (e.g. law, regulation, announcement, treaty)
- Official publication of the Austrian Federal Law Gazette in the Internet

The legislative process in Austria has been reformulated in the following way:

- A draft of a bill is prepared by a ministry
- The ministry sends the draft bill for internal consultation (expert's opinion) to different interest groups (e.g. trade unions, chamber of commerce)
- The draft bill can also be put into RIS legal information system
- Decision of the Council of Ministers (which is a weekly meeting of the Austrian federal ministers)
- The draft bill becomes a government bill and has to be put into RIS
- The government bill is transferred from the Government to the Parliament which runs an independent system
- The government bill is discussed by the Parliament
- The decision of the Parliament is transferred back to the Federal Chancellery

- Signing by the Federal President and countersigning by Federal Chancellor on paper
- Server based electronic signature by the Federal Chancellery
- Official publication of the authentic version of the Federal Law Gazette in the public RIS information system <http://ris1.bka.gv.at/authentic/index.aspx>

In the drafting of draft bills, documents are written in MS Word supported by the dedicated macros. All documents are structured by legal categories (formats). The correct use of the special templates are necessary for the conversion of the document to XML. Important functions of the templates are automatic format recognition (interactive / quick), E-Law validation (Protocol), creation of a table of contents for the law in the draft bill and comparison of text modules.

In Austria, a specific MOA (Module for Online Applications, with modern security technology, consisting of server modules and security modules for signature creation, signature verification, identification, delivery, etc.) is available free of charge (except of 3rd party libraries)). There are different types of workflow for laws, regulations and treaties.

France

In France a chain of confidence was in the beginning only in the publishing process.

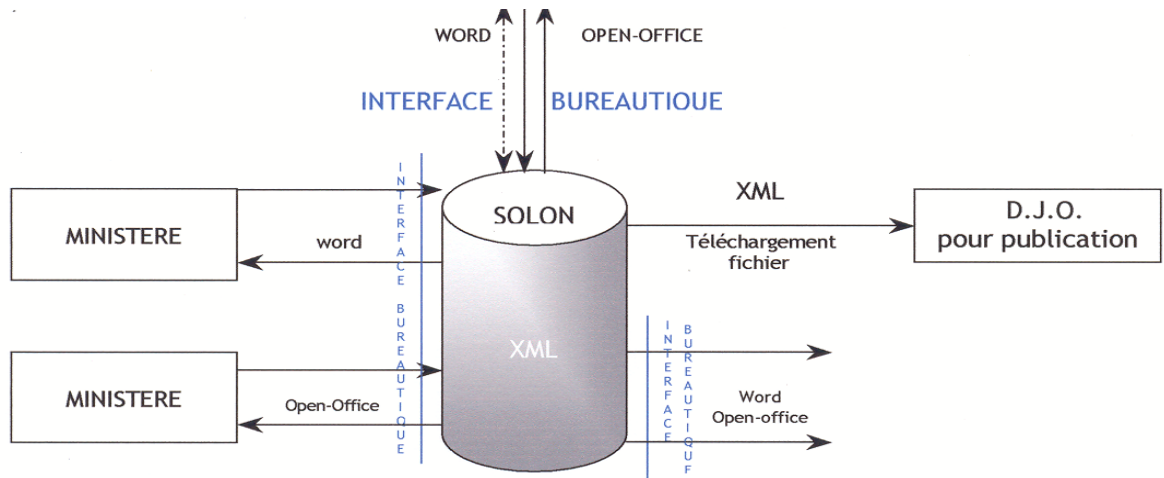
The chain of confidence was organised by the Official Journals Directorate for the purpose of authenticating the electronic version of the Official Journal. The chain of confidence was based on the probative value of electronic evidence given the same status as the traditional paper document. To back up this principle, the legislator allowed two conditions on the principle of equality:

"that it should be possible for the person from whom it emanates to be duly identified and that it should be kept under conditions that will ensure integrity."

These conditions were incorporated in the chain of confidence.

In France, a Government workflow a system called SOLON has been established (SOLON = Système d'Organisation en Ligne des Opérations Normatives).

The object of SOLON is to manage the flow of primary legislation for the relationship between the ministries and the parliament and the flow of secondary legislation. SOLON is to insure the validation flow (with corrections, if needed) of a text already written until publishing.



This project is managed by the General Secretary of the Government, technically realised by SAP and hosted by a private company at equipment level. The Official Journal is part of the technical team working on the project. SOLON is the front end of the Official Journal production.

The basis of the system is the SAP software but SOLON needs some specific functions done by parameterisation and some extra developments to personalize the tool. The preliminary work, necessary to get texts written corresponding to primary legislation or secondary legislation, is not part of SOLON. The data capture is done with Microsoft Word before downloading the content into Solon and the users must use the style sheets designed for the different type of acts produced as e-legislation. The “driving open office” in version number 2 allows an XML translation based on the use of some predefined style sheets.

SOLON system concerns first the secondary legislation, managed by ministries. The primary legislation will use Solon as soon as the secondary legislation will be in full production in 2007. 3 ministries are connected, plus the Official Secretary of the Government and the Official Journal. The Solon’s access is at ministries level (cabinet offices, State Council, Assemblies and Prime Minister Secretaries, (contributions) and finally the Official Journal (receptions). SOLON is be used by 500 people. It is really the administrative processing of texts elaboration, for the whole validation flow. SOLON uses the private network of administration called ADER.

Portugal

In Portugal, a system calle RedeLex is being established. RedeLex is the network of the Electronic Legislative Procedure.

The RedeLex project allows the interconnection, in a safe and private network, of some entities and

agencies of sovereignty that participate in the electronic legislative procedure (the Government, the Presidency of the Republic, the Assembly of the Republic and the Constitutional Court). It establishes a connection between this network and the General Secretariat of the Presidency of the Council of Ministers and the National Printing House. The RedeLex will use qualified digital signatures and safe data transmission.

Finland

In Finland a system called PTJ (Government Decision-making System) is the network of electronic legislative procedure. The first PTJ was established in 1995 and the new PTJ2 was introduced in 2005 and it is based on Documentum software. The draft laws are transferred within the system from the ministries to the government sessions and further to the Parliament in structured XML format. The tools for the actual drafting is MS Word, with tailormade templates and macros.

6. On the use of secure servers and certificates in the delivery of electronic Legal Gazettes

The use of secure server or secure protocol in the delivery of electronic Legal Gazettes ensures the reliability of any electronic document source and the transfer of data from the server, e.g. from the server of the Legal Gazette. A secure server provides secure connections and the data in the in-transit process between the user and the server is encrypted.

SSL (Secure Socket Layer) server authentication allows users to confirm a Web server's identity. SSL-enabled client software, such as a Web browser, can automatically check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) - such as VeriSign, Thawte or GeoTrust - listed in the client software's list of trusted CAs. SSL server authentication is essential for secure e-commerce or e-government transactions.

An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, protecting private information from interception over the Internet. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering - that is, for automatically determining whether the data has been altered in transit.

Secure sessions and server IDs work in the following way:

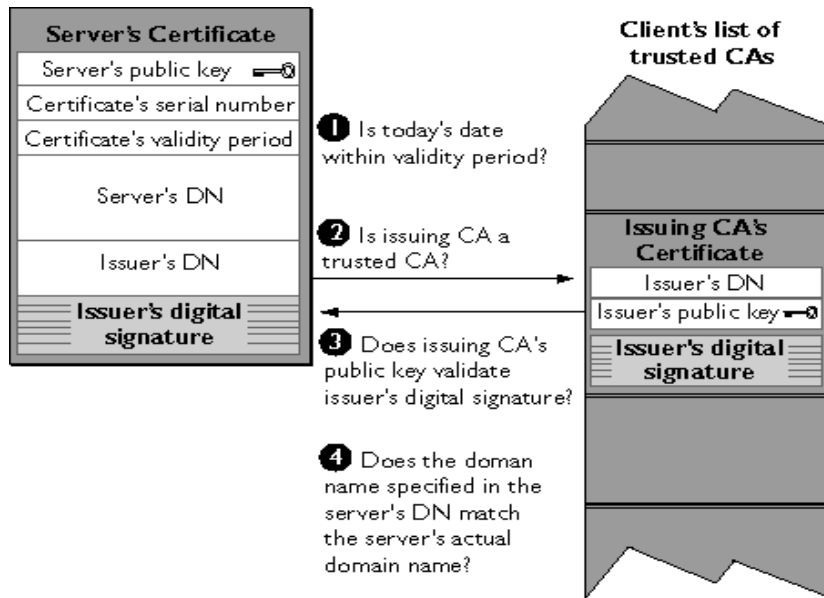
1. A user contacts the site of the Legal Gazette (here: LG) and accesses a secured URL: a page secured by a Server ID (indicated by a URL that begins with "**https:**" instead of just "http:" or by a message from the browser).
2. Legal Gazette server responds, automatically sending the user the digital certificate of the LG site, which authenticates the site.
3. The Web browser of the user generates a unique "session key" to encrypt all communications with the LG site.
4. The browser encrypts the session key itself with the site's public key so only the site can read the session key.
5. A secure session is now established. It all takes only seconds and requires no action by the user. Depending on the browser, the user may see a key icon becoming whole or a padlock closing, indicating that the **session is secure**.

A secure server is a Web server that supports any of the major security protocols, like SSL, which encrypt and decrypt messages to protect them against third party tampering. Major security protocols include SSL, SHTTP (Secure HTTP), PCT, and IPsec (Internet Protocol Security).

A secure protocol (e.g. HTTPS) can be used to protect the transfer of data from a secure server, with security protocol such as SSL, TLS or PCT. Usually the use of certificates (by Thawte, Verisign, Multicert etc.) is recommendable, in order to verify that the address of the web server actually belongs to the publisher of the Legal Gazette.

The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines

to establish an encrypted connection.



The client uses the public key from the Certification Authority's (CA's) certificate to validate the CA's digital signature on the server certificate being presented. If the information in the server certificate has changed since it was signed by the CA or if the CA certificate's public key doesn't correspond to the private key used by the CA to sign the server certificate, the client won't authenticate the server's identity. At this point, the client has determined that the server certificate is valid.

The next step confirms that the server is actually located at the same network address specified by the domain name in the server certificate. Users must perform this step and must refuse to authenticate the server or establish a connection if the domain names don't match. If the server's actual domain name matches the domain name in the server certificate, the client goes on to next step, where the server is authenticated.

The SSL protocol supports the use of a variety of different cryptographic algorithms, or ciphers, for use in operations such as authenticating the server and client to each other and transmitting certificates. The well known algorithms include:

- DES. Data Encryption Standard, an encryption algorithm used by the U.S. Government.
- DSA. Digital Signature Algorithm, part of the digital authentication standard
- RSA. A public-key algorithm for both encryption and authentication, developed by Rivest, Shamir, and Adleman.

Among the open source products, ModSSL module provides strong cryptography for the Apache 1.3 webserver via the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols by the help of the Open Source SSL/TLS toolkit OpenSSL. Additional information can be found at

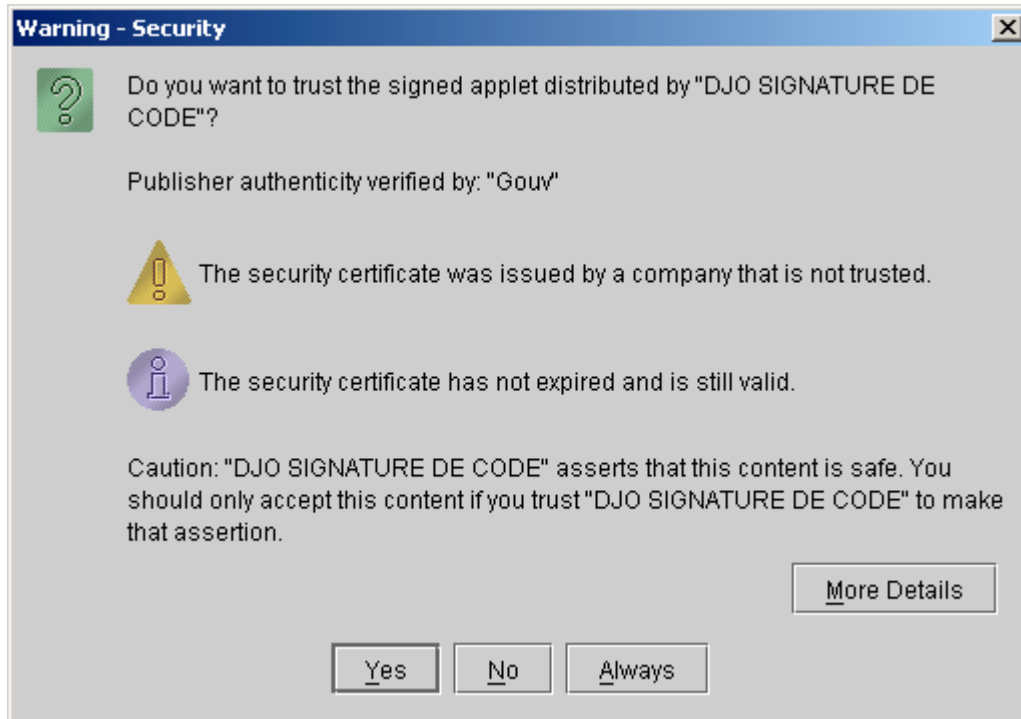
www.modssl.org

On OpenSSL further information can found at <http://www.openssl.org/about/>

Practices

France

A secure server with certificate is used in the French Journal Officiel.



Estonia

In Estonia, a certificate based HTTPS web server has been established for the Legal Gazette. It incorporates a Thawte certificate, which guarantees validity.

Portugal

In Portugal, a certificate based HTTPS web server has been established for the Legal Gazette. It incorporates a Multicert certificate guarantees validity, which means that a root authority has taken steps to verify that the web address actually belongs to the publisher of the Legal Gazette, INCM.

7. Other measures of authentication

7.1. Software for online authentication

In addition to the different measures or methods of authentication of electronic legal gazettes, a number of other measures can be used, as well. In **Hungary**, the user of an electronic legal gazette has the possibility to check on-line the authenticity of the document using specific software. The Hungarian publisher of the legal gazette, Magyar Hivatalos Közlönykiadó, has worked out a separate technological process to the electronic version of legal texts and official journals and this authentication process is based on an SHA-512 algorithm. The electronic version of official journals that was earlier downloaded or purchased somehow can be determined to be official or not. The monitoring program and the instruction for use can be downloaded from the 'Hitelesség' (=authentication) link of the www.magyar kozlony.hu website.

The authentication program (Auth) asks for the location and name of OJ file and sends the hash code made from the user's file to the server of MHK, where – after identification – yes or not answer arrives from. The experience shows that very few of the users have actually used the possibility to confirm the authenticity of the electronic legal gazette in Hungary. The authentication with specific software may be difficult or impossible on certain workstations, if the user is not allowed to install the software.

7.2. Use of time stamps in the resigning of electronic signatures

The validity of the electronically signed legal gazettes or other documents is a serious challenge already in the near future. Usually the electronic signatures are valid for a limited period of time, e.g. 2-3 years.

In France, the Journal Officiel has experience in the resigning of electronic documents. The texts of the legal gazettes will have to be resign after the **outdate of their certificates** (except with time stamping) or algorithms (RSA 1024, RSA 2048, SHA 1). The choice of electronic signatures is very important to minimize the tasks to resign but it is important to check the compatibility with the tools used (Navigators, Adobe reader, Class Java, etc.). In France, in June 2006 the first resigning operation was carried out at the Direction des Journaux officiels: all the texts since 2.6.2005 were resigned (altogether nearly 60 000 files). One week was required to operate the “resignature operation” with good practices. The resign tasks were led by a signatory with a technician and followed a protocol near the original task of signature.

In the use of time stamp standards, a new OpenTSA project has been started. the aim of the OpenTSA project is to develop an RFC 3161 compliant, stable, secure, open source and free time stamping authority client and server application. The following deliverables have already been produced:

- * Time Stamp patch for OpenSSL: The time stamp request creation, response generation and response verification functionality is implemented as an extension to the latest stable version of OpenSSL. This patch adds a new ts command to OpenSSL with which the time stamping operations can be carried out. This patch and the time stamp client have been merged into the official version of OpenSSL and will be available from openssl-0.9.9 onwards.

- * Time Stamp client: A simple command-line driven TSA client that can be used for creating and sending time stamp requests over HTTP or HTTPS to a TSA and for receiving and verifying the

responses. The utility is distributed with the OpenSSL Time Stamp patch.

* Time Stamp module for Apache: This package is an extension module for the latest stable version of the Apache HTTP server. Using the functionality of the OpenSSL Time Stamp patch this module functions as an RFC 3161 compliant time stamp server over HTTP and HTTPS transport protocols, issued time stamp tokens can be stored in a MySQL or a FireBird database. Further information can be found at www.opentsa.org

8. Good practices in the authentication of legal gazettes: a preliminary inventory

8.1. General principles

1) Cutting down the number of paper copies

It is fairly easy to cut down the number of paper copies, if the number of subscribers to the Official Gazette is e.g. 500-2000. Nevertheless, there should be some assistance give to those citizens, who do not have access to the electronic media. One solution is to start a help-desk (like in Belgium), to support the access to paper documents at the local libraries (like in Estonia) or at district courts (Belgium).

For archiving, a few copies should be made and handed over to the National library and National archives.

2) Defining the level of information security and authenticity – how much authenticity is enough?

With electronic copies being utilized to a growing extent, the risk that the electronic copies are not authentic should be kept in mind. For the majority of users, the authenticated electronic versions of acts are not necessarily the most usable ones. For utilizing and distributing the electronic versions, the authentic one may not be best one. This has been found out in the studies in Austria and France. In Austria, currently 51% use the pdf version of the Legal Gazette, 36% use the html version, 11% use the word version and only 2,3% use the authentic version, which incorporates the electronic signature.

There are slightly similar results from Portugal. In Portugal the electronic version is authentic since July 2006. It is accessible via a secure system, using HTTPS, and a non-secure system, with traditional http protocol. Currently only about 7% use the secure system.

3) Using electronic signatures

Nowadays electronic signatures are used with electronic legal gazettes only in a small number of countries (Austria, France, Greece and Slovenia). The signature keys develop fast and in many countries the signature key will have to be changed soon, and a solution has to be found.

One practical problem with electronic signatures is the limited period validity and therefore the long-term archiving is challenge already in the near future.

8.2. Steps towards authenticity – a checklist

1) Check the availability of pdf

Make pdf files available, if the Legal Gazette is not yet available in pdf format

- a. pdf is a standard format in the information market (easy to use, easy to transfer)
- b. xml is another option

2) Check the production chain of the Legal Gazette, in order to make it as secure as possible

- a. checkpoints in the legislative process
- b. checkpoints in the printing house
- c. possible use of electronic signatures and certificates

3) Check the legislation

The legislative norms on the publishing of the electronic version of the legal gazette need to be prepared carefully, taking into account

- i. the legal status of the electronic version: primacy of electronic version or balanced relation between the paper and electronic version,
- ii. entry-into-force of the electronic version and paper version,
- iii. possible need to make reference to the use of electronic signatures in the electronic version
- iv. possibility to publish electronic-only acts/decrees/secondary legislation
- v. the needs of publishing consolidated acts in electronic form
- vi. the access to law: is the electronic version free-of-charge
- vii. force majeure situation: what is to be done if the electronic publishing is not working

4) Check the use of secure servers and certificates

- i. firstly, check and secure the physical protection of document databases and access control to the original databases (firewall etc.)
- ii. establish a secure server e.g. with https protocol. SSL certificates activate the secure padlock using https and assures the visitors that data sent via the Internet are secured by using data encryption.
- iii. utilize secure servers with open architecture and lower costs. E.g. Plone is a ready-to-run content management system that is built on the free Zope application server. Zope is an open source web application server, featuring a transactional object database which can store also dynamic HTML templates, scripts, a search engine, and relational database (RDBMS) connections and code.
- iv. utilize open source server software applications, e.g. Apache SSL.

5) Check the use of electronic signatures: if the use of electronic signatures is preferred, choose the most suitable type of electronic signature for your purposes

- i. is it necessary to use electronic signatures (e.g. when you already have a reliable production process and a secure server)
- ii. if XML-based system, use XML-DSIG or XAdES or OpenXAdES
- iii. if PDF-based system, use PDF-digital signature (based on PKCS#7 standard)

- iv. try to keep the utilization of electronic signatures flexible and at the most suitable level
- v. if archiving is necessary, consider the use of time stamps (easiest with XAdES or general time stamp protocol standard, RFC 3161 Internet X509 PKI Time Stamp Protocol)

6) Check the possibilities to use of workflow and chain of confidence

- i. try to minimize the number of different workflows
- ii. start with a limited scope of chain of confidence
- iii. explore the possibilities to use generic elements (e.g. Austrian Generic elements: Modules for Online Applications) for the signature verification, identification and delivery of documents
- iv. consider the possibilities to use standard software and generic word-processing applications and standards (e.g. DigiDoc)
- v. Specifications have to be well defined and the steps of workflow should be easy to change, if needed
- vi. Software in the workflow should be easy to use and easy to understand
- vii. Which way to progress from Word-keyboarding with style sheets to XML well structured file (with specific XML editor for drafting) ;
- viii. Steps of workflow easy to change.

7) Keep the users informed about your authenticity policy: tell the users what is the level of security and authenticity, use FAQ pages and updated documents on the authentication methods used in your legal gazette

8) Pay attention to the standards and methods used by the contractors and subcontractors.

- i. Use the Common Criteria standards
- ii. Observe the other existing standards (in electronic document management, metadata, longterm preservation of electronic documents, electronic signatures, time stamping, secure servers, etc.)
- iii. Utilize the open source software and open source solutions

9) Check proportionality

- i. Evaluate the costs and benefits of the different techniques and methods
- ii. Consult the users of your services and find out the practical needs of the users of Legal Gazettes

10) Carry out risk analysis

- i. Make a SWOT analysis of the different techniques and methods
- ii. Do not become too enthusiastic about technical solutions

Annex List of useful standards or de facto standards

1. Electronic signatures

- XMLDSIG - IETF/W3CXML – RFC 3275: Signature Syntax and Processing specification, www.ietf.org and <http://www.ietf.org/rfc/rfc3275.txt>
- XML Advanced Electronic Signatures (XAdES), W3C Note 20 February 2003, latest version: <http://www.w3.org/TR/XAdES/>, www.etsi.org

XAdES extends the IETF/W3CXML-Signature Syntax and Processing specification (XMLDSIG) into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the EU Directive 1999/93/EC and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature.

- OpenXAdES is a free software development project aiming at profiling XAdES (XML Advanced Electronic Signatures), www.openxades.org
- PKCS#7 – PKCS#15. PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security. They are not actually official standards, but many of them have in recent years become “de facto standards” with one or more of the standards organizations (notably, the IETF PKIX working group).
- **PKCS #7: Cryptographic Message Syntax Version 1.5**, <http://tools.ietf.org/html/rfc2315>
- PDF electronic signature (uses PKCS#7). www.adobe.com

2. Time Stamp

- RFC 1305 Network Time Protocol; <http://tools.ietf.org/html/rfc1305>
- RFC 3161 Internet X509 PKI Time Stamp Protocol (TSP); <http://www.ietf.org/rfc/rfc2459.txt>
- OpenTSA Open Time Stamp Architecture
- The aim of the OpenTSA project is to develop an RFC 3161 compliant, stable, secure, open source and free time stamping authority client and server application. <http://www.opentsa.org>

3. Secure servers, secure socket layers and computer security

- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
 - Transport Layer Security (TLS): The TLS Protocol, version 1.0, <http://tools.ietf.org/html/rfc2246>
 - OpenSSL and OpenSC, <http://www.opensc-project.org/opensc/wiki/OpenSSL>
- OpenSC provides a set of libraries and utilities to access smart cards. Its main focus is on cards that support cryptographic operations, and facilitate their use in security applications such as mail encryption, authentication, and digital signature. OpenSC implements the PKCS#11 API so applications supporting this API such as Mozilla Firefox and Thunderbird can use it. OpenSC implements the PKCS#15 standard and aims to be compatible with every software that does so. OpenSC is licensed as Open Source software under the LGPL license.

The Common Criteria (CC) standard

- Common Criteria is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140, Common Criteria does not provide a list of product security requirements or features that products must contain. CC describes a framework in which computer system users can specify their security requirements, and testing laboratories can evaluate the products to determine if they actually meet the claims. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. Additional information is found at <http://www.commoncriteriaportal.org/>

Evaluation Assurance Level (EAL)

- Evaluation Assurance Level is part of Common Criteria standard. The numerical rating of EAL is assigned to the target to reflect the assurance requirements fulfilled during the evaluation. Each EAL corresponds to a package of assurance requirements which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL1 being the most basic (and therefore cheapest to implement and evaluate) and EAL7 being the most stringent (and most expensive). Higher EAL levels do not necessarily imply "better security", they only mean that the claimed security assurance of the Target Of Evaluation (TOE) has been more extensively validated.

4. Document formats

- XML Extensible Markup Language. W3C Recommendation 16 August 2006, <http://www.w3.org/XML/>

- GDigiDoc is a GUI frontend built with GTKMM for DigiDoc (alias OpenXAdES - <http://www.openxades.org>) library allowing users to create digitally signed documents and verify signatures of other users. Signatures follow the XAdES (alias ETSI TS 101 903), <http://sourceforge.net/projects/gdigidoc>

- Open architecture for electronic documents

- Reference Model for an Open Archival Information System (OAIS), Management Council of the Consultative Committee for Space Data Systems (CCSDS) 650.0-B-1, Blue Book, January 2002
- <http://public.ccsds.org/publications/archive/650x0b1.pdf>
- in French: [http://public.ccsds.org/publications/archive/650x0b1\(F\).pdf](http://public.ccsds.org/publications/archive/650x0b1(F).pdf)

5. Electronic Records Management (ERM) and creation of electronic documents

- Information and documentation — ISO standard 15489, parts 1 & 2
- MoReq – Model Requirements for the Management of Electronic Records. Published by the Office for Official Publications of the European Commission, 2002, ISBN 92-894-1290-9.
- ISO 12651:1999 Electronic imaging - Vocabulary
- ISO 12652 Technical report on planning considerations addressing preparation of documents for scanning system
- ISO 12033 Electronic imaging - Guidance for selection of document image compression methods
- ISO/TS 12022:2001 Electronic imaging – Guidance of document image compression methods

6. Access controls

- ISO/IEC 15816:2002 Information technology - Security techniques - Security information objects for access control
- ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for

information security management

- ISO/IEC 18028-1:2006 Information technology - Security techniques - IT network security - Part 1: Network security management

7. Storage, search & retrieval of electronic documents

- ISO 15801:2004 Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability
- ANSI/AIIM TR25-1995 – The use of optical disks for public records www.aiim.org
- Information retrieval protocol (ANSI Z39.50/ISO 23950)

8. Metadata

- The Dublin Core Metadata Initiative (DCMI) www.dublincore.org
- AIIM (Integrated EDM/ERM Functional Requirements) www.aiim.org
- Information and documentation — ISO 15489, parts 1 & 2
- MoReq - Model Requirements for the Management of Electronic Records, IDA/European Commission 2001
- Records Management processes - Metadata for records – ISO 23081, part 1
- Information retrieval protocol (ANSI Z39.50/ISO 23950)

9. Digital longtime preservation and electronic archiving

- ISO 19005-1:2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
- ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model
- Digital Preservation Coalition – <http://www.dpconline.org>
- PRONOM - <http://www.nationalarchives.gov.uk/pronom/>

10. Security classification

- ISO/IEC 15816:2002 Information technology - Security techniques - Security information objects for access control
- ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management

11. Legislation and regulations

- ISO 12654 - Electronic imaging -- Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk
- ANSI/AIIM TR31-2004 – Legal acceptance of records produced by information technology systems

Sources:

Authenticity of Electronic Records – A Report prepared for UNESCO (ICA Study 13-1), International Council of Archives, Committee on Archiving Legal Matters, 2002

Authenticity Task Force Report, InterPARES research project, www.interpares.org (InterPARES = International Research on Permanent Authentic Records in Electronic Systems)