

EUROPEAN COMMISSION

SECRETARIAT-GENERAL

The Secretary General

Brussels, 29.11.2005

SEC(2005) 1578

ELECTRONIC AND DIGITISED DOCUMENTS

IMPLEMENTING RULES

FOR THE PROVISIONS ON ELECTRONIC AND DIGITISED DOCUMENTS, ANNEXED TO THE COMMISSION'S RULES OF PROCEDURE BY COMMISSION DECISION 2004/563/EC, EURATOM

TABLE OF CONTENTS

I.	ADO	ADOPTION PROCEDURE					
II.	SCOI	SCOPE OF THESE IMPLEMENTING RULES					
III.	DEFI	DEFINITIONS					
IV.	RULES FOR IMPLEMENTING ARTICLE 4(1) – VALIDITY OF ELECTRONIC DOCUMENTS						
	IV.1. General principles						
	IV.2.	IV.2. Principles of management of electronic documents drawn up by the Commission and signed by means of an advanced electronic signature					
	IV.3. Principles of management of electronic documents received by the Commission and signed by means of an advanced electronic signature 10						
	IV.4. Guarantee of integrity of the content of the document, the relevant metadata and their preservation						
V.		ES FOR IMPLEMENTING ARTICLE 4(2) – VALIDITY OF CTRONIC DOCUMENTS	0				
	V.1.	General principles	0				
	V.2.	Due identification of the person from whom the document emanates	0				
	V.3.	Guarantee of integrity of the content of the document, the relevant metadata and their preservation	1				
	V.4.	Types of documents drawn up by the Commission not requiring a signed original (non-exhaustive list)	2				
	V.5. Types of documents received by the Commission not requiring a original (non-exhaustive list)						
	V.6.	V.6. Commission's digitisation procedure					
		V.6.1. General principles	3				
		V.6.2. Formats	3				
		V.6.3. Quality control	3				
		V.6.4. Preservation of original paper copy	4				
		V.6.5. Documentation of the digitisation procedure	4				
VI.	RULI ELEC	ES FOR IMPLEMENTING ARTICLE 5(1) – VALIDITY OF CTRONIC PROCEDURES	5				
	VI.1.	Due identification of the person authorised to be involved in the procedure . 1.	5				
	VI.2.	Protection of content and stages of the procedure against alteration 1	5				
VII.	RULI ELEC	ES FOR IMPLEMENTING ARTICLE 5(2) – VALIDITY OF CTRONIC PROCEDURES	6				
VIII		ES FOR IMPLEMENTING ARTICLE 6(1) AND (2) - TRANSMISSION LECTRONIC MEANS	6				

	VIII.	1.	Priority u	se of the workflow system for structured transmissions	16
	VIII.			ble use of ordinary electronic means for non-structured transmissions.	
IX.	RUL	ES FOR	IMPLEMI	ENTING ARTICLE 7(1) – <u>PRESERVATION</u>	17
	IX.1.	Require	d retentior	n period	18
	IX.2.			he document in its original form or in a form which grity not only of its content but also of its metadata	
		IX.2.1.		conditions applicable to documents not signed cally	
		IX.2.2.		ns applicable to documents bearing a simple or advanced c signature	
	IX.3.	Preserva	ation of ele	ectronic signatures	19
X.				MENTING ARTICLE 7(2) – <u>Electronic file</u>	
	X.1.	Content	of the ele	ctronic file repository	20
	X.2.	Entire li	ife cycle of	f electronic and digitised documents	20
	X.3.	Archite	cture of the	e Commission's electronic file repository	21
		X.3.1.	-	of single storage of the document in a single place duly justified cases	
		X.3.2.	electronic and elec	f requirements depending on the retention period c file repository for the current and intermediate records tronic file repository for the definitive or historica	.s ıl
			X.3.2.1.	Electronic file repository for current and intermediate records	
			X.3.2.2.	Electronic file repository for definitive or historica archives	
	X.4.	Function	nalities of	the electronic file repository	21
XI.	RUL	ES FOR	IMPLEMI	ENTING ARTICLE 8 - SECURITY	23
XII.	. COO	RDINAT	TION BY	THE SECRETARIAT-GENERAL	23
XII	[.ENT]	RY INTO) FORCE	OF THESE IMPLEMENTING RULES	23
XIV	V.ANN VER			IFICATIONS FOR THE CREATION AND HE VALIDITY OF ELECTRONIC SIGNATURES	-
	XIV.	1.	Introduct	ion	25
	XIV.	2.	Creation	of electronic signatures; phase one	25
	XIV.	3.	Creation	and verification of electronic signatures: Phase two	25
XV	. ANN	EX II: L	IST OF PF	RIORITY ELECTRONIC PROCEDURES	27
	XV.1	.Circle1:		27	7

XV.2.Circle 2 :	27
XV.3.Circle 3:	
XVI.ANNEX III: LIST OF ABBREVIATIONS AND ACRONYMS USED)

I. ADOPTION PROCEDURE

The implementing rules are adopted in accordance with Article 9 of the Commission's provisions on electronic and digitised documents,¹ as annexed to the Commission's Rules of Procedure by Decision 2004/563/EC, Euratom.²

II. SCOPE OF THESE IMPLEMENTING RULES

These implementing rules and Decision 2004/563/EC, Euratom supplement the legal framework established by the Commission provisions on document management annexed to the Commission's Rules of Procedure by Commission Decision 2002/47/EC, ECSC, Euratom³ together with their implementing rules.⁴

They cover all electronic born documents and electronic documents resulting from the digitisation of documents originally on a physical medium⁵, as drawn up or received by the Commission and belonging to the <u>Commission's documentary resources</u>^A, and the procedures managed by IT systems.

They are implemented in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data⁶, with the Commission Decision on the security of information systems⁷ and with the Commission's provisions on security, annexed to the Rules of Procedure by Commission Decision 2001/844/EC, ECSC, Euratom.⁸

The basic principle underlining these implementing rules is that an electronic system for document management, procedures or transmission must offer the same guarantees, in terms of security and controlled access to data, as would be provided in the traditional environment of physical media, in particular paper.

They constitute the minimum common standards to be complied with by all Directorates-General and equivalent Services in the Commission.

They may apply, *mutatis mutandis*, under agreements to be concluded between the Commission or its DG's/Services, on the one hand, and external bodies with which the Commission or its DG's/Services intend to have electronic transactions, on the other hand.

¹ For ease of consultation, the articles of the provisions to which the implementing rules relate are reproduced here. 2 = 0.11, 251, 27, 7, 2004, r = 0

² OJ L 251, 27.7.2004, p. 9.

³ OJ L 21, 24.1.2002, p. 23.

⁴ SEC(2003)349/1, SEC(2003)349/2, SEC(2005)1419.

⁵ Such as paper, microforms, etc.

^A In the English translation of Decision 2004/563, the French word "espace documentaire de la Commission" was mistranslated by "Commission's document system", whereas the right translation should have been "Commission's documentary resources". In these implementing rules, the correct wording "Commission's documentary resources" is used.

⁶ OJ L 8, 12.1.2001, p.1.

⁷ Commission Decision of 23 November 1995 [C(95)1510 final], to be replaced by the new Commission decision on the security of information systems used by the European Commission.

⁸ OJ L 317, 3.12.2001, p. 2.

They are supplemented by technical annexes, which will be updated in line with the development of information technologies and the emergence of new standards, by means of circulars adopted by the Secretary-General, in collaboration with the Informatics Directorate-General and the Security Directorate and sent to Directorates-General and equivalent Services for application.

They do not preclude the production of more detailed or more stringent technical standards in specialist areas.⁹

III. DEFINITIONS

The following definitions are added to those contained in Article 3 of the provisions on electronic and digitised documents.

- 1) <u>Audit trail</u>: mechanism incorporated in a computer system which guarantees the traceability and hence the history of the major stages (e.g. identification, receipt, creation, modification, addition, digitisation, filing, destruction, signing, transmission, transfer and archiving) throughout a process for the electronic management of documents, metadata, files or procedures.
- 2) <u>Certification authority (CA)</u>: recognised trustworthy authority which issues certificates enabling the recipient of a document to check that the signature is indeed that of the person who has signed in with his/her private key.
- 3) <u>Circles of parties involved in exchanges of Commission documents</u> Parties involved in exchanges of Commission documents fall into the following three circles:
 - a) <u>circle 1</u>: internal circle made up exclusively of the Commission and its Directorates-General and equivalent Services, which exchange among themselves documents drawn up or received;
 - b) <u>circle 2</u>: semi-open circle made up, on the one hand, of the Commission and its Directorates-General and equivalent Services and, on the other, partner administrations (other institutions, Member States, national public administrations and duly identified bodies with which the Commission has regular transactions) which exchange documents via networks and procedures mutually agreed between the parties;
 - c) <u>circle 3</u>: entirely open circle made up, on the one hand, of the Commission and its Directorates-General and equivalent Services and, on the other, of organisations, non-member countries, commercial businesses, corporate bodies, recipients of Commission payments who are not members of its staff and the citizen, who exchange documents via networks such as Internet, Extranet or electronic mail.
- 4) <u>Certificate</u>: electronic attestation which links signature-verification data to a person and confirms the identity of that person, within the meaning of Article 2,

⁹ E.g. for the award of public procurement contracts by electronic means.

point 9 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.¹⁰

- 5) **<u>Qualified certificate:</u>** qualified certificate within the meaning of Article 2, point 10 of Directive 1999/93/EC.
- 6) <u>**Cross certification**</u>: process by which two certification authorities mutually certify the public key of the other. When two certification authorities conclude a cross certification agreement, they place mutual trust in each other and will rely on the public key certificates and private keys of the other as if they had issued them themselves.
- 7) **<u>Private Key</u>**: private cryptographic key, which must be used only by the signatory to create an electronic signature.
- 8) **<u>Public key</u>**: public cryptographic key, which is used to verify the electronic signature and must therefore be known by the addressee. The identity of the signatory is confirmed by the creation of a certificate containing the public key of the signatory signed electronically by the private key of the certification authority.
- 9) <u>**CommisSign:**</u> Commission certification authority with the role of issuing, signing and managing certificates for use within the Commission.¹¹
- 10) <u>Cryptography</u>: cryptography is one of the elements of the process of coding and decoding messages which ensures confidentiality of the data. It consists in converting data by means of mathematical operations to protect them. It is an essential tool to ensure confidentiality of data, as only authorised persons can view such data. It also guarantees data integrity, as it can detect any unauthorised modifications.
- 11) <u>ECAS</u>: *European Commission Authentication Service*. ECAS is used by the Commission to authenticate users of internal IT systems. This system offers centralised authentication of users with various levels of guarantee concerning the person providing authentication details. With a centralised authentication process it is therefore no longer necessary for each application to use its own authentication process.
- 12) **Digital fingerprint**: the digital fingerprint is to a document what the fingerprint or genetic print is to a person. Technically the fingerprint of a document (*or hash-value*) is the result of a calculation performed by means of an appropriate algorithm to verify that the integrity of the signed electronic document has not been altered.
- 13) <u>**IDABC</u></u>: Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens. The IDABC programme, which came into force on 1 January 2005, helps the Commission and the Member States to meet their legal requirements under a large number of directives and sectoral decisions which require the Community and the Member States to exchange computerised data.</u>**

¹⁰ OJ L 13, 19.1.2000, p. 12.

¹¹ The Commission has offered the services of CommisSign to the Interinstitutional Informatics Committee (CII), on which all the European institutions are represented.

- 14) **<u>Public key infrastructure (PKI)</u>**: infrastructure for issuing and managing keys to permit reliable electronic exchanges.
- 15) <u>Electronic seal</u>: image and text which can be printed with the document containing all the information of the electronic signature, the time stamp and a reference to a system for ensuring validity and integrity.
- 16) **<u>Time stamp</u>**: electronic system used when a document and its metadata are entered into the electronic file repository to serve as proof of the exact date and time of entry. To have probative value, the time stamp must satisfy the following two requirements: 1) the date and time shown cannot be falsified or altered; 2) it must be synchronised with an officially recognised reference clock.
- 17) **Workflow**: automation of a process in full or in part during which documents, information or tasks move from one participant to another, within a working group, in accordance with a set of predefined rules. A workflow system defines, creates and manages implementation of such processes.

IV. RULES FOR IMPLEMENTING ARTICLE 4(1) – VALIDITY OF ELECTRONIC DOCUMENTS

(Article 4(1)) "Whenever the applicable Community or national provision requires the signed original of a document, an electronic document drawn up or received by the Commission satisfies this requirement if the document in question bears an advanced electronic signature which is based on a qualified certificate and which is created by a secure signature-creation device¹² or an electronic signature offering equivalent assurances with regard to the functionalities attributed to a signature."

IV.1. General principles

Only electronic born documents can be signed by means of an electronic signature.

Article 4(1) is about signing as a substantial formality, a situation in which only the advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device is acceptable as it meets the same requirements (authenticity, non-repudiation and integrity) and has the same legal effects as a handwritten signature, in accordance with Article 5 of Directive 1999/93/EC.

As far as possible, the Commission uses the same type of electronic signature,¹³ whatever circle is concerned, or interoperable systems that are transparent for the final user.

The use of an advanced electronic signature within the Commission does not affect the rules of competence under which the signatory is or is not empowered to take decisions binding on the Commission.

Whereas only a small proportion of Commission documents require a signature as a substantial formality in order to be valid, an advanced electronic signature

¹² As defined in Article 2, point 6) of Directive 1999/93/EC.

¹³ For the specifications relating to the creation and verification of electronic signatures, see point XIV, Annex I.

may be required for electronic exchanges in particular within circle 3,¹⁴ which require clear and unambiguous identification of a person, in accordance in particular with the need-to-know principle.¹⁵

The types of electronic documents drawn up by the Commission for which signature is a substantial formality would include minutes and acts to be authenticated pursuant to Articles 11 and 18 of the Commission's Rules of procedure.

The types of electronic documents received by the Commission for which signature is a substantial formality would include documents constituting legal commitments, in particular tenders under public procurement procedures, grant agreements and declarations of expenditure, annual accounts and statements of assurance drawn up, in particular, under the shared management arrangements with the Member States.

IV.2. Principles of management of electronic documents drawn up by the Commission and signed by means of an advanced electronic signature

Within the Commission, the Informatics Directorate-General, assisted by the "Security" Directorate,¹⁶ is putting in place the technical infrastructure and secure devices required for the creation and utilisation of a public key infrastructure in accordance with the rules of Community law governing electronic signatures, in particular Directive 1999/93/EC.

Secure signature-creation devices¹⁷ must, by appropriate technical and procedural means, ensure at the least that:

a) the signature-creation-data used can in practice occur only once and their secrecy is reasonably assured;

b) the signature-creation-data used cannot, with reasonable assurance, be derived and the signature is protected against forgery by the most advanced technology available;

c) the signature-creation-data used can be reliably protected by the legitimate signatory against use by others.

In addition secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

Within the Commission, the "Security" Directorate is responsible for certification services, either because it performs these functions itself or because it concludes, on behalf of the Commission, a contract with a certification-service-provider. When it performs the functions of certification-services-provider itself, the

¹⁴ Within circles 1 and 2 a person can be clearly identified with reasonable assurance by means of a simple electronic signature, as the institution (or the partner institutions in circle 2) have control over all the security aspects of the systems, networks and persons using them. A simple electronic signature is an electronic signature within the meaning of Article 2(1) of Directive 1999/93/EC.

¹⁵ E.g. where the document contains information or data which only the addressee is entitled to know.

¹⁶ The "Security Directorate" is commonly referred to as the "Security Office" in official documents.

¹⁷ See Annex III to Directive 1999/93/EC.

"Security" Directorate puts in place the essential organisational infrastructure to guarantee creation, issue and management of certificates.

IV.3. Principles of management of electronic documents received by the Commission and signed by means of an advanced electronic signature

The Informatics Directorate-General assisted by the "Security" Directorate makes available to the other Directorates-General and Services the infrastructure and software required to read and technically validate an advanced electronic signature in accordance with generally accepted standards and, in particular, as specified in Annex I to these implementing rules.

IV.4. Guarantee of integrity of the content of the document, the relevant metadata and their preservation

Whatever the circle of parties involved and the system used for exchanging documents, the content received is presumed to be equivalent to the content sent unless proved otherwise.

The conditions for preserving the integrity of the content of the document, its metadata over time and, where appropriate, the electronic signature are set out in points IX and X.

V. Rules for implementing article 4(2) – Validity of electronic documents

(Article 4(2)) "Whenever the applicable Community or national provision requires a document to be drawn up in writing without, however, requiring a signed original, an electronic document drawn up or received by the Commission satisfies this requirement if the person from whom it emanates is duly identified and the document is drawn up under such conditions as to guarantee the integrity of its contents and of the relevant metadata and is <u>preserved</u>^B in accordance with the conditions laid down in Article 7."

V.1. General principles

Article 4(2) concerns documents for which signature is not required as a substantial formality. These form the bulk of the administrative documents drawn up by the Commission.

Points V.4 to V.5 deal with electronic born documents. Point V.6 deals with the Commission's digitisation procedure.

Electronic born documents drawn up by the Commission must comply, at the time of their creation, with the format required for the type of procedure concerned.

V.2. Due identification of the person from whom the document emanates

The requirements of the system making it possible to duly identify the person from whom the document emanates are laid down according to the circle

^B In the English translation of Decision 2004/563, the French word "conservé" was mistranslated by "stored", whereas the right translation should have been "preserved". In these implementing rules, the correct wording "preserved" is used.

concerned and the formalism required for the area or the stage of the procedure to which the document relates. The guarantees of clear identification must accordingly be stricter if the document is to have legal effects (e.g. if it sets deadlines or if it contains data which only the addressee is entitled to know). On the other hand, they can be less stringent if the document is a simple exchange of information.

Within circle 1 electronic identification of persons is performed by the ECAS system or any other equivalent certified system.¹⁸ The Informatics Directorate-General is responsible for the operation and maintenance of the identification system (currently ECAS).

Within circle 2 the parties involved in the electronic exchange process must be identified by a system mutually accepted by the parties.

Within circle 3 an outside person can, as appropriate, be duly identified:

- by the use of a simple electronic signature within the meaning of Article 2(1) of Directive 1999/93/EC, unless the clear and unambiguous identification of the author and/or the addressee is required, e.g. for reasons of confidentiality linked to the content of the document to be transmitted;
- by the authentication function required by a Commission application which complies with the principles of these implementing rules;
- by successive acceptance of exchanges of documents by senders/receivers.¹⁹

V.3. Guarantee of integrity of the content of the document, the relevant metadata and their preservation

The required guarantee of integrity of the content of the document and the relevant metadata and the method used to provide this guarantee are directly proportional to the degree of formalism required by the type of exchange of documents concerned.

Whatever the circle of parties involved and the system used for the exchange of documents, the content received is assumed to be equivalent to the content sent unless proven otherwise.

The conditions for preserving the integrity of the content of the document and the relevant metadata over time and where appropriate of its electronic signature are laid down in points IX and X.

¹⁸ ECAS is used for authentication when an IT application is used. For transmission of documents by email, the SECEM *(Secure Electronic Mail)* system offers a guarantee of identification of the sender.

¹⁹ While receipt of a single document may raise doubts as to the author (e.g. simple electronic address), the continuation of exchanges and acceptance of messages increases the guarantees of proper identification of the person. If necessary a check can be conducted at the end of the procedure. This occurs, for instance, with requests for access to documents, where the final decision can give rise to the right to appeal, submission of applications for a competition where a check can be made at the final selection stage.

V.4. Types of documents drawn up by the Commission not requiring a signed original (non-exhaustive list)

These are in particular most documents relating to administrative procedures, whether purely internal (e.g. relations between the administration and officials) or external (relations with the other Community institutions and bodies, Member States, firms or the citizen), in particular:

- a) documents drawn up by the Commission relating to the internal²⁰ or interinstitutional²¹ legislative process. This series comprises not only the preparatory documents themselves but also notes and studies or other reports aimed at evaluating the content or consequences of the legislation to be proposed, and those preparing public documents, such as green papers, white papers, communications, etc.;
- b) certain documents concerning the management of contracts and grants,²² such as information about calls for tenders, reports of opening or evaluation committees;
- c) documents drawn up by the Commission having legal effect in internal administrative procedures (e.g. application of the Staff Regulations);
- d) documents relating to the purely internal operation of a Directorate-General or Service (e.g. minutes of meetings);
- e) documents of an administrative nature drawn up by the Commission and intended to be sent outside (other institutions, Member States, firms, citizen);
- f) documents of a financial or budgetary discipline nature drawn up by the Commission or its Services and intended for the other institutions, the Member States or outside bodies acting under Community policies.

V.5. Types of documents received by the Commission not requiring a signed original (non-exhaustive list)

These are in particular most of the documents relating to administrative procedures coming from Community institutions and bodies, Member States, firms or citizens, in particular mail coming to the Commission from outside, where national or Community legislation or the administrative practice concerned does not require the signed original of the document, for example:

- a) exchanges of information with Member States and other institutions and bodies under Community policies;
- b) requests by citizens for access to documents;
- c) complaints about infringements of Community law;

²⁰ Excluding the authentication of acts, as provided for in the Commission's Rules of Procedure.

²¹ Transmission of such documents can nevertheless require an electronic signature as proof of the origin and of the preservation of the integrity of the content during transmission.

²² This does not mean the contract proper and the grant agreement, which, if they are electronic documents, require an advanced electronic signature.

- d) submission of applications for competitions, selections or unsolicited applications;
- e) supporting documents for the submission of projects and, where appropriate, the submission form itself, following a call for proposals under a framework programme;
- f) statistical and financial data required under Community legislation, in particular those relating to common policies, their management, control or financing.

V.6. Commission's digitisation procedure

V.6.1. General principles

In order to build up, within the Commission, a fully electronic management system for its documentary resources allowing the gradual introduction of exclusively electronic procedures, the Commission is systematically digitising all documents drawn up or received on other supports, in particular paper.

V.6.2. Formats

Documents are digitised in a format which offers guarantees of permanence, legibility over time and facility of access to the information they contain. Without prejudice to other original media,²³ future developments and standards which might be recognised at international level, the digitisation format for paper is:

a) PDF or PDF/ A^{24}

or

b) TIFF image with a minimum resolution of 300 DPI.

These formats are then enriched by an optical character recognition (OCR) procedure leaving the image intact but facilitating searches in the text.

V.6.3. Quality control

The department in charge of digitisation within each Directorate-General or equivalent Service will put in place a verification procedure to provide a reasonable assurance that the digitised document obtained corresponds to the original document in content and form (quality control).²⁵

²³ Such as audio or video files, photographs, films.

²⁴ When documents digitised from paper are entered in the electronic file repository containing the current and intermediate records, the permanent format is PDF, PDF/A or TIFF. When these digitised documents are transferred to the electronic file repository containing the definitive or historical archives, all formats are converted into PDF/A approved by ISO 19005 or equivalent formats depending on developments in technology or standards, provided that the authenticity and legibility of the format in question will be guaranteed over the long term.

Quality control takes place at two levels – automatic and manual. Automatic quality control is provided by the combined digitisation/OCRisation system. In the event of errors relating to the metadata, duplications, etc., the system automatically sends an error message to the digitisation department which corrects them. The manual quality control focuses on the pages (check that all pages of the document have been digitised, especially for documents printed front and back, that the pages have not been inverted, wrongly digitised, etc.).

The strictness of the quality control is directly proportional to the value and/or retention period of the digitised documents.

Without prejudice to the rules concerning the disposal of originals, as a precaution, all documents are kept on their original medium for six months, during which time any errors reported are immediately corrected. Depending on how the DG/Service is organised, these originals can be stored by the Document Management Centre (DMC), by the originating department or by the department in charge of digitisation if it is not one of those two.

V.6.4. Preservation of original paper $copy^{26}$

When the original is a paper copy for which signature is a substantial formality, in accordance with Article 7 of Commission Decision 2002/47/EC, ECSC, Euratom, this original is transferred to the Commission's Historical Archives Service no later than fifteen years after it is produced.

If the original paper copy is required for control or audit purposes, it is preserved during the period stipulated by the rules governing such controls or audits.²⁷ All internal administrative requirements are properly satisfied by production of the digitised electronic document and external administrative requirements can likewise be satisfied.

When the original paper copy is a document for which signature is not a substantial formality and when this original paper copy is not required by any express rules, it is eliminated at the end of the period of quality control and validation of the results of digitisation stage.

Any subsequent requirement to produce the document is properly satisfied by production of the digitised document.

V.6.5. Documentation of the digitisation procedure

The digitisation procedure must, in all cases, be duly documented as follows:

- documentation of the scope;
- documentation of the procedural framework;
- documentation of the validation of results;
- documentation relating to the elimination²⁸ of the original medium.

All documentation relating to digitisation operations must be kept permanently.

²⁶ The rules set out in point *V.6.4*. concern official documents and files which form part of the Commission's documentary resources. They do not prevent users from keeping paper copies they need for everyday management purposes.

For example, Article 49 of the regulation laying down detailed rules for the implementation of the Financial Regulation applicable to the general budget of the European Communities provides that supporting documents must be kept for at least five years following the discharge.

²⁸ Save in cases where the paper original must be kept.

VI. RULES FOR IMPLEMENTING ARTICLE 5(1) – VALIDITY OF ELECTRONIC PROCEDURES

(Article 5(1)) "Where a procedure specific to the Commission requires the signature of an authorised person or the approval of a person at one or more stages of the procedure, the procedure may be managed by computer systems provided that each person is identified clearly and unambiguously and that the system in question ensures that the content, including the stages of the procedure, cannot be altered."

VI.1. Due identification of the person authorised to be involved in the procedure

Within the Commission the computer systems which manage its specific procedures use ECAS or some other equivalent certified system for electronic identification of persons.

VI.2. Protection of content and stages of the procedure against alteration

In order to be able to check that the content of documents and the stages of procedure have not been altered, the computer systems managing procedures specific to the Commission must:

- a) offer effective control measures over rights of access in order to prevent any access, any elimination, any alteration, any illegal, malicious and unauthorised moving of documents, files, metadata and stages of the procedure;
- b) be equipped with systems of protection against virus attacks, hackers, theft, fire, excessive temperature or water damage;
- c) prevent, by various means, any unauthorised change and incorporate integrity mechanisms (via digital fingerprint) to check that a document has not changed over time;
- d) keep an audit trail for each essential stage of the procedure;
- e) save stored data in a safe environment;
- f) provide reliable format conversion and migration procedures in order to guarantee legibility and accessibility of documents throughout their entire retention period;
- g) provide sufficiently detailed functional and technical documentation on the operation and characteristics of the system, accessible at all times to the organisational entities responsible for the functional and/or technical specifications;²⁹ this documentation must be kept up to date and, in the event of a change in the departments concerned, transmitted directly to the new lead departments for the functional or technical aspects.

²⁹ By organisational entities responsible for the functional and/or technical specifications is meant in particular departments which are the project owners of the IT systems (e.g. Secretariat-General or Directorates-General), the Informatics Directorate-General, the Security Directorate, as well as the Document Management Officers (DMO) and IT departments (Information Resource Managers – IRM and their teams) in the Directorates-General and equivalent Services.

VII. RULES FOR IMPLEMENTING ARTICLE 5(2) – VALIDITY OF ELECTRONIC PROCEDURES

(Article 5(2)) "Where a procedure involves the Commission and other entities and requires the signature of an authorised person or the approval of a person at one or more stages of the procedure, the procedure may be managed by computer systems offering conditions and technical assurances determined by agreement."

Computer systems which manage procedures in which the Commission and other entities are involved and for which the conditions and technical guarantees are determined by agreement must offer *mutatis mutandis* guarantees equivalent to the computer systems managing procedures specific to the Commission.

VIII. RULES FOR IMPLEMENTING ARTICLE 6(1) AND (2) - TRANSMISSION BY ELECTRONIC MEANS

(Article 6) "1. The transmission of documents by the Commission to an internal or external recipient may be carried out by the communication technique best adapted to the circumstances of the case.

2. Documents may be transmitted to the Commission by any communication technique, including electronic means: fax; e-mail; electronic form; website etc.

3. Paragraphs 1 and 2 shall not apply where specific means of transmission or formalities connected with transmission are required by the applicable Community or national provisions or by an agreement between the parties."

Article 6(1) and (2) concerns the transmission of documents drawn up or received by the Commission where transmission is not subject to any special requirements, whether such requirements be laid down by law or by simple agreement between the parties.

VIII.1. Priority use of the workflow system for structured transmissions

In order to overcome some of the drawbacks linked to intensive use of electronic mail³⁰ and fax, Commission Directorates-General and Services must put in place workflow systems³¹ wherever possible.

³⁰ The use of electronic mail multiplies the number of copies of any document and makes management difficult and preservation uncertain as they depend entirely on the sending or receiving user.

³¹ Giving preference, wherever possible, to the formula of single storage of the document in a place accessible to all the persons concerned and them alone.

These workflow systems may take the following forms:

- a) electronic form in XML³² format, the metadata of which are entered by the user, which is sent via an internal or external Web application and which contains in an annex that cannot be separated from it the document or documents to be transmitted;
- b) information system managing a process which can contain, in an annex that cannot be separated from it, the documents linked to this process;
- c) information system for transmitting documents in a particular area of activity;
- d) electronic signatory providing a hierarchical validation chain and enabling at all times any person with the necessary access rights to modify, validate/sign or send back the documents to be signed.

VIII.2. Reasonable use of ordinary electronic means for non-structured and/or short-lived transmissions

For non-structured and/or short-lived transmissions the Commission shall make reasonable use of the following means of communication:

- a) the Commission's standard electronic mail system for exchanges of documents which do not fall under a workflow handled by a computer application or which contain only short-lived information;
- b) notification via electronic mail with a hyperlink to the document and the relevant metadata, without the document being sent.

IX. RULES FOR IMPLEMENTING ARTICLE $7(1) - \frac{PRESERVATION}{C}$

(Article 7(1)) "Electronic and digitised documents shall be preserved by the Commission throughout the required retention period D , under the following conditions:

- a) the document shall be preserved in the form in which it was drawn up, sent or received or in a form which preserves the integrity not only of its contents but also of the relevant metadata;
- *b) the content of the document and the relevant metadata must be readable throughout the retention period by any person who is authorised to have access to them;*

³² Structured by means of DTD (Document Type Definitions) or XML schemas.

^C In the English translation of Decision 2004/563, the French word "Conservation" was mistranslated by "Storage", whereas the right translation should have been "Preservation". In these implementing rules, the correct wording "Preservation" is used.

^D In the English translation of Decision 2004/563, the French word "durée de conservation" was mistranslated by "storage period", whereas the right translation should have been "retention period". In these implementing rules, the correct wording "retention period" is used.

- c) as regards a document sent or received electronically, information which makes it possible to determine its origin and destination and the date and time of dispatch or receipt are part of the minimum metadata to be preserved;
- d) as regards electronic procedures managed by computer systems, information concerning the formal stages of the procedure must be preserved under such conditions as to ensure that those stages and the authors and participants can be identified."

IX.1. Required retention period

"Throughout the period required" means at least the "minimum retention period" of a document depending on the administrative rules and legal obligations as stipulated in particular by Article 49 of the Regulation laying down implementing rules for the Financial Regulation,³³ and by the second and third paragraphs of Article 6 of the provisions on document management and their implementing rules.

IX.2. Preservation of the document in its original form or in a form which preserves the integrity not only of its content but also of its metadata

IX.2.1. General conditions applicable to documents not signed electronically

When entering in the <u>electronic file repository^E</u>, the document is preserved:

- in its original format and/or in a permanent format³⁴ throughout the entire period of short- and medium-term accessibility;³⁵
- in the permanent format alone beyond that period³⁶ if it is of interest for the definitive or historical archives and must not be eliminated under the standard administrative practices for review/elimination set out in the "preservation" implementing rules.

Once a document has been entered in the electronic file repository, any change of whatever kind is identified in an audit trail.

³³ Regulation (EC, Euratom) No 2342/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 357, 31.12.2002, p. 1).

^E In the English translation of Decision 2004/563, the French word "dépôt électronique" was mistranslated by "electronic file deposit system", whereas the right translation should have been "electronic file repository". In these implementing rules, the correct wording "electronic file repository" is used.

³⁴ E.g. PDF, PDF/A approved by ISO 19005, structured XML (by means of DTD or XML schemas), TIFF, JPEG or equivalent formats depending on developments in technology or standards.

³⁵ Short- and medium-term accessibility means accessibility relating to documents or files less than fifteen years old. In this connection see the "Preservation" implementing rules [SEC(2005)1419].

³⁶ When documents are entered in the electronic file repository containing the definitive and historical archives, all formats are converted into PDF/A approved by ISO 19005 or equivalent formats depending on developments in technology or standards, provided that the authenticity and legibility of the format in question will be guaranteed over the long term.

IX.2.2. Conditions applicable to documents bearing a simple or advanced electronic signature

Documents drawn up or received by the Commission and signed by means of a simple or advanced electronic signature form part of the Commission's documentary resources as soon as they are registered.

As soon as:

• the electronic document, both in its original format and in a permanent format,

and

• its simple or advanced electronic signature in its original format,

are entered in the electronic file repository, they become part of the Commission's documentary resources.

For each document bearing a simple or advanced electronic signature, the electronic file repository generates and automatically associates with the document a time stamp which serves as proof of the date of entry in the system and certifies that the electronic signature, the key, the algorithm and the digital fingerprint were valid at the time of entry.

Provided this time stamp is generated (with renewals at appropriate intervals depending on security risks³⁷), the validity of the document cannot be challenged on the grounds that any element used to create the original electronic signature, valid when becoming part of the Commission's documentary resources, has been cancelled or become obsolete.

Should it become necessary to produce a paper version of an electronic document issued by the Commission and bearing a simple or advanced electronic signature, the electronic file repository generates the document in a permanent format on Commission headed paper and produces the electronic seal containing all the information of the electronic signature and time stamp, leaving the electronic version as the "original".

IX.3. Preservation of electronic signatures

In order to guarantee the preservation of electronic signatures over time, the electronic file repository referred to in Article 7(2) must offer guarantees that signed documents cannot be altered or that any intentional or accidental alteration can at least be detected.

³⁷ To extend the length of the key, change the algorithm or method in line with developments in technology.

At the time of entry in the electronic file repository, the electronic signature is preserved:

- in its original format throughout the period of short- and medium-term accessibility.³⁸ This electronic signature, in its original format, is stored in the electronic file repository for current and intermediate records;³⁹
- beyond this period⁴⁰ the function of the electronic signature, i.e. to guarantee the integrity and authenticity of the documents, is guaranteed by the electronic repository as such and certified by means of a digital fingerprint. The original formats of the signatures must not necessarily be preserved beyond that period.

X. RULES FOR IMPLEMENTING ARTICLE $7(2) - \underline{\text{Electronic file Repository}^{F}}$

(Article 7(2)) "For the purposes of paragraph 1 the Commission shall set up an electronic file repository to cover the entire life cycle of the electronic and digitised documents.

The technical conditions of the electronic file repository shall be laid down by the implementing rules provided for in Article 9."

X.1. Content of the electronic file repository

As soon as they are registered, all electronic documents must be integrated into the electronic file repository referred to in the second subparagraph of Article 7(2) of the provisions laid down by Decision 2004/563/EC, Euratom, together with all the relevant metadata required by Decisions 2002/47/EC, ECSC, Euratom and 2004/563/EC, Euratom and their implementing rules.

If they are signed electronic documents, the electronic signatures or the certificates of authenticity of these signatures must also be integrated into the electronic file repository.⁴¹

X.2. Entire life cycle of electronic and digitised documents

The Commission's electronic file repository must cover the entire life cycle of an electronic or digitised document, i.e. the stages or periods in the life of a document from when it is received or formally drawn up within the meaning of Article 4 of the provisions on document management, until it is transferred to the Commission's historical archives and opened to the public or eliminated within the meaning of Article 7 of those provisions.⁴²

³⁸ Short- and medium-term accessibility means a period extending up to fifteen years at most.

³⁹ See point X.3.2.1.

⁴⁰ Beyond fifteen years.

^F As explained in footnote E, in these implementing rules, the correct wording "electronic file repository" is used.

⁴¹ See point IX.3.

⁴² OJ L 21, 24.1.2002, p. 25.

X.3. Architecture of the Commission's electronic file repository

X.3.1. Principle of single storage of the document in a single place, except in duly justified cases

The electronic file repository referred to in Article 7(2) is based on a common electronic file repository for all the Directorates-General and Services of the Commission, other than in duly justified exceptional cases which have received the prior approval of the Secretariat-General.

X.3.2. Level of requirements depending on the retention period: electronic file repository for the current and intermediate records and electronic file repository for the definitive or historical archives

The architecture of the Commission's electronic file repository takes account of the fact that the requirements are not the same for short- and medium-term preservation (current and intermediate records) as for long-term preservation (definitive or historical archives). For this reason the electronic file repository is made up of two separate modules:

X.3.2.1. Electronic file repository for current and intermediate records⁴³

When captured in the system, electronic and digitised documents are automatically integrated into the electronic file repository for current and intermediate records in their original and/or permanent⁴⁴ format, together with all the relevant metadata. They remain there throughout the retention period required under point IX.1, unless this period exceeds fifteen years;

X.3.2.2. Electronic file repository for definitive or historical archives⁴⁵

If they are not eliminated under the standard administrative practices for review/elimination,⁴⁶ electronic and digitised documents with a retention period exceeding fifteen years are transferred to the electronic file repository for definitive or historical archives, solely in the permanent format,⁴⁷ together with all the relevant metadata.

X.4. Functionalities of the electronic file repository

The electronic file repository must offer the following minimum functionalities:⁴⁸

- a) registration of documents in accordance with the "Registration" implementing rules;
- b) filing of documents in accordance with the "Filing" implementing rules;

⁴³ See definition given in point III of the "Preservation" implementing rules [SEC(2005)1419].

⁴⁴ See footnote 34.

⁴⁵ See definition given in point III of the "Preservation" implementing rules [SEC(2005)1419].

⁴⁶ See point V.2.4. of the "Preservation" implementing rules [SEC(2005)1419].

⁴⁷ See footnote 36.

⁴⁸ These functionalities may be provided directly by the electronic file repository or by modules communicating with it via an effective interface.

- c) preservation of documents, the relevant metadata and the stages of the procedure in accordance with the "Preservation" implementing rules and these implementing rules;
- d) digitisation in a permanent format, followed by an optical character recognition (OCR) procedure;
- e) migration of format and/or computer environment at sufficient intervals to guarantee legibility and accessibility of documents throughout the retention period required;
- f) management of major historical and language versions of the same document;
- g) time stamp certifying the deposit of the document and the relevant metadata on the date of deposit and renewal of this time stamp at suitable intervals depending on any security risks;⁴⁹
- h) non-alteration of documents bearing an electronic signature, via digital fingerprint (*hash-value*);
- i) access management and control based on the predefined rights of users, owner departments of documents and on the level of accessibility to the documents themselves;
- j) elimination, under the standard administrative practices, of files, documents, metadata and stages of the procedure which are to be eliminated upon expiry of their retention period and preservation of an audit trail of such eliminations;
- k) efficient search tools enabling documents, the relevant metadata and stages of the procedure to be found easily;
- reporting function displaying reports on the basis of predefined criteria, with sorting facilities according to various criteria, and possibility of saving these reports, exporting them or printing them;
- m) material protection of the electronic file repository against any danger of loss or alteration of its integrity (appropriate temperature and levels of humidity, fire and theft detection systems, protection systems against virus attacks, hackers and any other non-authorised access);
- n) regular backups and availability of a mirror site mirroring the entire content of the electronic file repository and ready to take over whenever the emergency plan has to be applied.

The Informatics Directorate-General is responsible for the operation and maintenance of the common electronic file repository, both as regards the electronic file repository for current and intermediate records and the electronic file repository for definitive or historical archives, in agreement with the Secretariat-General and the Commission's Historical Archives Service.

⁴⁹ See footnote 37.

XI. RULES FOR IMPLEMENTING ARTICLE **8** - SECURITY

(Article 8) "Electronic and digitised documents shall be managed in compliance with such security rules as are incumbent on the Commission. To that end, the information systems, networks and transmission facilities <u>used for the Commission's documentary</u> <u>resources</u>^G shall be protected by adequate security measures concerning document classification, protection of information systems and personal data protection."

The information systems, networks and means of transmission used for electronic and digitised documents and allowing them to become part of the Commission's documentary resources must be checked for compliance with the legislation or rules governing security, personal data protection, information systems security and management of access rights,⁵⁰ either directly by the Security Directorate or under its control.⁵¹

Each department owning an information system is responsible for the security of this system in its entirety. If an information system is subject to major changes⁵² after being found compliant, a request for renewal of the statement of compliance is essential.

XII. COORDINATION BY THE SECRETARIAT-GENERAL

The Directors-General and Heads of Service will inform the Secretariat-General, upon formal approval, of all agreements⁵³ they conclude with outside bodies in their area of responsibility, and of the validation procedure put in place for quality control as referred to in point V.6.3, with a view to possible harmonisation on the basis of the most effective criteria.

The Secretariat-General, in close collaboration with the Informatics Directorate-General and the Security Directorate, will draw up and keep up to date a summary list of computer systems complying with the requirements of these implementing rules.

The Secretariat-General, in close collaboration with the Informatics Directorate-General and the Security Directorate, will update the technical annexes in line with the development of information technology and the emergence of new standards.

XIII. ENTRY INTO FORCE OF THESE IMPLEMENTING RULES

These implementing rules will enter into force in accordance with the following timetable:

- from the date of adoption of these implementing rules, Directorates-General and equivalent Services will have six months to inform the Secretariat-General of the list

^G For further explanation, see footnote A.

⁵⁰ As regards personal data protection, see Regulation (EC) No 45/2001 and in particular Articles 4, 21 and 22 thereof concerning the management of access rights.

⁵¹ For the list of electronic procedures identified as having priority see point XV, Annex II.

⁵² "Major changes" means, for instance, an information system intended initially solely for Commission departments (circle 1), but then extended to the other institutions and Member States (circle 2) or to the outside world in general (circle 3).

⁵³ Within the meaning of the second paragraph of Article 2 of the provisions on electronic and digitised documents annexed to the Commission's Rules of Procedure by Decision 2004/563/EC, Euratom.

of electronic procedures referred to in Annex II which can already be considered compliant for the time being and the electronic procedures they would like to make compliant;

- the IT infrastructure, information systems, networks and means of transmission existing at central level will be gradually adapted in accordance with a timetable that the Secretariat-General will lay down in collaboration with the Informatics Directorate-General, the Security Directorate and the Budget Directorate-General, on the one hand, and the Directorates-General and equivalent Services on the other;
- as soon as the adapted IT infrastructure, information systems, networks and means of transmission are made available at central level, the Directorates-General and equivalent Services will take the necessary measures so that the documents, procedures and electronic systems they are responsible for are compliant with these implementing rules. To this end the Directorates-General and equivalent Services will inform the Secretariat-General of an implementing action plan for their DG/Service within six months from the date of availability at central level. The timetable and content of the action plan of each DG/Service will be approved by the Secretariat-General, in collaboration with the Informatics Directorate-General and the Security Directorate.

The Secretary-General

Catherine DAY

XIV. ANNEX I: SPECIFICATIONS FOR THE CREATION AND VERIFICATION OF THE VALIDITY OF ELECTRONIC SIGNATURES

XIV.1. Introduction

Electronic signatures for documents are still rarely used in the Commission. For reasons of effectiveness and pragmatism the Commission has decided to work in two successive phases.

XIV.2. Creation of electronic signatures; phase one

In an initial phase, CommisSign, as the Commission's certification authority and under the responsibility of the Security Directorate, will be responsible for issuing, signing and managing for the Commission <u>non-qualified certificates</u> on which electronic signatures are based.

The Commission's objective is ultimately to use the same electronic signature standard⁵⁴ whatever the circle of parties involved.⁵⁵ Nevertheless, for a transitional period of no more than five years, the Commission's electronic applications or procedures which already use or are about to use – for secure transmissions with the outside world⁵⁶ - PKI of IDABC-type electronic signatures with, for example, Certipost as certification authority, may continue to do so.

XIV.3. Creation and verification of electronic signatures: Phase two

At the end of the transitional period, CommisSign will have to be able to issue, sign and manage for the Commission <u>qualified certificates</u> on which are based the advanced electronic signatures within the meaning of Article 4(1) of the provisions on electronic and digitised documents.

The electronic signature creation and verification systems will be technologically neutral so as to allow receipt and dispatch of electronic documents signed with the following instruments:

 a cross-certification system, including networks of certifiers, multicertification and certification bridge/gateways, as proposed by IDABC

(http://europa.eu.int/idabc/en/document/2318;

- an identification, authentication and signature system integrated in an electronic chip card.⁵⁷ In the case of the Commission, this triple function could be integrated in the staff card of officials and other staff;
- an identification, authentication and signature system integrated in a mobile phone (GSM), smart phone, PDA, etc;

⁵⁴ For instance ETSI TS 101 733.

⁵⁵ See definition in point III, 3.

⁵⁶ E.g. with permanent representations, etc.

⁵⁷ As exists, for instance, in Austria, Belgium, Estonia, Finland, etc.

 an identification, authentication and signature system integrated in a calculator (*token* with PIN code and generation of a volatile number for security purposes).

The Security Directorate is responsible for the operation and maintenance of CommisSign.

XV. ANNEX II: LIST OF PRIORITY ELECTRONIC PROCEDURES

A number of electronic procedures must be declared compliant with these implementing rules or brought into conformity with them.

The following is a non-exhaustive list, broken down by circle of parties involved, which may be extended and/or amended.

XV.1. Circle 1:

- a) budgetary procedures (ABAC, SINCOM2, RAD, etc.);
- b) administrative procedures (SYSPER2, ADONIS/ARES, HERMES, etc);
- c) interservice consultation procedures (CIS-NET).

XV.2. Circle 2:

- a) decision-making procedures (Greffe2000, e-Greffe, parliamentary questions, documents sent by Parliament and the Council, notifications to Member States);
- b) CCN/CSI OLAF interinstitutional procedures, data-transmission exchanges with national administrations and outside bodies, private or public, acting under obligations laid down by Community legislation (common policies, market organisations, shared management of the Community budget), etc;
- c) scrutiny of budget procedures (European Court of Auditors, Parliament's Committee on Budgets and Committee on Budgetary Control, etc).

XV.3. Circle 3:

- a) *E-procurement*, calls for tenders, calls for expressions of interest, calls for proposals, contracts, grant agreements, etc;
- b) access to documents;
- c) complaints (clear identification of complainant);
- d) mail sent to the Commission or its departments from outside;
- f) citizens' petitions (if the Constitution is ratified);
- g) unsolicited applications for a job, requests to take part in open competitions.

XVI. ANNEX III: LIST OF ABBREVIATIONS AND ACRONYMS USED

CA:	certification authority
CCN/CSI:	Common Communication Network/Common System Interface
CII :	Comité informatique interinstitutionnel (Interinstitutional Informatics Committee)
DMC:	Document Management Centre (Centre d'administration des documents – CAD)
DMO:	Document Management Officer
DPI:	Dots per inch
DTD:	Document Type Definition
ECAS:	European Commission Authentication Service
ETSI:	European Telecommunications Institute
GSM:	Global System for Mobile communications
IRM:	Information Resource Manager
ISO:	International Standards Organization
IDABC:	Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens
IR:	Implementing rules
JPEG:	Joint Pictures Experts Group – compressed file format for graphics
OCR:	Optical Character Recognition
OJ:	Official Journal of the European Union
PDA:	Personal Digital Assistant
PDF:	Portable Document Format
PIN:	Personal Identification Number
PKI:	public key infrastructure
SECEM:	Secure Electronic Mail
TIFF:	Tagged Image File Format
XML:	Extensible Markup Language