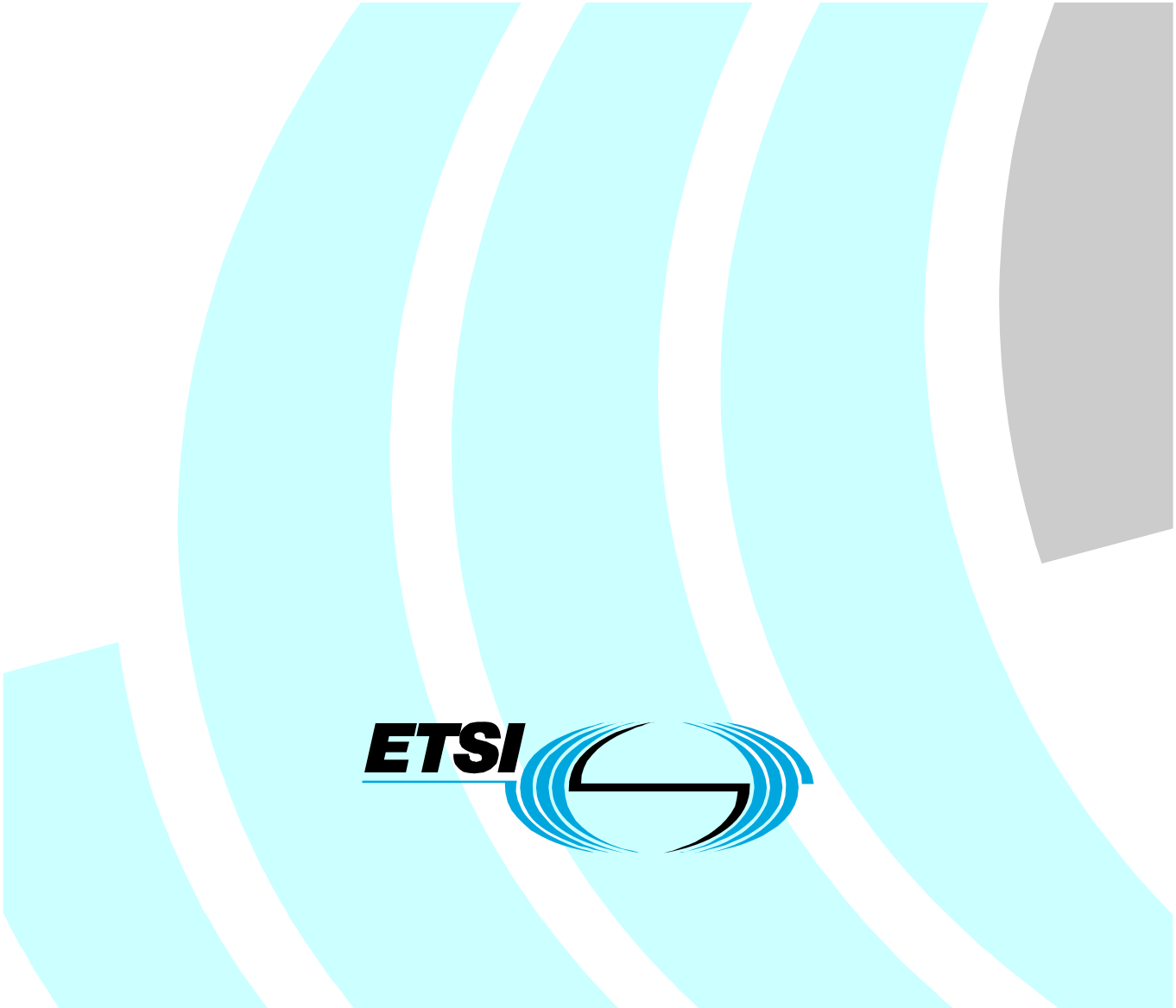
ETSI TR 102 605 V1.1.1 (2007-09)

Technical Report

Electronic Signatures and Infrastructures (ESI); Registered E-Mail



Reference
DTR/ESI-000051

Keywords
e-commerce, electronic signature, security,
e-mail, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

The present document is the result of a study into existing and prospective Registered E-Mail systems in Europe with the aim of identifying requirements leading to standardization in this area.

Business and administrative relationships among companies, public administrations and private citizens, are now more and more implemented electronically. Trust is becoming essential for their success and continued development of electronic services. It is therefore important that any entity using electronic services have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their partners. In this respect the electronic signature is an important security component that can be used to protect information and provide trust in electronic business.

Electronic mail is another major tool for electronic business and administration. It has been recognized that additional security services are necessary for e-mail to be trusted. In some European Union Member States (Italy, Belgium, etc.) regulation(s) and application(s) are already in place on mails transmitted by electronic means providing origin authentication and proof of delivery. Such security services may be used to provide trusted evidence of submission and delivery of electronic mail equivalent to the existing physical registered postal service. Several approaches are possible in order to realize the goal of trusted 'Registered E-Mail' services. This may be enhanced, for example, by other facilities such as sender origin authentication. Also, existing services such as the 'Electronic Postal Certification Mark' (formerly referred to as Digital Post Mark CEN and Electronic Post Mark by Universal Postal Union) provides further electronic evidence about the handling of messages. In order to move towards the general recognition and readability of evidence provided by registered e-mail services, it is necessary to specify technical formats, as well as procedures and practices for handling registered e-mail, and the ways the electronic signatures are applied to it.

Executive Summary

A range of differing services for what is being referred to as Registered E-Mail (REM) are being established in Europe. Registered e-mail is an enhanced form of e-mail which provides evidence relating to the handling of an e-mail including proof of submission and delivery.

The present document summarizes the results of a survey among organizations with interests in REM services for Europe with the aim of identifying requirements for standardization in this area.

The survey described in the present document identified significant deployment of REM with services existing or planned in at least 10 European nations with an existing user community of over 500 000 and potential community of 100 million. The body of the present document also provides information on the basis for these services including the most prevalent forms of evidential services supported in Registered E-Mail services and products, the legal basis for REM. In addition the report identifies how these services are provided and the technical basis for the security features.

The report also surveys the procedural and policy basis for the provision of REM services. Finally, existing standardization activities of relevance to REM including the Universal Postal Union's Electronic Postal Certification Mark (formerly called Digital or Electronic Post Mark) Standard which, whilst it does not define standards for full REM services, has relevance for certain aspects of REM.

The report identifies that there were a range of solution architectures on which existing REM services are based. The basis of a generic architecture is proposed to which solution architectures may be related and which may be used as the basis for future standardization.

The report proposes that further standardization is required for the provision of signed evidence for Registered E-Mail, in particular:

- Architecture for the provision of signed evidence in support of Registered E-Mail.
- Data requirements and formats for signed evidence in support of Registered E-Mail.
- Policy requirements for trust service providers supporting Registered E-Mail.

1 Scope

The present document summarizes the results of a survey among organizations with interests in Registered E-Mail services for Europe including state authorities, standardization bodies, e-mail product and service providers, local experts. The survey included information on Registered E-Mail services outside Europe to place the work within a global context. The survey investigated current and prospective Registered E-Mail implementations with the aim of identifying requirements for standardization in this area.

Registered e-mail is an enhanced form of e-mail which provides evidence relating to the handling of an e-mail including proof of submission and delivery.

Based on this survey and on the results of further work within ETSI, a number of Technical Specifications (TSs) are to be produced for Registered E-Mail. The present document gives specific recommendations as to the scope of these specifications based on the results of this survey.

The results given below include tables giving general data relating to particular questions in the survey. These are given for the **overall** totals for particular questions as well as, in some tables, sums for the following sub-categories:

- Existing **Products** for registered e-mail.
- Existing **Services** for registered e-mail.
- **Regulatory** requirements for registered email including implemented standards.
- **Other** categories of respondent including potential future product products and services, potential users of registered of e-mail, standards to be implemented.

In addition, annex A gives an overview of the main approaches in regulations, products and services.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Informative references

[1] Universal Postal Union S43-3: "Secured Electronic Postal Services Interface Specification".

NOTE: To be published. Formerly entitled Electronic Post Mark Interface Specification.

[2] CEN TS 15130: "Postal Services - DPM infrastructure - Messaging supporting DPM applications".

[3] OASIS Committee Specification Electronic PostMark (EPM): "Profile of the OASIS Digital Signature Service Version 1.0, Ed Shallow, 13 February 2007".

[4] ISO/IEC 13888 (Parts 1 to 3): "Information Technology Security Techniques Non repudiation".

[5] ISO/IEC 27001 "Information technology Security techniques Information security management systems - Requirements".

[6] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service.

[7] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[8] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[9] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[10] W3C/IETF Recommendation: "XML-Signature Syntax and Processing".

[11] W3C Recommendation (version 1.2 parts 0 to 2): "Simple Object Access Protocol (SOAP) , 24 June 2003".

[12] IETF RFC 4510: "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map".

[13] ITU-R Recommendation TF.460-4: "Standard frequency and time-signal emissions".

[14] ETSI TS 101 861: "Time stamping profile".

[15] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

3 Definitions and abbreviations

3.1 Definitions

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

Registered E-Mail (REM): enhanced form of mail transmitted by electronic means (e-mail) which provides evidence relating to the handling of an e-mail including proof of submission and delivery

3.2 Abbreviations

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

AdES Advanced Electronic Signature
AFNOR Association Française de NORmalisation

NOTE: French standards body.

CA Certification Authority
CAdES CMS Advanced Electronic Signatures 8
CEN Comité Européen de Normalisation

NOTE: CEN was founded in 1961 by the national standards bodies in the European Economic Community and EFTA countries that is contributing to the objectives of the European Union and European Economic Area with voluntary technical standards.

CMS Cryptographic Message Syntax 7
CNIPA Centro Nazionale per l'Informatica nella Pubblica Amministrazione

NOTE: CNIPA is an Italian governmental body in charge, among other things, for technical support to legislators in matters of REM and for accreditation and supervision of REM service providers.

CP Critical Path
EPCM Electronic Postal Certification Mark

NOTE: Formerly referred to as Digital Post Mark or Electronic Post Mark.

FTPS File Transfer Protocol over SSL or TLS
HTTPS Hypertext Transfer Protocol over SSL or TLS
LDAP Lightweight Directory Access Protocol
MAP Ministerio de Administraciones Publicas (Spanish Ministry of Public Administrations)
NTP Network Time Protocol
PEC Posta Elettronica Certificata

NOTE: Italian term for Registered E-Mail.

PKI Public Key Infrastructure
REM Registered E-Mail
SOAP Simple Object Access Protocol 11
SLDAP Standard Lightweight Directory Access Protocol
SSL Secure Sock Layer

NOTE: Newer versions of SSL are also called TLS

STNC Secure Telematic Notification Service
TLS Transport Layer Securtiy

TST	Time-Stamp Token
UPU	Universal Postal Union

NOTE: UPU is the primary forum for cooperation between postal-sector players and helps to ensure a truly universal network of up-to-date products and services.

UTC	Universal Coordinated Time
W3C	World Wide Web Consortium
XAdES	XML Advanced Electronic Signature 9
XML	eXtensible Markup Language
XMLDSig	XML Digital Signatures 10

4 Questionnaire

The STF-318 team produced a questionnaire to survey existing and prospective REM systems. This questionnaire was distributed among organizations with interests in Registered E-Mail services for Europe including state authorities, standardization bodies, e-mail product and service providers as well as local experts.

Information on certain REM service providers was not gathered through the questionnaire but are reflected in the present document as those gathered through questionnaire. Some questionnaires reflect more than one variation of a REM implementation (e.g. IncaMail and IncaMail Public).

The STF-318 conducted a process of identification of entities that could potentially be interested in answering such a questionnaire throughout all Europe, also including pan-European and worldwide entities.

This questionnaire (see annex B) contains 73 multi-choice questions organized in 10 sections with a place for respondent to enter other choices and further information. These sections survey information as follows:

- Section 1 of the questionnaire addresses the profile of the respondent to the questionnaire. This allowed to the team to address a study of both, existing and prospected REM systems on a per-country basis, as well as what specific profiles have the entities that have shown more interest in answering the questionnaire, i.e. in REM systems.
- Questions in section 2 aim at getting clear information of the extent of REM market by addressing a number of relevant points, as follows:
  - Whether the answers given in the questionnaire relate to:
    - a specific REM service implementation, and if so the current status of such a service;
    - a specific REM product and if so its presence in the market;
    - a certain regulation, or standard and if so its degree of deployment.
- The market sectors addressed by these REM systems, and the current and expected number of users of such a systems.
- Questions of section 3 are focused on different services that the STF-318 team has identified as potentially relevant for REM systems, as well as on the type of users and business areas they directly support. Different kind of services where addressed:
  - Evidence provision. A pre-identified evidence services set appears in the questionnaire, with options to add further evidential services.
  - Security related services (confidentiality, malware absence verification, etc).
  - Gateway to other mail services, whether regular postal services or regular e-mail.
- Questions of section 4 aim at getting details of current laws and regulations that identify requirements or assign specific legal validity to the services provided by REM systems in several European Union Member States and States from outside the EU, and on the evidential value that the legal frameworks assign to the aforementioned evidences.

- Section 5 contains questions that aim at getting details on how the system is designed to provide the different services already mentioned. First of all the questionnaire presents one REM system model where relevant entities exchange information (see clause 8.2): REM providers, sender, recipient, security services providers and gateways to postal mail or to and from regular e-mail. Respondents were asked to indicate whether the model applies to the system they are providing details for. If so each clause in clause 5 makes questions on a specific entity or on a dialogue maintained between two entities of the model. Relevant issues addressed at these clauses are, among others: entities authentication (and employed mechanisms), evidences of entities authentication (and the mechanisms employed), provision of other evidence services, and messages identification.

- Questions of section 6 deal with different technical issues, including: signature formats, time-stamp formats, time-marks implementations, security protocols, used PKI and signature supporting services.

- Section 7 addresses REM systems reported security policies and practices: registration requirements (if registration is actually required), operation of the system under an ISO/IEC 27001 [5] based Information Security Management Service, used signing device, etc.

- Section 8 is an empty space that respondent may fill with whatever additional information they consider relevant to provide.

- In section 9 respondents may include any other useful source of information that they think might be useful for carrying the STF-318 study.

- At the end of the questionnaire there are the so-called continuation tables that respondent may use in case the questionnaire does not provide enough space to answer with the required granularity of detail certain questions: they are white spaces that respondent may fill with free text.

STF-318 team members conducted a number of follow up interviews, clarifying their information sources doubts and so making them easier to fulfil the questionnaire.

The questionnaire was created using PDF forms which enabled the answers to be extracted as XML data and imported into a spreadsheet for analysis. This spreadsheet included totals against the possible answer as well as correlation information to identify similarities and difference between the different questionnaire responses. The results of the questionnaire from both qualitative and quantitative analysis are outlined in the following clauses.

By the time the present report version has been written, information has been gathered and processed by the STF team from 39 sources. Some questions are not filled in by all respondent and so the analysis is given as a ration for those who responded to a particular question.

5 Market

As anticipated in the previous clause, the questionnaire aimed at getting information on both the current and the expected extent of REM systems market mainly within Europe but without discarding either getting information of pan-European or world wide operating entities. Questions were designed so as different types of analysis might be performed based on the answers: per-country based analysis, sectorial analysis, etc.

The present document classifies the responses in categories, based on different criteria. Below follows the classification details:

- A number of responses report REM systems actually existing or being deployed. The present document differentiates the following categories:

  - Services.

  - Products.

  - REM regulations specifying requirements on REM existing systems.

- Other responses do not actually report existing or being deployed services/products/REM regulations but expected features of REM services. These responses were classified as Other, which includes future services to be deployed, and responses from those not concerned with particular REM systems but have interests in REM.

In addition to that, the STF also conducted studies of services and regulations whose information was publicly available and fulfilment of a questionnaire did not take place.

The present document takes in account into consideration 39 completed questionnaires.

This clause first summarizes the results obtained by the team and then gives conclusions on both the current and the prospected market for REM systems mainly within Europe, without forgetting considerations from a wider perspective.

The questionnaire answers and the studies conducted identify the market penetration in terms of services and products deployed as well as more general interest in use of REM services and products. This aims to identify the degree of existing uptake of REM services, as well as interest in the provision of REM services in the future, and hence the need for standardization.

Table 1 presents the distribution of gathered answers, REM services and REM products by countries. The second column of the table indicates the number of answers gathered from each country. The third column indicates the number of respondents that reported the existence of REM products in each country. The fourth column presents the number of REM services reported in each country. The fifth column indicates where a regulatory body governing REM exists. This table does not represent the full extent of the market penetration of REM rather gives an indication of the existing distribution of REM across Europe based on the investigated sample. The study team is aware of other existing REM services for which completed questionnaires were not received.

REM services /products already provided or envisaged are (from questionnaire sections 2.1, 2.4 and 1.2).

Table 1

Country	Overall	Products	Services	Regulatory	Other
Austria	2		2		
Belgium	1		1 Service planned/envisaged		
France	1		1	1	
Hungary	2	2 (1 of them also reports a service)	1 (it also reports a product)		
Italy	5	1 (it reports also a service)	4 (1 of them also reports a product)	1	
Macedonia	1				1
The Netherlands	1			1	
Serbia	1				1
Slovak Republic	1			1	
Slovenia	1		1		
Spain	12	4 (3 of them also report services)	6 (3 of them also report products. 2 of them report envisaged/planned services)	2	4
Sweden	1	1 (it also reports a service)	1 (it also reports a product)		
Switzerland	1	1 (it also reports a service)	1		
Europe	5	1 (it reports also 1 service)	2 (1 of them also report product)		2
USA and Europe	1	1 (it also reports a service)	1 (it also reports a product)		
Worldwide	3	2 (both of them also report on a service)	2 (both of them also report on a product)	1	
Total	39	13	22	7	8
NOTE: As identified above a number of the respondents fitted into more than one category.					

Table 2 contains details of the current status of the service and products that were reported to exist in the processed questionnaires. The team distinguished between those already deployed and in operation from those that are currently being implemented and from those ones that are planned or envisaged. Making these distinctions was crucial for knowing first the actual degree of REM system penetration in the market and support by stakeholders to its further deployment.

Of these systems the approximate status of the systems and products is (from questionnaire sections 2.1, 2.2, 2.4 and 2.5).

Table 2

Status	Number services	Number products
Already deployed and in operation	14	7
Is currently being implemented	3	3
Planned or envisaged	5	3

The next aspects to be taken into account, when dealing with market penetration, are both the current number of users making usage of REM systems and the prospected number of users that these systems already deployed or being developed will have. The table below summarizes the details for currently served communities. First column in table 3 shows different community size ranges. The second column shows the number of services reporting REM services provision to communities whose size falls within the corresponding range at the same row. It must be taken into account that not all the respondent answered this question.

Current size of user community of products / services: (from questionnaire sections 2.3 and 2.6).

Table 3

Size	product	service
≤ 1 000	2	4
> 1 000 and ≤ 10 000	2	2
> 10 000 and ≤ 50 000	1	1
> 50 000 and ≤ 100 000	0	2
> 100 000 and < 500 000 (see note)	1	1
≥ 500 000		1

The rest of respondents do not provide figures of users communities' current sizes for products and services.

One Italian company reports provision of REM services to 1 000 organizations.

Table 4 provides details on the prospected community sizes reported by respondent for both services and products.

Planned size of user community of products / services: (from questionnaire sections 2.3.c and 2.6.b).

Table 4

aSize	product	service
≤ 1 000	1	1
> 1 000 and ≤ 10 000	2	3
> 10 000 and ≤ 50 000	1	2
> 50 000 and ≤ 100 000	1	2
> 100 000 and < 500 000	0	0
≥ 500 000 and < 1 000 000		2
> 1 000 000		2
About 100 000 000		1

The last relevant aspect addressed by the questionnaire focussed on first the business area addressed by the implementations and second the business area where respondent report to operate.

Table 5 summarizes the respondent's profiles (questionnaire section 1.3). It must be taken into account that certain respondent have declared to have more than one profile.

Table 5

Profile	Number of responses
REM service provider	12
Standardization body	5
Regulatory body	7
Provider of services that may be used in REM	
PKI services provider	13
Time-stamping authority	16
Delegate path validation service	6
Long term storage services	11
Notarization services	9
Other profiles (3: 1 of each of the indicated below)	
Management Consultancy specialized in supporting implementation of International management Standards (ISO 17799/27001)	
Certification Service provider for citizens. Advices to regulatory bodies on techniques and rules related to e-government, and to public administrations for the e-transformation of their administrative processes	
Scientific institution	
Addressed REM service user type	
Single user	3
Bank / Financial institution	6
Insurance	3
Public administration	11
Other type of users (9: 1 of each of the indicated below)	
Telecommunication companies and any organization that needs a REM system	
Association	
Industry	
Various services to members of association of lawyers	
Third-party certification and classification, consulting (use of REM clearly relevant)	
National Railway Company	
Postal services provider	
Business organization	
Chamber of Commerce subsidiary and non profit organization	

Table 6 shows information on the profile of the entities that, having answered the questionnaire (and in consequence showing interest or involvement in REM services provision), did not report any service implementation or product.

Table 6

Entity profile	Number of entities
Regulatory body	4
Standardization Body	2
Service/ software provider	4
Public administration as REM user	2
Industry (energy sector)	1
Professional association with public administration acknowledgment, providing services to its members	1
Financial institution that also plays the role of regulatory body (national bank)	1
Consultancy	2
National Railway Company	1
Services provider (PKI, time-stamping authority, delegate path validation)	1
Scientific institution	1

The STF has also contacted a number of entities in other countries from which it did not receive information on REM services or products: United Kingdom, Germany, Poland, Estonia, Montenegro, Ireland and Turkey.

5.1 Specific Conclusions on Market

The following conclusions may be derived from an initial analysis of the responses:

- There is significant interest across Europe with already a number of REM products and services deployed. Whilst there are some areas where REM is yet to penetrate, the majority of European countries contacted indicated that REM services or products existed. In addition to that, the STF has got information from three organizations acting at a world wide level, which report services and products, from 6 organizations that operate within several European countries, and from one that also reports activities outside Europe (Brazil and South Africa).

- Table 2 helps to better understand the current situation: 14 respondents reported on REM services currently in operation throughout several European countries from the 24 mentioned in the questionnaires. Three more services have to be added that were identified through investigation by the study team. Three more services are being deployed and five more are envisaged or planned. Seven respondents reported on REM products also already deployed and in operation, from the 13 reported in the questionnaires. Three respondents reported on products being developed and other three respondents reported on planned products. For both services and products, the number of those ones deployed is higher than the number of those ones being implemented or just planned. This means that the need for this kind of service was already identified in different communities some time ago and several organizations have already made the effort of designing, implementing, deploying and running it. In addition the number (non negligible by any means) of services/products being implemented and planned seems to indicate that there is margin for increasing the penetration of REM systems.

- Tables 3 and 4 provide details of the number of users, both current and prospected. And here also the figures seem to support two main ideas. Firstly, that the size of current REM services user communities is relevant enough for what we could consider a first phase of wide spreading (one organization reports more than 500 000, another one more than 100 000). Secondly that the prospected growth is, in certain cases, of even greater orders of magnitude, as one organization has expectations of serving about 100 000 000 users, and two other organizations expect to provide these services to more than 1 000 000 users.

- As for business areas being addressed by the respondent interested in REM services provision an inspection of tables 5 and 6 lead to the following conclusions:

    - Interest in REM services is wide spread among entities operating within different sectors: from REM related service providers (logically) to users in different industrial sectors, including Public Administration, regulatory and standardization bodies.

    - Current and/or potential REM services users are counted within a number of sectors, including banking, insurance, postal services, railway, bar associations, business organizations, chambers of commerce and Public Administrations.

6 Regulations and legal validity

The questionnaire sent to interested parties was meant to provide information on those regulations of existing or prospective registered e-mail mechanisms that give to the sender and to the recipient trusted information on when a certain e-mail was sent and received. In order to know whether a specific national legislation provides legal validity to the evidence of such shipment that can be exhibited by a trusted third party, section 4 of the questionnaire was drafted.

As a result of the survey, it seems there is a lack of international specific regulations for general REM services. An EU Directive has been issued on community postal services (EU Directive 97/67/CE [6]), however its scope is not considered to include REM.

6.1 Survey overview

Specific regulation requirement relating to REM were identified for the following countries.

Table 7

Country	Specific statute for evidential services (section 4.2.a)	No specific statute for evidential services. (section 4.2.b) Legal validity is based, then, on explicit preliminary acceptance or explicit agreement by the parties, binding therefore only to the parties involved
Italy	Y	
Spain	Y (FNMT, MAP, BdeE)	Y (Bankinter, UPM-ACEPTA)
France		Y
Austria		Y
Netherlands		Y
Norway		Y
Switzerland		Y
Hungary		Y
Sweden		Y
Nordic countries		Y
Pan Europe		Y
Worldwide		Y

The legal recognition given to REM is as follows: (table type vs. country). It is to be remarked that in this table there are some seemingly contradictory replies for the same country, for example that REM services have 'full and general validity' and have 'no "per se" legal validity'. This depends on respondents referring to different solutions. More in detail: in the same country, and at times within the same responder, some implemented services comply with the specific REM legal regulations, while some other services enjoy no such compliance.

Table 8

	France	Italy	Spain	Austria	Netherlands	Norway	Switzerland	Hungary	Sweden
a) has full and general legal validity through specific statute		Y	Y		Y				
b) has legal validity based on explicit preliminary acceptance or explicit agreement by the parties (i.e. the rules set is already defined, users can just accept them)	Y	Y	Y	Y		Y	Y	Y	Y
c) has legal admissibility as a trial evidence, but no 'per se' legal validity	Y	Y	Y	Y	Y		Y		

18 of 39 organizations have answered 4.2.a) that the evidential services have full and general legal validity through specific statute.

11 of 39 organizations have answered 4.2.b) that the evidential services have legal validity based on explicit preliminary acceptance or explicit agreement by the parties (i.e. the rules set is already defined, users can just accept them).

12 of 39 organizations have answered 4.2.c) that the evidences provided by the services have legal admissibility as trial evidence, but no 'per se' legal validity.

6 of 39 organizations have marked 4.2.d) Others:

- SwissPost: expected to be applicable 'de facto' through multi-level, consistent and auditable set of architecture standards implementation (OSCI), technology use, and processes implemented - but no specific statute.
- Bankinter: Applicable.
- DNV: Norwegian law states that agreements can be by any means, and anything can be submitted as evidence. In a legal case, the evidence will be evaluated. A registered email need not obtain a particular status but will constitute a strong proof. An ordinary email is weaker evidence.
- Critical Path products offering provides a sound base to build a platform suitable to assist in providing legal effectiveness in any of the above listed cases (a, b, c), therefore its legal validity depends on the applicable legislation.
- Itelia: In Finland (at least) digital signatures have the same validity as physical signatures.
- Ingevuld Data: In general in the Netherlands one can proof legal validity by all means.

Is the evidence verifiable by (4.3)?:

- 8 of 39: only registered REM users (4.3.a).
- 18 of 39: any party trusting the Certification Authority(ies) used for signing Registered E-Mail (4.3.b).
- 12 of 39: other(s), please specify (4.3.c):
  - An Austrian respondent: some evidence is verifiable by the sender, other evidence is verifiable by the recipient.
  - ChamberSign as a trusted and independent third party.
  - IncaMail: Swiss prosecution bodies in the pursuit of their legal duties.
  - PosteItaliane: Legally recognized authorities are allowed to access the CA related information. By accessing via webmail the PosteitalianeMail@ services, all recipients can verify all the mail related information.
  - Argeon: legal parties, like police, courts etc.
  - Bankinter: General public.
  - DNV: Evidence from DNV's VA services can be verified by anyone. The VA must be trusted, including the VA's signature on the evidence (certificate from DNV's CA dedicated to the VA).
  - Any party trusting one of the attestation policies published by the REM service Provider.
  - AFNOR: An attestation policy contains in particular, but not only, the self-signed certificates that allow verifying the advanced electronic signatures of the attestations.
  - E-Group: when the mail is not signed by the sender itself, the REM would provide for a provable origin.
  - Ingevuld Data: Any party designated by sender.
  - UPU: Legally recognized authorities are allowed to access the CA related information.

6.2 National situation

So far, the team has identified the following situations.

6.2.1 Specific legislation on REM evidential services

Some specific domestic legislation is in place, or is being developed to cover REM or REM services legal validity and implementation. In these cases a number of REM aspects can be addressed by this applicable legislation, among which:

- evidence types and content (submission, delivery / non delivery, exchange between providers, error, etc.);
- involved actors, related responsibilities and relative sanctions in case of misdemeanour;
- possibility to demand for specific fulfilments by entities that want to make use of a REM service in order to be admitted in a relationship with REM system providers.

Where exhaustive legislations exist, full and general legal validity can be envisaged and enforced.

REM services have a specific legal framework where the evidential value is legally established. Upon the service request, any individual/enterprise is subject to the specific REM regulation and generally applicable statute/act.

That is due to the fact that the evidences services, as described in section 3.1 of the questionnaire, are individually regulated by a general binding act / statute / law that provides legal validity against third parties.

6.2.1.1 Posta Elettronica Certificata (PEC) (Italy)

CAD (see note 1) states that electronic transmission of communications that require a submission receipt and a delivery receipt shall be implemented by means of PEC as defined in Decree by the President of Republic 11 February 2005, No 68. The transmission of an electronic document with telematic means, done by means of PEC, is equivalent, where allowed by the law (see note 2), to notification by means of the post.

NOTE 1: Provision on Posta Elettronica Certificata - PEC (REM).

http://www.cnipa.gov.it/site/_files/DECRETO%20DEL%20PRESIDENTE%20DELLA%20REPUBBLICA%2011%20febbraio%202005.pdf

Decree by the Minister for innovation and technologies 2 November 2005 laying down the technical requirements for users and providers of Posta Elettronica Certificata - PEC (REM)

http://www.cnipa.gov.it/site/_files/DECRETO%202%20novembre%202005.pdf

Codice dell'amministrazione digitale - CAD - Digital Administration Code, stating provisions on forming, signing, keeping, exchanging electronic documents; it applies to Public Administrations, Companies and private citizens.

NOTE 2: In some cases, namely criminal trials, different kind of electronic transmission are required.

Time and date of submission and delivery of an electronic document transmitted by means of Posta Elettronica Certificata are opposable to third parties if conformant with dispositions of Decree by the President of Republic 11 February 2005, No 68, and to the related technical rules.

If a PEC user, such as a public administration, a private company or a private organization, is listed as a PEC subscriber in the Directory of Public Administration (IGPEC) managed by the National Centre for Information Technology in the Public Administration (Centro Nazionale per Informatica nella Pubblica Amministrazione - CNIPA), then the user can subscribe to one of these PEC Providers to take full advantage of the legal validity of PEC.

A sender may transmit its electronic messages through its certified e-mail provider (providing PEC). The electronic message (and the relevant attachments, if any) shall be considered to have been legally sent, if it is submitted to the sender's certified email provider. The certified e-mail shall be considered to have been legally received by the recipient, if it has been conveyed to the recipient's PEC mailbox from the relevant certified e-mail provider. The sender will receive both an acceptance receipt from its PEC Provider and a delivery receipt from the recipient's PEC Provider: these receipts will be signed by the relevant PEC Provider with an advanced electronic signature.

It should be noticed that the system does not guarantees the identity source (i.e. e-mail address) of the sender of the certified e-mail message, having the sender's authentication been left up to the single PEC implementation, nor guarantees that the recipient has retrieved the message from its mailbox. The acceptance receipt is the equivalent of the paper receipt that is given by the post office for registered physical post. The 'delivery receipt' provides more legal value than the equivalent 'advice of delivery' that currently exists for registered letters, since it has full legal value even in cases where the paper registered mail does not have it.

PEC services are subject to free competition. Public administrations and private companies who intend to act as PEC providers apply at CNIPA to be enlisted in the PEC providers list. The following enlisted providers have fulfilled the questionnaire: InfoCamere, Poste Italiane S.p.A. and I.T. Telecom s.r.l.

Centro Nazionale per l'Informatica nella Pubblica Amministrazione - CNIPA, that also fulfilled the questionnaire, operates a CA, within the Cybertrust hierarchical tree, by which 'accredited' PEC providers are given the signature certificates they need to issue AdES on receipts, advices, messages 'transport envelopes'.

6.2.1.2 Belgium

In Belgium, a Project of Law, concerning the trusted services legal framework, will provide legal recognition to the REM services. A time-stamped proof of submission for the sender and proof of delivery shall be provided by the REM service provider. The law project establishes that the REM service provider shall implement 'reasonable means' in order to ensure data security and to avoid unauthorized access. At the time of that this information of this report was collected, which was close to the deadline for approval (June 30, 2007) this law had not been approved.

6.2.1.3 France

A specific implementation of the EU Parliament Directive 2000/31/CE on E-commerce has been approved in France (Ordonnance no 2005-674 du 16 juin 2005 relative à l''accomplissement de certaines formalités contractuelles par voie électronique. JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE. 17 juin 2005).This legislation is limited to notifications concerning problems fulfilling/complying with contractual obligations. The evidential details are to be established by Conseil d'Etat decree, which is pending so far.

A contractual conclusion or performance notifications can be sent by electronic means provided that this mail is:

(i) dispatched by a third party;

(ii) according to a process which allows it to:

- identify that third party;
- to designate the sender;
- to ensure the identity of the addressee; and
- to establish whether the letter has been delivered or not to the addressee.

The appending of the date of sending shall result from an electronic process whose reliability has some legal presumption (''iuris tantum''), where it meets the requirements fixed by decree in Conseil d'Etat, unless there is evidence to the contrary.

At the option of the sender, the contents of that letter may be printed by the third party on paper in order to be delivered to the addressee or may be addressed to the latter by electronic means. In the latter case, where the addressee is not a professional, he must have requested the sending by that way or have accepted the use of it during previous exchanges.

Where the appending of the date of sending or of receipt results from an electronic process, the reliability of the latter is presumed, until evidence contrary to it, where it meets the requirements fixed by decree in Conseil d'Etat.

An advice of delivery may be addressed to the sender by electronic means or by any other device which allows him to store it.

6.2.2 REM services provided by public administrations with public notarization functions

These are REM services provided by public administrations, public law entities or entities recognized as having some kind of public function (i.e. Public Postal Services, Chambers of Commerce or professional associations) to specific professional groups or to individuals/citizens. In these cases, the public notarization functions reinforce the evidences legal value.

In Spain, both the Secure Telematic Notification Services (see note 1) and Lexnet (see note 2) have also specific regulation on evidences concerning shipment, time and date of notification, and proof of delivery.

NOTE 1: http://notificaciones.administracion.es/ . Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
http://www.cert.fnmt.es/legsoporte/RealDecreto209.PDF

NOTE 2: Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet.
Para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.
http://noticias.juridicas.com/external/disp.php?name=rd84-2007

6.2.2.1 Secure Telematic Notifications Service (Spain)

This is a services provided by Correos and MAP, where an individual designates a mailbox ('Dirección Electrónica Única') to receive notifications from public administrations. This service is technically supported by FNMT and implemented in different public authorities as Bank of Spain, Agencia Tributaria and Ministerio de Industria.

A Court notification system called 'Lexnet' for court professionals is being also implemented.

Both services provide legal proof of submission, delivery/non delivery, and of the message content. If the recipient refuses the notification this is forwarded by physical post.

6.2.2.2 ChamberSign Sverige AB (Sweden)

ChamberSign Sweden is a Stockholm Chamber of Commerce subsidiary and a non profit organization. It applies to the Swedish public procurement act where Stockholm Chamber of Commerce can be used to oversee opening of tenders. The main service is the third party notary which in combination with the technology used provides a legally binding traceability in different forms of internet communication (applications, e-mail, etc.).

REM is not marketed as a standalone service but offered as a part of all other services provided. Main services consist of e-tender and contract signing functionality through a web based application provided by ChamberSign. REM is provided as an add on to all services provided.

ChamberSign works as a hub for parties' agreements so they can communicate with each other without having to sign a preliminary agreement with each counterpart. ChamberSign, as a trusted third party, also has an original receipt store which is used as evidence.

6.2.2.3 Hybrid REM systems (send electronically - receive on paper)

In France and Belgium there exist REM services uses the classic postal acknowledge of receipt system, thus solving the legal problem of acknowledgement avoiding the use of any electronic technology in the notification.

6.2.3 General electronic signature and contractual legislation

In these services, evidences are governed by non specific REM regulation (i.e. electronic contract law, electronic signature regulations -national implementation of the Electronic Signatures Directive 1999/93/EC-, procedural law concerning e-documents' evidential value in trial, etc.).

These services/products are normally based both on the service technical documentation and on a previous contract endorsement or general terms and conditions acceptance. The legal validity is based, then, on explicit preliminary acceptance or explicit agreement by the parties, binding therefore only to the parties involved.

These services/products can be characterized by the absence of a general REM evidences services regulation and, more particularly, by the lack of a specific electronic notifications legislation.

Their legal validity is substantially the same as that of an email signed with an electronic signature, when QES is used, and is subject to legal evidential uncertainties (i.e. notification legal validity is never guaranteed). This means that the burden of proof is relatively weak unless the sender is able to provide evidence of a verifiable nature that the e-mail was sent at a particular time, to the person(s) intended and with the text allegedly sent.

Examples are:

- **Switzerland.** ZertES - Swiss Federal Law on Electronic Signatures. The services are based on an explicit preliminary acceptance based on the 'Obligationenrecht (OR)' Swiss Federal Law on Contractual Relationships.

- **Spain.** Bankinter, Cryptology Laboratory (Polytechnic University of Madrid) Acepta Project, CATCert, Camerfirma.

- **The Netherlands.** GBO.Overheid. It is a government organization of which PKIoverheid, the Dutch top level government PKI is a part. The central organization of PKIoverheid mainly consists of the Policy Authority, managing the Programme of Requirements ('Programma van Eisen'). GBO.Overheid does not, actually, implement a REM system of the kind addressed in the present document and what their system envisages is applying QES and TST to outgoing items. Therefore their services are based on the Dutch Electronic Signature Law.

- **Austria.** Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) is the office of the Telekom-Control Commission, which also acts as supervisory authority for electronic signatures. RTR provides e-government services and electronically delivers official documents to operators of public telecommunications networks and services.

- **Norway**. Det Norske Veritas (DNV) and eNotarius AS. The e-signature legislation gives high status to signatures generated from qualified certificates and sets criteria for publishers and how the signature was applied.

- **Hungary.** Argeon Kft. (Argeon Ltd.) and E-Group. In the case of E-Group, the Hungarian Government's Client Gateway provides for a mailbox for its users, that applies only to e-government services and is extensively used in G2B, G2C communications. This should be upgraded to a REM service. Interoperability between e-invoicing service providers could be improved by using REM.

- **Nordic countries** : eNotaris.

During the survey, some relevant product/services implementers and academic bodies have been identified that fulfilled the STF questionnaire, i.e. Critical Path products, PostX Corp**,** AFNOR AC and Mathematical Institute SANU (Serbian scientific institution expert on cryptography and an information protection) which may provide technical and procedural details in order to achieved services/products with evidential legal value under their respective national legal frameworks.

6.3 Specific conclusions on regulation and legal validity

As a conclusion, out of the three groups described in clause 6.2, the one under clause 6.2.1 is the more specific from a legal point of view, together with the one under clause 6.2.2 (due to the public notarization functions). The group under clause 6.2.3 is less specific. It should be noted that the ultimate decision on the strength of any evidence is for the court within the context national and international legislation.

Any REM model should take into consideration the following elements:

- The evidential services should be provided by a third party independent from the other actors or with public notarization functions. Evidences should be produce by a 'witness', which, by definition has to be independent of the parties involved. When a time reference is needed, time-stamping services should be provided by a trusted and independent third party.
- A process should be established that allows identifying the independent/trusted third party, to identify (designate) the sender, to ensure the identity of the addressee and to produce a proof of delivery legally valid.
- Internal Control Policies should be implemented by all the entities involved when producing evidences to ensure confidentiality, evidential integrity and authenticity in order to provide robust court proofs.

7 Services

7.1 Evidence

An essential aspect of registered e-mail is the provision of evidence of actions relating to the handling of messages. This evidence may require of actions at any stage of the flow of a message, origination by the sender, transfer of the messages within the REM service and final delivery and being read by the recipient.

The following table identifies the points within the message flow, where evidence may be required, and associates the evidence services.

The column 'overall% required' reflects the fraction of answers that support this service or at least consider this service a requirement and consists of 'products', 'services' and other answers falling into neither category. The column 'products' deals with the subset of the questionnaires related to actual products (ticked question 2.4) while the column 'services' only those questionnaires have been taken into account, that related to a specific service implementation (ticked box 2.1).

Table 9a

Evidence service	Overall% Required	Products	Services
Evidence of message origin authentication Provides evidence of the identity of the message originator to the recipient and also protects the integrity of the message	92 %	100 %	95 %
Evidence of submission Provide evidence to the sender that he did submit the message to the REM service and includes the time this submission happened	92 %	100 %	95 %
Evidence that message has been transmitted through a REM service provider Provides evidence to the receiver of a message that he has received the message using the REM services and includes the time this transmission was carried out	51 %	77 %	57 %
Evidence that message has been successfully exchanged between two REM service providers Provides mutual evidence between two REM service providers that they have exchanged a message, including the time this has happened	36 %	46 %	38 %
Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded Provides evidence to the sender that the REM provider has notified the recipient of an incoming message and includes the time of this notification	56 %	69 %	52 %
Evidence of delivery/download Provides evidence to the sender of a message that the message has been delivered to the recipient and the time this has happened	87 %	92 %	90 %
Evidence of acceptance or rejection of message by the recipient Provides evidence to the sender of a message that the recipient has accepted or rejected the message and the time this has happened	64 %	69 %	52 %
Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.) Provides evidence to the sender of the message that the REM-provider was unable to deliver the message to the recipient due to technical errors and other problems and includes the time this failure has been detected	87 %	77 %	81 %
Evidence of non delivery/download within a predefined time limit Provides evidence to the sender of the message that the REM-provider was unable to deliver the message to the recipient within a given time period and includes the time this failure has been detected	72 %	62 %	71 %
If applicable please specify if this time limit is:			
I. Pre-defined	68 %	63 %	87 %
II. Defined by the sender	46 %	63 %	33 %
Evidence that an email has been 'opened' or 'viewed' by recipient Provides evidence to the sender of a message that the message has been opened or viewed by the recipient and includes the time this has happened	54 %	69 %	52 %

7.2 Other security related services

This clause covered services not directly related to evidence, but related to the security and limitations of the process.

- The majority of implementations do not support malware detection capabilities; this correlates well with the overall 56 % of the answers considering this important. One provider also mentioned providing Anti-Spam and Anti-Phishing measures.

- 75 % of the answers consider confidentiality protection as being important and only one of the products covered by questionnaires do not implement it. One implementation only provides confidentiality when messages are transported between postal services.

- Only 62 % consider revealing the content to the recipient only if the email has been accepted to be important, which corresponds well to the 62 % of the services supporting this (but 77 % of the products do).

- Most implementations have no limit concerning the size of messages and attachments on their own. Only six questionnaires gave a limit, which, being between 1 MB and 30 MB respectively, will not be a relevant limitation only for the lower numbers (two answers). One implementation only deals with PDFs; other implementations do not have any restrictions, besides blocking active content or self-modifying formats; one other sets a minimum limit a server must handle of 50 MB obtained by multiplying the overall size of the single message by the number of recipients.

7.3 Other Services

Table 9b

<table>
<tr><th>Service</th><th>Overall% Required</th><th>Products</th><th>Services</th></tr>
<tr><td>Sender Message Archival - i.e. Long term storage of all messages after being submitted by the sender and notifications, regardless of whether it has been delivered to / retrieved by the recipient.
The messages are typically stored from five to ten years. Some providers store them only a few months (and consider this long-term). Others have configurable durations or store the message as long as the user subscribes to the service.</td><td>69 %</td><td>77 %</td><td>62 %</td></tr>
<tr><td>Recipient Message Archival - i.e. Long term storage of all messages and notifications made available for download / retrieval even after being retrieved by the recipient or removed from an online message store
Mostly the retention period matches those of the sender. Some services however currently provide a much shorter service to the recipient, maybe because the recipient does not have a contractual relationship to the service provider.</td><td>62 %</td><td>69 %</td><td>52 %</td></tr>
<tr><td>Storage of messages containing malicious code in quarantine area for future reference.
In most cases this is a much shorter period. One provider stores them for up to 30 months, but does not provide an archival service for senders or receivers.</td><td>36 %</td><td>38 %</td><td>38 %</td></tr>
<tr><td>Storage of logs containing information about messages
The period here typically matches the retention period for senders and receivers above. The following tables show the information fields archived and the number of questionnaires.
<table>
<tr><th>Information</th><th>Stored</th></tr>
<tr><td>Message identifiers</td><td>5</td></tr>
<tr><td>Time and date of log entry</td><td>6</td></tr>
<tr><td>Message subject</td><td>6</td></tr>
<tr><td>Sender and Recipient</td><td>8</td></tr>
<tr><td>Event type</td><td>3</td></tr>
<tr><td>Operational results and error messages</td><td>3</td></tr>
<tr><td>Senders provider identifier</td><td>3</td></tr>
<tr><td>Receipts of delivery</td><td>2</td></tr>
<tr><td>Attachment list</td><td>1</td></tr>
<tr><td>Time stamps and time marks</td><td>5</td></tr>
<tr><td>Message hash and signatures</td><td>1</td></tr>
<tr><td>Complete Logfiles</td><td>2</td></tr>
</table>
Sender, Recipient, Subject and time information are the most prominent fields here. Only one provider saves message hash and signatures. Overall many questionnaires did not contain any information on this.</td><td>85 %</td><td>85 %</td><td>90 %</td></tr>
<tr><td>Maintenance of signatures on archived data to ensure sufficient data is available to verify signature over long term.</td><td>69 %</td><td>62 %</td><td>52 %</td></tr>
<tr><td>Directory services to assist senders in obtaining recipients email addresses.</td><td>51 %</td><td>46 %</td><td>48 %</td></tr>
<tr><td>Directory services to assist senders / recipients in obtaining certificates required to secure messages.</td><td>62 %</td><td>62 %</td><td>52 %</td></tr>
</table>

Service	Overall% Required	Products	Services
Other Directory services for: • checking revocation status; • listing of accepted certificates & their provider needed for service registration and use on services home website; • assisting REM Providers in identifying REM registered domains; • presenting information about sender and recipients roles and right in the organization represented; • LDAP, Active Directory, PGP keys, internal databases, external databases, others; • assist sender in getting physical address.	28 %	38 %	33 %
Supports individuals.	87 %	85 %	81 %
Supports organizations.	95 %	92 %	90 %
Supports both.	89 %	83 %	84 %
Supports other entities (devices, applications etc.).	31 %	46 %	33 %
Supports E-purchasing.	69 %	77 %	62 %
Supports E-tendering.	69 %	77 %	67 %
Supports E-accounting.	72 %	69 %	62 %
Supports official communication between and with public administrations.	92 %	100 %	90 %
Supports general purpose transmission of messages and/or files.	54 %	77 %	57 %
Other(s), please specify (e-Invoicing, other special purposes, contract signing, Burofax).	15 %	31 %	14 %

7.4 External

This section of the questionnaire covered external connections from REM provides either to physical post or to electronic non-REM services.

Table 10

Service	Overall% Required	Products	Services
Always forward to physical post in case of failure of registered email	10 %	0 %	10 %
Forward to physical post in case of failure of registered e-mail if requested by the sender	23 %	8 %	24 %
Forward to physical post instead of electronic post where addressed as such by the sender	21 %	8 %	24 %
Forward e-mail to other non Registered E-Mail network where addressed as such by the sender	36 %	38 %	38 %
Forward e-mail received from external e-mail network (e.g. Internet) to Registered E-Mail recipient	26 %	31 %	29 %
Other(s), please specify: • Forward notification of the availability of a stored message to physical post in case of non-delivery. • Forward to physical post if requested by the recipient. • A PEC provider can choose as a general rule not to forward to its users messages sent from non PEC addresses. • Alternative address to notify there is mail in REM. • email from non-REM are forwarded to the recipient inside an anomaly envelope. • PosteitalianeMail@ delivers e-mails to recipients belonging to any domain. The integrity/authenticity is verified via a webmail based service.	21 %	31 %	29 %

7.5 Specific conclusions services

The following services are almost unanimously seen as the most important basic services to be provided by a REM-service, and almost all services either implemented them or consider them necessary:

- evidence of message origin authentication;
- evidence of message submission;
- evidence of delivery and non-delivery.

For the other services, this is different:

- Only about 50 % of the answers provide evidence of exchanging messages between two REM providers. This may be due to the fact that these services are related to a centralized system only that do not provide for senders and/or recipients belonging to external providers, where such exchanges are not necessary and possible or, as it is the case for UPU, the cross border exchange has not yet been defined.

NOTE 1: This depends on the fact that, as per the UPU rules, only national Postal Services can operate a EPCM service in one country, thus, so long as the cross border exchange is not ruled, this might be a serious hindrance to international REM exchange.

- Also, overall only half of the answers provide an evidence of notification of availability, but 2/3 of existing products implement this.
- Evidence that the message has been opened or viewed is overall seen important by 50 % too - but significantly more questionnaires related to products have that implemented or consider it important (75 %) though.
- For the other evidence services, such as malicious code presence and errors, no clear trend is to be recognized (overall more than 50 % of those answering consider them important). Products tend to support more services or consider them more important than the overall average shows.

The results show that none of the evidence services identified is seen to be completely useless or unnecessary. Any standard supporting evidence services must consider all of them and may decide to group them into mandatory, recommended and optionally supported services.

Currently there is only limited support for external connections to physical post or other non-REM-services. The only service that is supported to a certain extent is interfacing with non-registered e-mail networks. Any standard should consider implications on the possibility of such interconnections.

To summarize the answers received regarding **other services**:

- The majority of the respondents consider message archival important and about 2/3rds of the products provide such services. Since the intent of REM is to support evidence the sender has indeed sent something to a recipient, it is not surprising that there is more support for archival at the sender side, but only slightly so.

NOTE 2: Where archival is used to support the integrity of data alone this might be achieved through use of message digest thereby reducing risks to the privacy of the message.

- Most respondents consider archiving log files to be important, but they diverge on what logs and log contents are to be archived (if this has been answered at all).
- Long term signature maintenance is seen by more than half of the respondents as being important, but this is not yet reflected in the number of services or products supporting it.
- Directory services for certificates is seen as being more important as directory services for email addresses, but neither of them is considered to be very important. Apparently this is considered to be a service to be provided by a CA.
- There is generally a very high level of support for both, support for individuals and organizations, with a slight margin for organizations. Approximately three quarters of products and services support both user groups. Support for other entities is seen less important.

- Official communication between and with public administrations is clearly the dominating application (all products support this), while support for other e-Applications is still generally very high. General purpose communication is of less importance, only 50 % of the respondents consider this a requirement - but 73 % of the products support it.

For this STF, the conclusions are:

- There is little input for formats and protocols, since many of these services are internal issues of a service provider. Recommending use of XAdES and CAdES to support long term signature maintenance will make it easier to provide such services. Also discussing ways to handle archiving log files while ensuring their integrity and verifiability in case of disputes should be a topic of interest.
- For policies, a discussion on messaging and log file archival policies make sense.
- Since neither support for individual users and organizations can be neglected, as can any of the application scenarios, all discussions need to take applicability for all user types and all application into account.

8 REM system overviews

8.1 Introduction

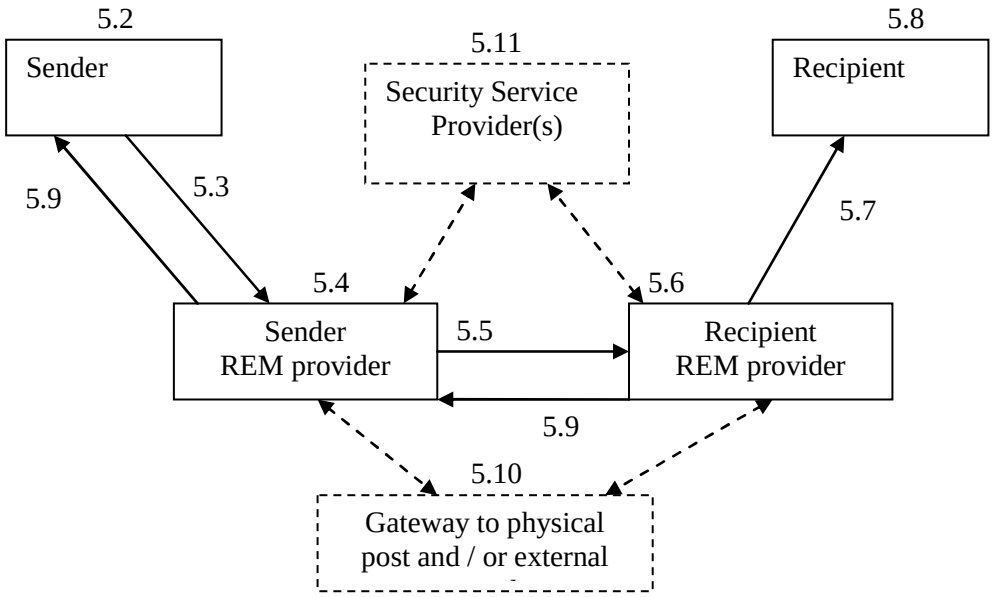
In order to get some consistency between the technical responses to the questionnaire an initial architecture was developed with the aim of relating the respondent's systems to this architecture in order to identify their key features.

In reviewing the responses, however, it became clear that there are significant differences in the basic approaches and architectures adopted by the REM systems covered by this survey. So, following a description in clause 8.2 of the initial architecture used in the survey, clause 8.3.1 provides a revised architecture which takes into account the approaches described by the respondents. It is suggested that this is used as the basis for future standardization in this area, as it aims to provide a framework whereby interoperability with existing systems may be maximized.

Clauses from 8.3.2 on provide an overview of the main approaches taken by the respondents.

8.2 Initial architecture

The questionnaire was based upon the following model.



NOTE 1: External e-mail means e-mail services which do not provide Registered E-Mail services directly to the sender or the recipient. Additionally, conventional physical postal services (registered or otherwise) may be interfaced.
NOTE 2: Some security services, like encryption, validation, time-stamping, can be outsourced.
NOTE 3: Sender and recipient may require associated software and hardware on sender's / recipient's system.
NOTE 4: Continuous (i.e. not dashed) lines identify elements of what is henceforth referred to as 'basic model'.
NOTE 5: The numbers appearing in figure 1 identify subsections of the questionnaire. Each subsection contains questions on specific elements of the model. Subsection 5.1 contains questions regarding the model as a whole.

Figure 1: Initial architecture

8.3 Generic Model and Specific Adaptations

The following clauses provide:

- In clause 8.3.1 a general description of the entities involved in a REM transaction and a graphic overview of their architecture taking into account the initial one indicated in the questionnaire (see clause 8.2) and the approaches described by the respondents.

NOTE 1: This is the preliminary development of a model to be further enhanced in the next phase of standardization for Registered E-Mail.

NOTE 2: Annex A includes an outline of the main approaches taken in existing regulations and service / product implementations from which this new model is derived.

- In clause 8.3.2 onward graphic overviews of some REM models, selected for their prominence due to legal standing, endorsement by national or international standard bodies, widespread adoption.

8.3.1 REM relevant entities

The following basic components of a general REM service have been identified.

- **Message:** it can be:
  - A simple message.
  - A message with attachments.
  - A reference message carrying an address where the original message and/or its attachments can be downloaded from. Usually this reference is a URL pointing to a location at a REM transport provider's (generally the sender's).
- **Sender:** it is the entity originating the message; in most implementations the sender must authenticate to the relevant REM provider, but the choice of the authentication mechanism is left to the specific REM provider.
- **REM transport provider:** it is the organization that, through one or more servers:
  - Authenticates the sender or the recipient, were applicable.
  - Accepts the message being sent or forwarded, with or without attachments, on which it can apply limitations regarding size, format, virus absence, etc.
  - When operating within a specific legal or operational environment, can perform validity verifications relevant to that environment.
  - Exchanges REM messages with other REM providers or directly with the recipient.

There may be one or more REM transport providers, depending on two basic cases:

- the REM mechanism is implemented in a closed domain where only one single trusted REM transport provider is envisaged in order to provide full legal validity to the REM exchange; in this case sender and recipients are likely to belong to the same REM transport provider domain and, where they do not, this may affect the entirety of the message transmission full legal validity;
- the REM mechanism is open to more transport providers providing legal validity; the recipient and the sender may however belong to the same provider.

In some implementations the REM Transport provider may be designed as the deposit of binary objects, be they the e-mail itself or other objects, upon which deposit a specific evidence may be issued. The recipient will be notified of this object availability and, based on the information provided with this evidence and on other credentials, can withdraw this object.

- **Evidence:** is the electronic document (receipt, warning, exception, etc.) generally signed by the issuing provider, stating that a certain event had occurred at a certain moment; generally speaking one evidence proves that a certain message, alternatively or in combination:
  - existed at a certain moment;
  - was sent from one specific sender;
  - was accepted by a specific transport provider;
  - was sent from one specific transport provider;
  - was delivered to a certain recipient's mailbox;
  - was downloaded by a certain recipient;
  - was opened / read by a certain recipient;
  - was rejected by a certain transport provider or recipient for a certain reason (virus presence, format error, etc.);
  - etc.

- **Evidence provider:** it is the organization that provides requesters with evidences. In one single REM system there may be one or more evidence providers depending on the applicable regulation, be this a legislation or a recognized standard.

Generally speaking there are two different basic cases:

- the Evidence provider is separate and independent from any REM transport provider;
- a REM transport provider acts also as Evidence provider; in this case there are two possible sub-cases:
  - the provider acting both as evidence and REM transport provider may be the sole Evidence provider for a REM domain, serving all the users belonging to that domain;
  - each evidence and REM transport provider issues its users evidences related to its own operations.

Usually an Evidence provider bears the responsibility for storing the evidences for the time required by the applicable regulation, even when it outsources the storage service to another entity.

- **Evidence verifier:** in some implementation this entity, upon request by one of the other entity types and after having verified an evidence, may vouch for this evidence authenticity. There may be the following cases:
  - an Evidence verifier is separate from the Evidence provider;
  - an Evidence provider acts also as Evidence verifier;
  - Evidence providers/verifiers are separate from REM transport providers;
  - REM transport providers act also as Evidence providers/verifiers.

The evidence verification can be performed in two basic ways:

- The evidence is sent to the Evidence verifier that sends back a signed assertion.
- The requesting entity connects with the Evidence verifier along an internet connection. If the reply is signed it may have an absolute validity, otherwise its validity is limited to the duration of the internet connection.

NOTE: An evidence may have or have not absolute validity depending on the applicable regulation and on its intrinsic structure. For example it may have absolute validity if it is signed in abidance by the applicable regulation. In this case the Evidence verifier's task could be to just verify the evidence signature and to return a signed assertion on the validity of the signature against the evidence.

Where the evidence has no such intrinsic validity the Evidence verifier's task would be to verify the evidence trustworthiness as a whole, based on mechanisms that can depend on the applicable regulation, for example based on an evidence trusted storage.

- **Recipient:** it is the entity to which the message is addressed; in most implementations it must authenticate to the relevant REM transport provider, but the choice of the authentication mechanism is left to the specific REM provider. The Recipients can, depending on the implementation, retrieve directly the intended e-mails from their related mailbox or download them from the deposit where they are kept by the REM Transport Provider (see item 3).
- **Intermediary:** in some implementations this kind of service is envisaged. It interfaces on the one hand an evidence requester, that may have no right, or will, to ask a specific Evidence provider for an evidence, and on the other hand the specific Evidence provider. The Intermediary requests the Evidence provider for a specific evidence on behalf of the requester. The evidence might be directly delivered to the requester by the Evidence provider, or the requester, or any authorized party, might withdraw it from the Evidence provider.

- Optional mail service providers can be interfaced, namely:
  - **Traditional e-mail providers:** these entities can interface REM transport providers in both directions, in that REM messages can be handed over to traditional e-mail providers to be delivered to non REM recipients, as well as traditional e-mail can be accepted by REM transport providers to be delivered to REM recipients as non fully Registered e-mail. Depending on the REM implementation, users of these e-mails cases may only partly enjoy the benefits of REM Evidences, for example:
    - when a REM is sent to non REM recipients, the sender may be able to exhibit just the Evidence of the related submission to his/her Provider;
    - when a non REM is forwarded to a REM recipient, the latter may be able to exhibit just the Evidence that that very e-mail was delivered at a certain time and date.
  - **Physical mail transport providers:** these entities can be delivered REM to be printed and conveyed as paper mail.
- **Additional service providers** can be interfaced, in particular security services providers, among which: Signature creation providers, Signature verification providers, Long term storage providers, Time Stamping service providers, etc. These components are modelled as integral parts of the elements identified above.

In figure 2 the basic REM components are sketched that can be combined in various implementation models described further on.

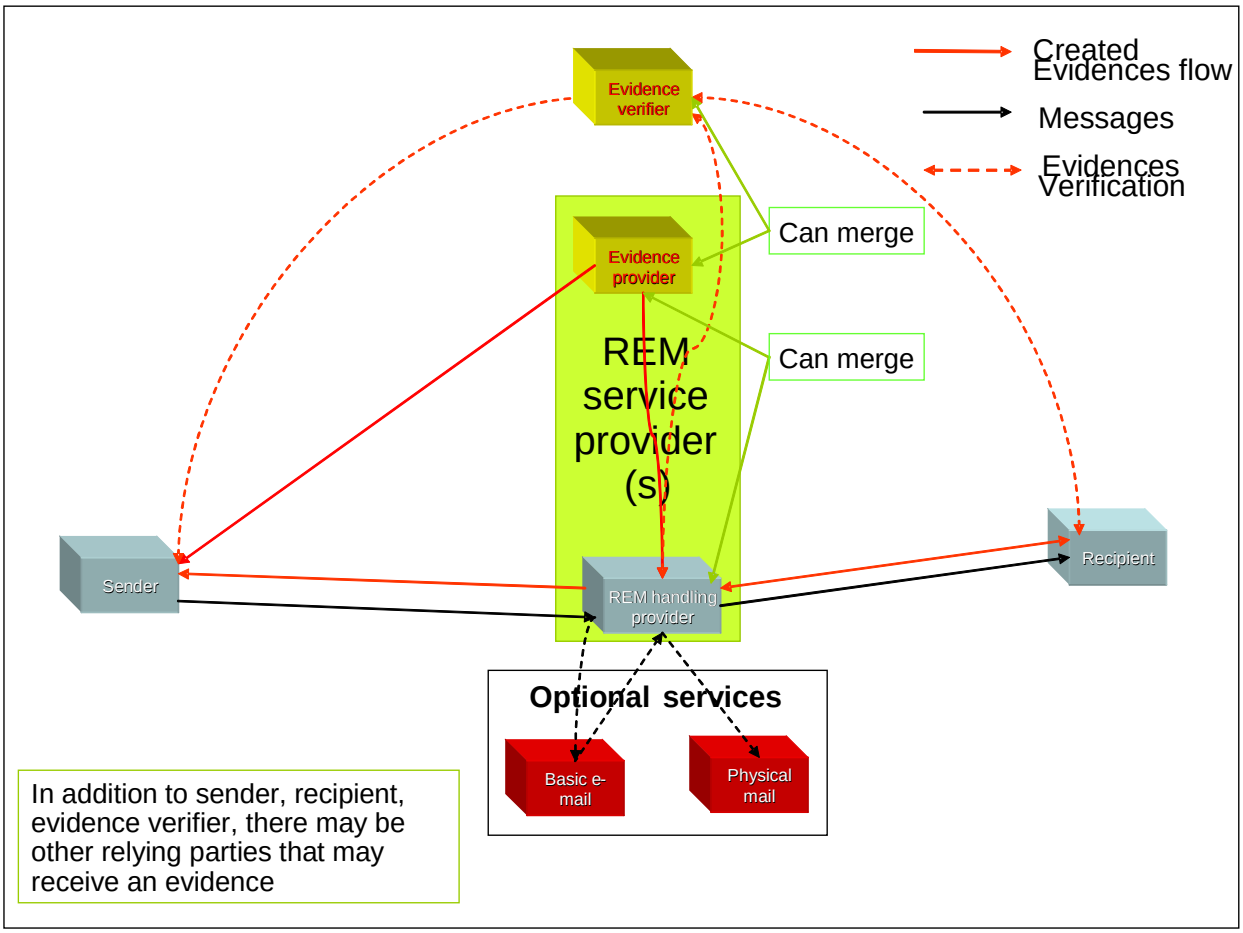


Figure 2: REM Basic Model Components

8.3.2 AFNOR REM service

Based on the AFNOR model description provided in clause A.1.1, figure 3 graphically represents the relationships among the various actors envisaged in the AFNOR standard.

In this model the entities in the REM system take care only of messages and evidences deposit and transmission and, where necessary, of the evidences request or verification, while Evidences are produced by a specific entity. Where not specifically acknowledged by a legislation these Evidences have no legal value per se, although they can be freely evaluated by judges on whether they can be used as legally valid Evidence in court.

The main peculiarities of the AFNOR model versus the figure 2 basic model are:

- Evidence provider is an independent authority that may act also as Evidence verification authority.
- Interfaces towards basic e-mail and physical mail are not envisaged.

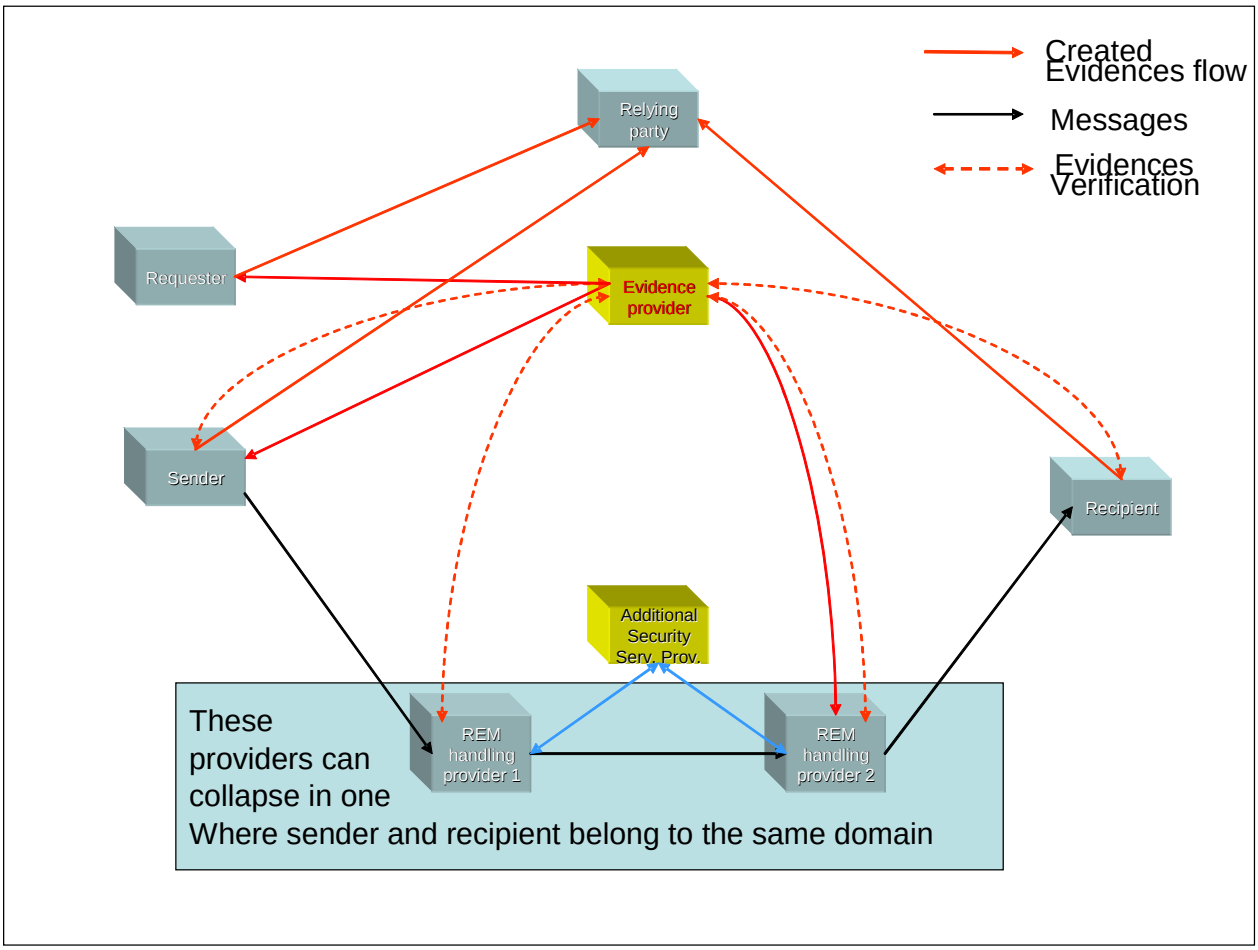


Figure 3: Model Adaptation for AFNOR

8.3.3 Italian REM service (a.k.a. "CNIPA" model)

REM service providers, in order to act as such, must be accredited by CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), the Governmental organisation in charge also of supervising REM providers. It manages one CA that issues REM providers the certificates required to support their signatures on Evidences, among which those of mail acceptance and delivery are delivered to users.

Figure 4 graphically represents the relationships among the various actors envisaged in the Italian REM service (a.k.a. 'CNIPA' model), bolstered by a specific set of rules of law that provide these Evidences legal validity per se.

In this model, production of all communications and evidences occurs only within four directly involved entities: sender, recipient and their REM servers.

The main peculiarities of the CNIPA model versus the figure 2 basic model are:

- REM services providers are also Evidence providers.
- Evidences can be verified by anyone trusting the CNIPA CA without the need of specific entities. This is automatically done by most e-mail clients since the CNIPA CA is part of the GTE Cybertrust RootCA, the self-signed certificate of which is present in most Operating Systems.
- No interface with physical mail is envisaged, only e-mail exchange with ordinary e-mail providers.

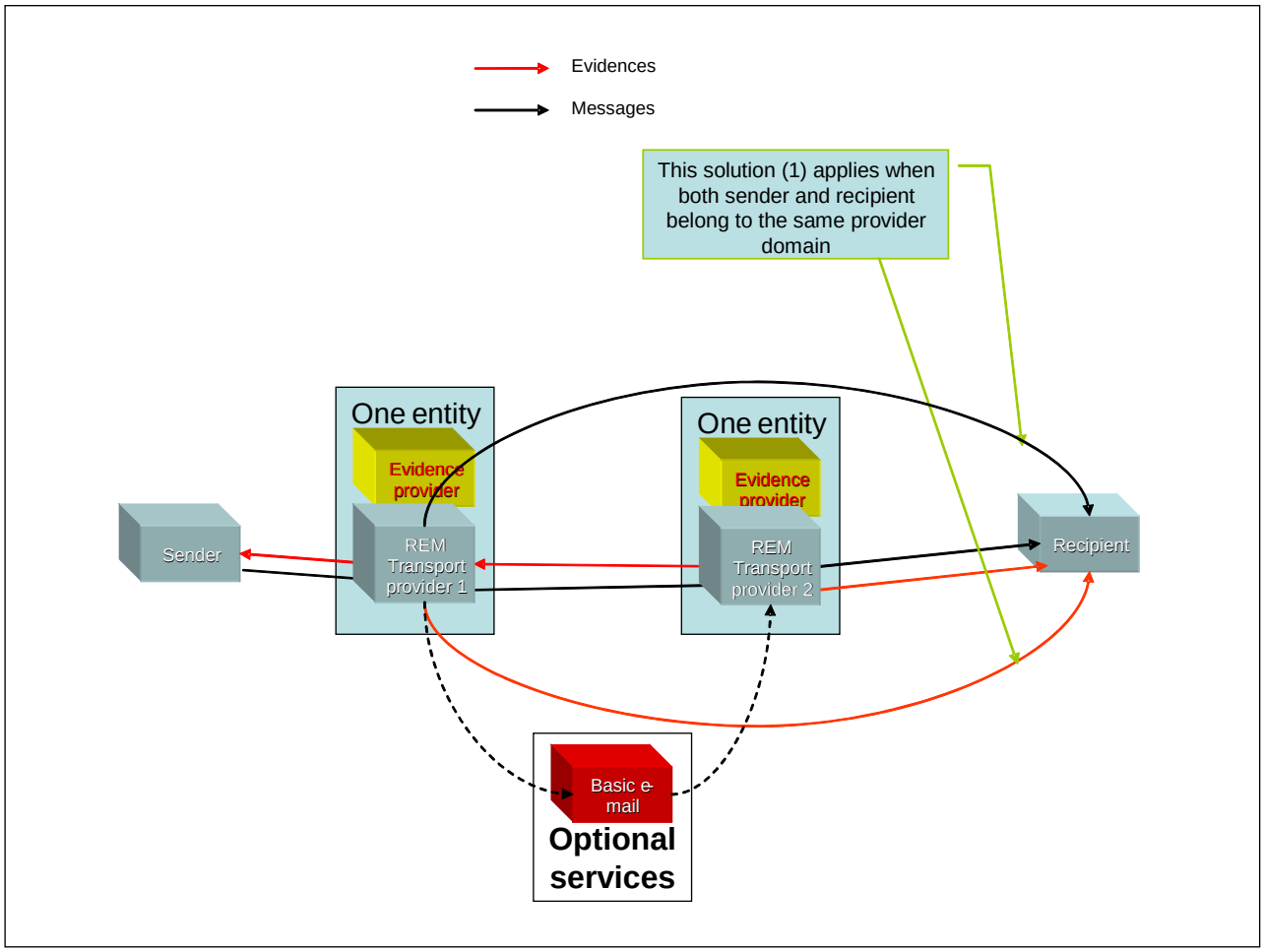


Figure 4: Model Adaptation for CNIPA

8.3.4 UPU ECPM model

The UPU - EPCM (formerly Electronic Post Mark or Digital Post Mark) set of services provides basically a non-repudiation service the main features of which are:

- issuance of Evidences based on digital signature and time stamping;
- evidence validation covering also certificate trust chains;
- storage of evidences in order to support subsequent validation requests.Evidence issuance, storage and verification are governed by the Postal Administrations.

Although the EPCM, strictly speaking, is not 'per se' a Registered E-Mail service, since it neither provides nor addresses e-mail transport, it is a service that can validly supplement the sheer e-mail transport, endowing the latter with an Evidence provision and validation service that can transform it into a REM.

Clause 8.3.5 graphically represents the relationships among the various actors envisaged in the model based on the Universal Postal Union standard S43-3, for Secured Electronic Postal Services and EPCM.

The current status of the EPCM standard is focused on ensuring national operations. Cross-postal Administration Interoperability is not yet addressed, however in clause 8.3.5 it is anticipated what could be such a cross Administration REM exchange between UPU relevant domains.

Per each country there may be more evidence (i.e. EPCM) providers, namely Postal Administrations that can license a number of transport providers. One of these transport providers can coincide with the EPCM provider. Users have the information suitable to ascertain EPCM authenticity and integrity.

The main differences versus the figure 2 basic model, in addition to the already hinted to non interoperability issue, are the lack of gateway with usual e-mail and physical mail.

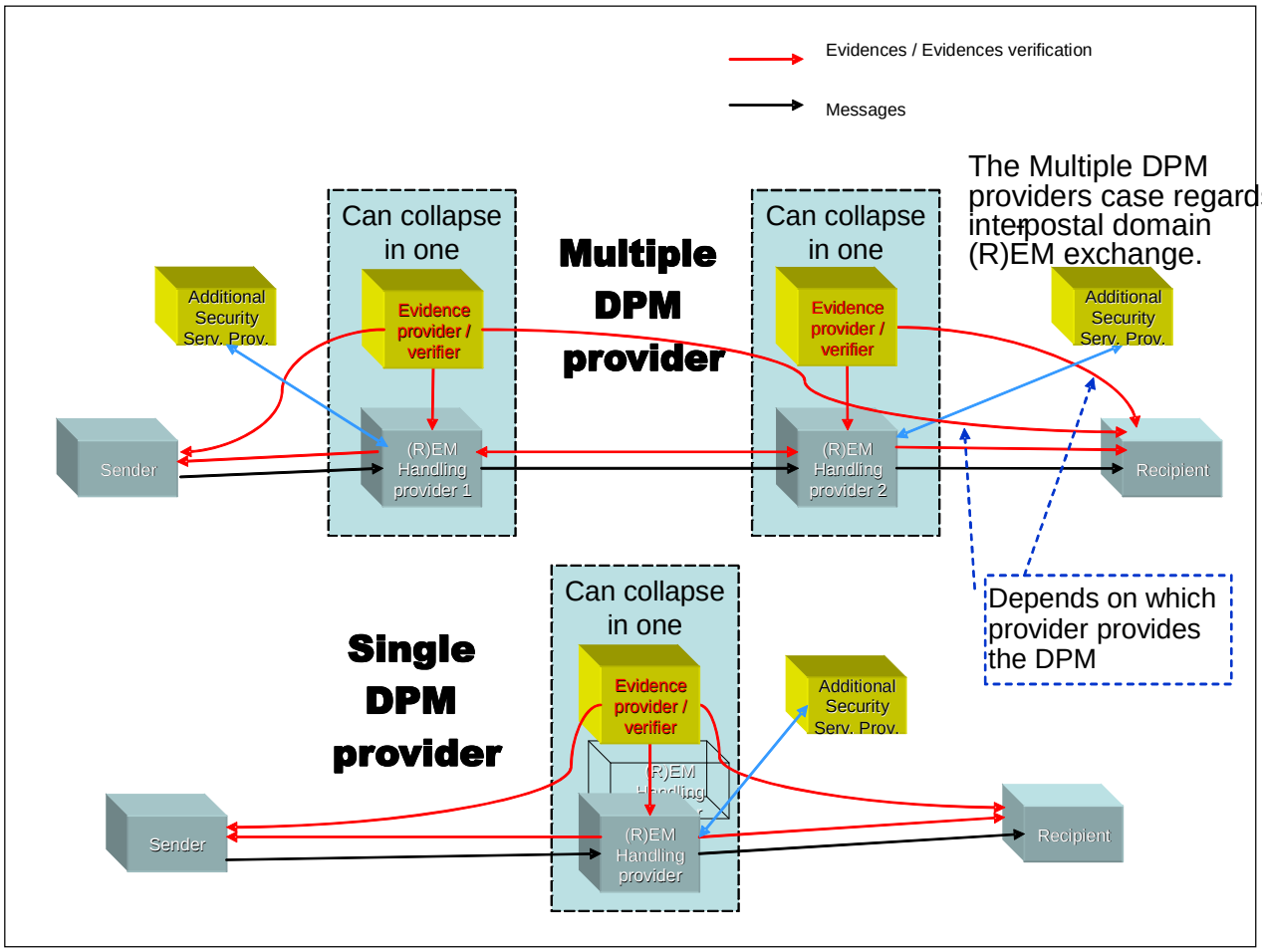


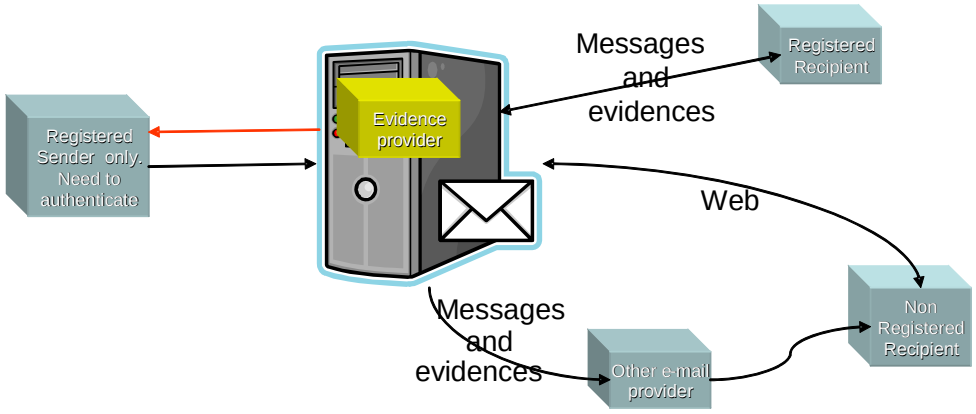
Figure 5: Model Adaptation for UPU ECPM

8.3.5 Critical Path model

Clause 9 graphically represents the various entities as in the international system developed by Critical Path (clause A.2.11).

NOTE: Other variants of the Critical Path system exists which are more aligned with the CNIPA model variant.

It is based on a unique mail repository where the being transported mails are stored. The recipient is notified via usual e-mail of the presence of an e-mail he/she can download from a URL specified in the notification.



- Senders must be registered.
- Recipients can be any and they receive an e-mail with the URL of the location the message can be downloaded from. Future implementations can envisage delivery to registered recipients of the entire message.
- Messages sent by "non CriticalPath" senders are forwarded to the CP registered user.

Figure 6: Model Adaptation for Critical Path

9 Services within REM

The present clause is about a more precise collocation of evidence services as described in clause 7, in the context of the model outlined in clause 8. In particular, the flow of services between the parties participating in the REM process will be explored, as well as some details given on how these services are provided, though leaving security issues to clause 10.

The analysis is based on answers to some questions in sections 5 and 6 of the questionnaire, and on some further non-structured investigations performed by the team. Some points of attention:

- 8 out of 39 respondents did not provide any reply to questions in sections 5 and 6. These questionnaires have not been taken into account for the purpose of the present analysis. The remaining 31 valid questionnaires are distributed as follows with respect to the category of respondents:
  - 7 from vendors of products;
  - 11 from service providers;
  - 5 from regulatory agencies;
  - 8 from respondents of other categories.
- 13 out of the 31 valid questionnaires did not provide any reply to questions in section 5.5. We assume that these responders refer to a model (see clause 8.1) where a single provider is present (see a similar conclusion at the end of clause 7).
- There are some cases where some light inconsistencies have been detected. Some cleaning of the source data was carried out where there was clear inconsistency between responses which could be easily resolved.
- There are some possible inconsistencies between answers in section 3.1 and answers in section 5. These differences were not taken into account.

9.1 Availability of evidence

This clause reports the results on the availability of evidence generated by the REM process, coming from answers to questions 5.3.2, 5.5.2, 5.7.2 and from further information collected by the team. The four elements which have been taken into account with respect to availability are:

- whether a given evidence is automatically produced (always) or only upon request of some party (on request);
- who generates each evidence (we did not consider whom is it directed to, since this point is not always clear);
- how the evidence is carried;
- whether a given evidence is delivered to the requester for his own records, or only provided as an on-line service.

9.1.1 Flow of evidence between parties

The table below presents data on who generates each evidence, giving details on the need of producing it. Figures inside one cell are in the form **X** + **Y** / **Z**, where: 'On Z respondents, X declare that the party to which the corresponding column relates always provides the evidence related to the corresponding row, while Y declare that the party indicated in the column provides the evidence related to the row only on request'.

The columns have the following meaning:

- **SND**: evidence generated by the sender.
- **SND REM**: evidence generated by the sender's REM provider.
- **RCV REM**: evidence generated by the receiver's REM provider.
- **RCV**: evidence generated by the receiver.

It is to be noted that there is not a clear match between answers to questions 5.3.2, 5.5.2, 5.7.2 and data collected in clause 7. Nevertheless no effort was done to reconcile data.

Table 11

Evidence service	SND	SND REM	RCV REM	RCV
a) Evidence of message origin authentication	24+5/31			
b) Evidence of submission		22+7/31		
c) Evidence that message has been transmitted through a REM service provider		16+5/30		
d) Evidence that message has been successfully exchanged between two REM service providers			9+3/16	
e) Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded		12+10/30	6+5/17	
f) Evidence of delivery/download		19+10/31	12+4/8	
g) Evidence of acceptance or rejection of message by the recipient		12+11/31	7+3/17	
h) Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)		21+6/30	12+2/17	
i) Evidence of non delivery/download within a predefined time limit		12+12/29	9+5/17	
j) Evidence that an email has been 'opened' or 'viewed' by recipient		9+11/31	4+4/16	7+8/25
k) Notification of errors		18+5/24	9+2/13	
l) Check for malicious code by receiver's provider			8+1/14	

Since the most relevant data is in the SND REM column, we slice the data above according to the type of respondent, considering the four categories Product vendor, Service provider, Regulatory agency, Other.

Table 12

Evidence service	Product	Service	Regulatory	Other
b) Evidence of submission	6+3/8	10+1/11	2+2/4	4+2/8
c) Evidence that message has been transmitted through a REM service provider	5+2/8	7+1/10	2+1/4	2+1/8
e) Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded	2+4/7	5+3/11	1+1/2	4+2/8
f) Evidence of delivery/download	3+4/8	10+1/11	1+3/4	5+2/8
g) Evidence of acceptance or rejection of message by the recipient	3+4/9	4+3/10	1+2/4	4+2/8
h) Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)	5+2/8	8+1/10	2+/4	6+1/8
i) Evidence of non-delivery / download within a predefined time limit	1+5/8	5+3/9	2+2/4	4+2/8
j) Evidence that an email has been 'opened' or 'viewed' by recipient	2+5/8	5+3/11	0+0/4	2+3/8
k) Notification of errors	4+6/6	10+0/10	2+1/4	2+2/4

9.1.2 Carrying evidence

Table 13 summarizes the results on how the evidences are carried with the original message (question 6.3).

Table 13

Carrying the evidences with original messages	Number of answers
As text attachment	4
As XML attachment	12
S/MIME p7s detached signature	8
S/MIME p7m object	4
Others	9
Different forms are used for different forms of evidence	2

An Austrian authority reports to use electronic signature as specified by PDF Reference. ChamberSign stores evidences in a server; it may be retrieved through a web-based interface by both sender and recipient. Also with ChamberSign third party XML-based notification contains time-stamp and checksum of the message sent. CNIPA and Poste Italiane mention that the actual signed message is made of a standard body text, the original message and an XML attachment. AFNOR and E-Group mention that the evidences will not be carried with the original message, E-Group adds that they may be downloaded from the REM service itself. DigiNotar reports using signed XML. Izecom mentions the use of a signed message container. Another supplier of services used in REM mentions carrying the digest plus email sender and email recipient identifiers. An Austrian respondent reported use of an electronic signature as specified by PDF Reference mechanism.

Postx reports that the system is configurable for allowing combinations of the alternatives mentioned in the table, and also depending on the type of evidence. ChamberSign, for their part, mentions that third party XML-based receipt contains information, time-stamp and checksum of the information sent.

9.1.3 On-line querying services without signed evidences

Whilst it was not specifically identified in the questionnaire it was noted that a number of REM providers supported on-line access for the evidence. The use of electronic signatures to support the authenticity of the evidence provided was not considered necessary as the data was held by the REM provider in trusted storage.

Some systems only allow requesters to have on-line access to that information. Some systems also allow recipients to have an on line access to that information, only if the recipient may be authenticated. However, these systems do not allow demonstrating easily to someone else that the service has been fulfilled.

Four organizations were identified as providing such on-line evidence services.

9.1.4 Specific conclusions on the availability of evidence

The following general points can be concluded from the above:

- Respondents to questions on evidence services provided by the receiver's REM provider (section 5.5.2 of the questionnaire) sum up to half of the sample. It is very low, probably because of models with one single provider (a similar conclusion in clause 7).
- The most relevant data is found in column **SND REM** (highlighted). In agreement with clause 7, a clear clustering of services was found:
  - 'core' services, which are almost always available, are:
    - Evidence of submission.
    - Evidence of delivery/download.
    - Evidence of non-delivery for unknown reasons.
    - Notifications of errors.

The above services are provided on request in one quarter of the cases, automatically provided for the rest.

  - 'Complementary' services, which are provided in 2/3 of cases, are:
    - Evidence of transmission.
    - Evidence of notification.
    - Evidence of acceptance.
    - Evidence of non-delivery in a time frame.
    - Evidence of opening.

The above services are provided both automatically or just on-request. There is not a common ratio automatic/on-request for all services.

- Slicing data by the category of the respondents allows to add the following considerations:
  - For core services, product vendors and service provider have almost total coverage. Service providers tend to make core services automatic (not on request).
  - For complementary services no useful distinctions can be identified.

As for the carrying of evidence, a first analysis of the responses in the questionnaire shows that XML attachment seems to be most prevalent but other ways are also supported and require to be taken into account: the number of respondent reporting other ways equals the number of those reporting using XML attachment.

9.2 Message identification

9.2.1 Allocation of message identifier

Table 14 summarizes findings regarding message identification, taking from answers to sections 5.3.3 and 5.5.3 of the questionnaire. The columns report:

- **Total**: (estimated) total number of respondents.
- **Must provide**: how many respondents declare the party must provide a message identifier.
- **May provide**: how many respondents declare the party may provide a message identifier.

Table 14

	Total	Must provide	May provide
Identifier allocated by sender	31	15	1
Identifier allocated by sender's provider according to 5.3.3.b	31	21	1
Identifier allocated by sender's provider according to 5.5.3.a	18 (see note)	15	0
Identifier allocated by sender **or** sender's provider according to 5.3.3.b	31	26	2
Identifier allocated by recipient's provider	18 (see note)	5	0
NOTE: Number of respondents which filled in section 5.5, for which it can be assumed there is a receiver's provider distinct from the sender's provider.			

9.2.2 Message Identification in Notifications

Table 15 summarizes the results on how the original messages are referenced in the notifications (from questionnaire section 6.2).

Table 15

Message referencing mechanism in notifications	Number of answers
Message Identifier	20
Message Hash	10
Message copy including attachments	7
Message body + hash of attachments	6
Others	5
Different forms for referencing are used for different notifications	3

Among those ones reporting other ways for referencing, ChamberSign (which supports message identifier and message hash) mentions that including a message copy is not implemented in the solution by default, although the sender and/or the recipient may choose to always store a copy of the message at Chamberlin's server (this only applies to the web based interface). Another supplier of services used in REM reports to use a mail stamp. National Security Agency from Slovak Republic reports using a structure including among other things, the hash of the message. Argeon suggests using both the digest and the subject of the message for easy and readable reference. As above, when answering this question, Poste Italiane reinforced its request for standardization. One respondent mentions using hash and message subject for easy readable reference.

Among those ones that use different forms of referencing depending on the notifications, CNIPA reports that message identifier, message hash and message copy including attachments are used only in the evidence of delivery, and where the sender's mail client allows for it, the sender can choose which type of message notification is required in the evidence of delivery he expects back. Poste Italiane mentions that the acceptance message only references the message identifiers assigned by the sender's client and by the sender's provider. ChamberSign reports that notifications may be sent through SMS. InfoCamere envisages three types of receipts, depending on user's will: complete receipt that includes both body and attachments; short receipt, including body and hash of attachments; and synthetic receipt, including only certification data.

9.2.3 Specific conclusions on message identification

There is a large consensus on the necessity that either the sender or the sender's provider allocates a unique identifier for message traceability (see highlighted row in the table in clause 9.2.1).

Most of the respondents point to the message identifier as the preferred referencing mechanism, although from the reported implementations it is clear that a potential standard should also allow for other types of information and even envisage different mechanisms for different types of evidences.

9.3 E-mail clients

Table 16 summarizes the results on information regarding the e-mail clients being used (question 6.1).

Table 16

Client type	Number of reported supports for senders	Number of reported supports for receiver
Outlook	17	14
Outlook express	14	13
Eudora	12	11
Thunderbird	13	12
Other e-mail clients	14	12
Webmail using active X / Javascript	13	13
Other webmail	11	9
Other	6	6

Apart from the e-mail clients appearing in the table above, other clients have been reported as used by certain respondents. Lotus Notes, Gmail, HotMail, Yahoo mail, Netscape Messenger, Mozilla and even a free-of-charge Java client for standalone use on several platforms (Windows, Mac, Linux and Unix). One responded to use nearly any supporting attachments.

To the question on Webmail, the answers give some additional information: one respondent claims to use an Ajax based webmail; another respondent reports usage of an STD browser with a one-time plug-in that is auto-installed when signature and / or encryption are required; a third one (Italian) reported that the service is also deployed as a contract signing portal and a portal for sending electronic tenders under the public procurement act; proprietary webmail usage is also reported. Finally there is one remark by one of the respondent that there are known certain problems with some webmail applications that do not support signed or encrypted e-mail.

As for other type of clients, a respondent interestingly reports that the REM is provided as a web service. Other respondent mentions a free-of-charge software development kit available to facilitate development of third party clients capable to communicate with the service's platform or integrate the service with third parties' applications. A third one reports to use a specific mail agent, since none of the agents available can implement the protocol developed for the service provision. Another one responded to use nearly any supporting attachments.

Interestingly, Poste Italiane responded that it would be appreciated if a standard is developed allowing the integration of the e-mail clients with specific REM related features.

9.3.1 Specific conclusions on e-mail clients

A first analysis of the responses in the questionnaire allows extracting the following conclusions:

- They show widespread use of multiple client types. Both, e-mail and webmail clients are being taken into account and used within these systems.
- There is at least one implementation of the REM services based on Web services.
- One respondent supported the standardization in this field as a way for facilitating the integration of e-mail clients with specific REM related features.

9.4 Interface to external services

Table 17 summarizes findings regarding interface to external services (non-registered e-mail and traditional surface mail), taking from answers to section 5.10 of the questionnaire.

Table 17

External service	Product	Service	Regulatory body	Other	Total
Number of respondents in the category	7	11	5	8	31
Interface to non-REM	4	5	2	1+1 (see note)	12
Accepting non-REM messages	¼	3/5	2/2	1+1/2 (see note)	7/12
Sending REM message to non-REM recipients	4/4	4/5	2/2	1+1/2 (see note)	11+1/12 (see note)
Interface to physical post	2	1	1	3	7
Interface to physical registered mail	2/2	0/1	1/1	2/3	5/7
NOTE: X+Y/Z: X interfaces in place, Y devised on Z respondents.					

9.4.1 Specific conclusions on external interfaces

The following general points can be concluded from the above:

- A good fraction of the sample provides an interface to non-registered e-mail, almost all of them granting delivery of messages to non-REM users.
- The slicing by categories shows that respondents grouped in 'Other' are less likely to provide this interface.
- Only a small fraction of the sample provides an interface to physical mail, still less to physical registered mail.

9.5 Use of independent service providers

Table 18 summarizes findings regarding the possibility to delegate part of the service to an independent provider, based on answers to questions 5.11 and 5.1.2.

Table 18

	Product	Service	Regulatory body	Other	Total
Number of respondents in the category	7	11	5	8	31
a) Signature provider	6	7	1	4	18
b) Signature verifier (entire certif. Path)	5	4	1	5	15
c) Encryption service provider	4	3	0	4	11
d) Decryption service provider	3	3	0	4	10
e) Time stamping provider	6	8	3	3	20
f) Long term archival service provider	5	5	2	3	15
g) System hosting	2	1	0	0	3

9.5.1 Specific conclusions on use of independent services

The following general points can be concluded from the above:

- From textual responses it can be understood that there are no particular constraints on the possibility of outsourcing part of the service.
- From a practical point of view, a good fraction of the sample outsources part of the service.
- As it is natural, service providers and product vendors are the category most prone to outsourcing.

- The most natural candidate for outsourcing is Time Stamping.

10 Security features

This clause summarizes the answers to a number of questions related to security issues and presents initial conclusions.

The analysis is based on answers to some questions in sections 5 and 6 of the questionnaire, and on some further non-structured investigations performed by the team. Some points of attention:

- As in clause 9, only 31 questionnaires can be considered as valid, 13 of which did not fill in section 5.5.
- There are some cases where some light inconsistencies have been detected. Some cleaning of the source data was carried out where there was clear inconsistency between responses which could be easily resolved.
- There are some possible inconsistencies between answers in section 3.1 and answers in section 5. These differences were not taken into account.

10.1 Authentication of parties

This clause deals with security in authentication between parties involved in the REM process, taking data from answers to questions 5.3.1, 5.5.1, and 5.7.1 of the questionnaire. The table represents the different authentication techniques prospected in the questionnaire, and their application to the communication between parties. Columns have the following meanings:

- **SND ←→ SND REM**: authentication between sender and its REM provider.
- **SND REM ←→ RCV REM**: authentication between REM providers.
- **SND ←→ SND REM**: authentication between receiver and its REM provider.

Table 19

	SND ←→ SND REM	**SND REM ←→ RCV REM**	**RCV REM ←→ RCV**
Authentication required	**21/31**	**10/31**	**19/31**
a) Simple Password	8	-	6
b) One time password	4	-	5
c) Cryptographic device (e.g. smart card, USB token)	15	7	14
d) Password over SSL / TLS	15	7	13
e) Software key	6	3	7
f) SAML Assertion	3	2	3
g) Client Public key certificate	5	-	4
h) Required but not specified	6	3	2

10.1.1 Specific conclusions on authentication of parties

The following general points can be concluded from the above:

- As expected, there is a marked symmetry between authentication **SND ←→ SND REM** and **RCV REM ←→ RCV.** For the dialogue between these parties only 2/3 of the sample declare some kind of authentication. All the rest probably do not require authentication (one respondent explicitly denies authentication).
- Among those providing authentication, the highest values are given to cryptographic devices and secured password.
- Very few respondents declared some authentication on **SND REM ←→ RCV REM**. This can partly be ascribed to models with a single provider.
- It is not possible to derive significant conclusions by slicing on the category of respondents.

10.2 Authentication of evidence

Several security mechanisms may be used for the qualification of evidence generated by the REM process. In the following the information collected via the questionnaire on this point are summarized. Specifically, questions 5.2.1, 5.4.1, 5.6.1 and 5.8.1 are addressed.

The table below summarizes the results. The columns account for:

- **TRUE:** the evidence service is provided according to answers to questions in 5.2.1, 5.4.1, 5.6.1. and 5.8.1, after considering the points of attention mentioned above. The denominator represents the sample dimension (please take into account that 6 questionnaires have been discarded).
- **AES: Numerator:** Advanced Electronic Signature is used for the service. **Denominator**: the service is provided.
- **QES: Numerator:** Qualified Electronic Signature is used for the service. **Denominator**: the service is provided.
- **AES or QES: Numerator:** Advanced Electronic Signature or Qualified Electronic Signature are used for the service. Denominator: the service is provided.
- **TS: Numerator:** Time Stamp is used for the service. **Denominator**: the service is provided.
- **TM: Numerator:** Time Mark is used for the service. **Denominator**: the service is provided.
- **TS or TM: Numerator:** Time Stamp or Time Mark are used for the service. **Denominator**: the service is provided.

Table 20

Evidence service	TRUE	AES	QES	AES or QES	TS	TM	TM or TS
a) Evidence of message origin authentication provided by sender	24/33	15	22	24/24	17	8	19/24
a-bis) Evidence of message origin authentication provided by sender's provider on behalf of the sender	22/33	13	14	21/22	20	7	22/22
b) Evidence of submission	24/33	17	10	24/24	18	12	24/24
c) Evidence that message has been transmitted through a REM service provider	17/33	9	8	16/17	12	10	17/17
d) Evidence that message has been successfully exchanged between two REM service providers	12/33	10	5	12/12	7	10	12/12
e) Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded	14/33	8	6	13/14	7	10	14/14
f) Evidence of delivery/download	17/33	11	8	15/17	11	11	17/17
g) Evidence of acceptance or rejection of message by the recipient	11/33	7	7	11/11	6	10	11/11
h) Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)	16/33	11	7	16/16	9	9	15/16
i) Evidence of non delivery/download within a predefined time limit	12/33	9	5	12/12	8	7	12/12
j) Evidence that an email has been 'opened' or 'viewed' by recipient	15/33	9	12	15/15	15	4	15/15

10.2.1 Specific conclusions on authentication of evidence

The following general points can be concluded from the above:

- when an evidence service is provided, it is almost always supported either by an advanced electronic signature or a qualified electronic signature (sometimes both are allowed);
- when an evidence service is provided, it is almost certainly supported by either a time mark or time-stamp (sometimes both are allowed);
- there was no significant preference between use of advanced and qualified electronic signatures;
- there was no significant preference between use time-marking and time-stamping.

10.3 Signature formats

The signature format used in the REM systems was also surveyed (questionnaire section 6.4). Table 21 summarizes the results analyzed so far.

Table 21

Signature format	Number of answers
S/MIME (RFC 3851 or previous version)	12
CMS (other than within S/MIME - RFC 3851 or previous version)	8
XML Sig (RFC 3275 / W3C Recommendation)	6
CAdES (TS 101 733 [8])	6
XAdES (TS 101 903 [9])	7
Others	4

Among those that reported other signature formats, an Austrian respondent reports use of electronic signature as specified by PDF Reference (http://www.adobe.com/devnet/acrobat/pdfs/pdf_reference.pdf, section 8.7). ChamberSign uses a non standard XML signature. The Slovak Republic National Security Agency suggests the use of ZEP(ZIP) defined in Qualified Electronic Signature Formats (http://www.nbusr.sk/en/electronic-signature/approved-formats/index.html).

10.3.1 Specific conclusions on signature formats

The answers to this question indicate that services make use of different electronic signature formats. Formats traditionally associated to electronic mail (S/MIME and CMS) prevail so far. It is worth to note that XML-based formats are also present (XML Sig gets 6) and that formats for advanced electronic signatures are reported to be used almost as much as CMS (7 for XAdES and 6 for CAdES against 8 for CMS). The results suggest that solutions for REM should be designed in such a way that any signature format could be used, taking into account advanced electronic signature formats, as their use seems to be increasing.

10.4 Time-stamping and time-marking

The time-stamp format used in the REM systems was surveyed (questionnaire section 6.5). 20 respondents' use of RFC 3161. Some respondents report use of ETSI profile defined in TS 101 861 [14]. 6 respondents report on other formats. Bankinter reports preference for ISO 18014 time-stamps. UPM-ACEPTA reports to use its own time-stamping protocol developed by CryptoLab. Apart from that, CNIPA and Poste Italiane mention that time-stamping is used only when extracting the PEC system log to long term storage and that all evidences bear a time mark, that does not go below the second (i.e.: fractions of seconds are not envisaged). SETCC reports use of a time-stamp XML format specified by Entrust. CATCert suggests use of XML format as defined by OASIS Digital Signature Services TC. eNotaris reports use of internal marks. UPU reports that the server signs a XML document specifying time and date with a link to the message, as a way of building a trusted time on the message.

Six respondents report on time-marking (questionnaire section 6.6). InfoCamere uses time-marks with tolerance of 1 second, expressed in local time plus indication of distance to UTC time. IT Telecom manages time-marks as text in message body and in XML attachments. CNIPA and Poste Italiane report usage of time-marking for the evidences. CriticalPath mentions use of time references inside the REM provider generated messages, extracted from a trusted time source.

As for the time source for time-stamps and / or time-marks, the table below shows a summary of the answers got so far.

Table 22

Time source for time-stamps and / or time-mark	Number of answers
Synchronization with a source calibrated with UTC in line with ITU-R Recommendation TF.460-4 [13]	13
TP synchronization	4
GPS time source	10
Others	4
No synchronization	0

Among those reporting other ways, InfoCamere uses NTP synchronization, which is also suggested by the Slovak National Security Authority; Argeon just states that the time-stamp should be provided by a trusted/certified peer; Critical Path mentions NTP, radio or other cards for time-marks, and delegates in the TST provider the issue of the time source.

10.4.1 Specific conclusions on time-stamping and time-marking

RFC 3161 timestamps are used by a greater number of respondents than other formats. Nevertheless some responses seem to prove that other formats are also starting to be considered, some of them using XML syntax. REM solutions should, in consequence, be designed to accommodate use of different time-stamps formats.

Six respondents report on time-mark usage, which should also be taken into account when designing REM solutions.

As for the synchronization method, the preferred one seems to be calibrating the source with UTC in line with ITU-R Recommendation TF.460-4 [13].

10.5 Security protocols

Security protocols used by the REM systems were also surveyed. 24 entities responded pointing to Secure Socket Layer / Transport Layer Security. Among the 4 entities pointing to other protocols or additional notes IT Telecom reports SMTP/S, POP3/S and IMAP/S; SwissPost reports SOAP/WSS, CNIPA mentions that SSL is used by providers to access the CNIPA managed list of PEC providers' CNIPA issued certificates, via SSL certificates issued by CNIPA and that providers mutually authenticate to each other via commercially issued SSL certificates. Finally E-Notaris-Norway mentions using security protocols only for Web, not for e-mail.

10.5.1 Specific conclusions on security protocols

From what has been said above, it seems that SSL/TLS are the preferred security protocols among the entities that answered the questionnaire, although other protocols should not be banned.

10.6 Supporting services

The PKI / signature supporting services used by the REM systems were also surveyed (questionnaire section 6.9). The table below summarizes the answers obtained so far.

Table 23

PKI / signature supporting services	Number of answers
LDAP Directory	17
X.509 Certification Authority	27
X.509 Certificate Revocation Lists	27
OCSP (RFC 2560)	16
Digital Signing servers for signature creation	13
Digital Signing servers for signature verification	13
Hierarchical CA structure	18
Peer to peer CA structure based on Trust Status Lists (TS 102 231 [15])	0
Peer to peer CA structure based on TSL like	1
Other CA structure	0
Other Services	1

AFNOR mentions that full freedom in terms of supporting services should be given to REM providers as long as they allow to support CAdES as this as this is the mandatory signature format.

10.6.1 Specific conclusions on supporting services

From the answers gotten so far, it is clear that the well-known usual services are required; that CRLs are generally used, although the number of entities reporting on OCSP is also high, and that the trust model is hierarchical in all the cases.

11 Policies and practices

11.1 Registration

The results of the questions regarding registration (questionnaire sections 7.1 to 7.5) are as follows:

NOTE: Figures given in the following tables are for: Overall, (Products, Services, Regulatory, Other).

Table 24

Are senders / recipients securely identified at registration time? NOTE: In many cases a NO response was given as registration system was not secured.	**Yes - 18**	**No - 8**
Registration by face to face presence with documentation supporting identity	11	
Remote authentication through previous identity check	13	
Others responses: company register, no face to face required, previous face to face, variable depending on client, receivers not registered	7	
Users are always registered both as a sender and as a recipient. Other comments include: configurable per user, recipient unregistered, recipients may register when requiring to use service	Yes - 17	No - 11
Can an existing e-mail box, previously assigned to a person, be assigned to a new assignee, to be securely identified at registration time: (e.g. where a mailbox is identified as belonging to a department it can be assigned to several individuals in sequence) Special conditions include: • being within the same company or group or public administration; • upon death / guardianship; • Mailboxes are under a responsible person's control who can manage them as deemed suitable.	Yes - 13	No - 8
When registering, are senders / recipients required to sign a contract or agree to some other form of undertaking as individuals. This included: • Consent to communicate electronically. • CA/CSP Certificate issuance. • REM Service contract, service level agreement. • Agreement to download messages with given time-frame. • User agreement. • Agreement for paid commercial service. • Contract agreement to service conditions. • Follow usage rules. • Subscriber is aware of conditions. • Only applies to senders. Further documentation provided by (FNMT-RCM) (Royal Spanish Mint).	Yes - 17	No - 9

11.1.1 Specific conclusions on registration

Registration can be optional particularly for recipients. Users may need to indicate agreement with conditions on registration although this may not necessarily be signed.

Most systems require sender's registration and authentication. Registration may be necessary to create a user account, so that the sender may be charged for the service and easily re use its account, but does not necessarily imply that sender's authentication is supported as a service by the REM service provider. Some systems (e.g. the AFNOR model) do not require sender's registration and authentication.

Roughly half of the systems require the registration of the recipients. In these systems, senders may also be recipients within the same closed community (e.g. IncaMail from SwissPost). Some systems do not require any recipient pre-registration, (e.g. the AFNOR model). Some other systems allow for exchange of e-mails with non registered users, as senders or as recipients, by in this case they, therefore, might not fully benefit from the evidences mechanism.

11.2 Security management

The results of the questions regarding security management (questionnaire sections 7.6 to 7.7) are as follows.

Table 25

Does the system operate under a defined Security Policy?	Yes - 20	No - 4
Does the system operate under an ISO/IEC 27001 [5] based Information Security Management System? Or certified to be conformant	Yes - 7	Yes and certified 5

11.2.1 Specific conclusions on security management

Most of the respondent claim to operate the systems under a defined security policy. Half of them claim to operate them under an ISO/IEC 27001 [5] based Information Security Management System. AFNOR has published a policy for REM service providers (AFNOR AC Z 74-600 Part 4).

11.3 Security of signing device

The results of the questions regarding use of security management standards (questionnaire sections 7.8 to 7.9) are as follows.

Table 26

What type of signing device is employed in service provider: Others include: • solution / policy specific; • Software for servers.	HSM - 21 Smart card / USB - 12 Software key - 12 Other - 2
Are hardware security modules / smart card signing devices used for signing certified conformant to?	CWA 14167-2 = 0 CWA 14167-4 = 1 CWA 14169 = 5 Common Criteria (ISO/IEC 15408 or equivalent) = 7 Level: E3, EAL4+ ITSEC = 3 Level: E3 / E3(High) FIPS 140-1 0r 140-2 = 11 Levels 1 to 4

11.3.1 Conclusions on clause 11.3

11.3.1.1 Security of signing device

There is no prevalence of any security criteria, apart from FIPS (levels evenly distributed between 1 and 4 with a slight prevalence for 3).

12 Related standards activities

12.1 AFNOR Z 74-600

AFNOR has developed a workshop agreement dedicated to REM services targeted to mimic the existing services that exist for surface mail.

12.2 UPU & CEN Electronic Postal Certification Mark (EPCM)

Standards have been developed by the Universal Postal Union, in conjunction with CEN TC 331, for Electronic Postal Certification Mark (formerly referred to as Digital Post Mark or Electronic Post Mark) (see clause 8.3.3).

The current UPU / CEN standards for Digital Post Mark are:

UPU S43-3

This document is the UPU equivalent of CEN/TS 15121:2004. It specifies an XML based interface to third party verification, time-stamping and related services in support of EPCM (referred to previously as Electronic PostMark).

- **CEN TS 15130 [2]:** This specifies XML based messages for the use of supporting services for:
  - key management processes;
  - licensing and parameterization of mailing systems;
  - data collection and reporting processes;
  - audit-related process.
- **OASIS DSS EPM Profile [3]:** This defines XML messages for the use of network based digital signing services in support of EPCM (referred to as Electronic PostMark). Many of the XMLDSIG constructs in the Electronic Postmarking service were patterned directly after the OASIS DSS core and its EPM Profile. For the most part, the EPM and the OASIS DSS core and profile specifications evolved together and hence share numerous schema constructs.

Other standards relating to EPCM are understood to be under development but were not available to the study team.

- UPU S39: Trusted Time Stamp.
- UPU S33: Interoperability Framework for Postal Public Key Infrastructures.

12.3 General security standards

A number of standards exists for the security of information systems. Most relevant are:

- **ISO/IEC 27001 [5]:** This specifies a method of managing the security of information systems to ensure that the security controls are applied necessary to address the identified risks. Such 'Information Security Management System' provides a technique for assuring that the operation of providers of REM services are secure and apply the controls necessary to meet identified policy requirements.
- **ISO/IEC 13888 [4]:** This specifies mechanisms for provision of non-repudiation services including non-repudiation of origin, submission, and delivery which may be used to provide proofs for REM.

12.4 Specific conclusions on related standards activities

In France, AFNOR agreement Z 74-600 defines the structure of evidences and provides interoperability between REM service providers. It also defines a security policy generally applicable to REM service providers.

The EPCM specifications define a set of basic functions that may be used to build different kinds of services, including REM services. They essentially relate to a digital signature verification and timestamping authority which verifies and logs as evidence, the content integrity of electronic information. The EPCM specifications identified above are currently having only national Postal services implementations, therefore do not directly cover all the services relevant to a freely operated open Registered E-Mail, and do not appear as covering aspects required to ensure interoperability with such REM systems user, nor interoperability between these REM systems. As of now, in fact, it appears that no operation is yet implemented across EPCM authorities. These specifications primarily address standards for use of supporting services for EPCM.

The general approach underlying the EPCM standards has in any case relevance to REM and so any REM architecture should incorporate EPCM concepts. Interfaces to third party services supporting REM compatibility with the UPU S43-3 should be considered.

13 Conclusions and recommendations

13.1 General conclusions

The main conclusions of this study are:

1) There already exists significant number of deployments, as well as a large potential market, for Registered E-Mail services in Europe, with services existing or planned in at least 10 European nations with an existing user community of over 500 000 (see note) and potential community of 100 million.

2) Registered E-Mail services can be broadly categorized into operating under the following three classes of legislation:

   - REM evidential services operating under specific legislation.
   - REM services provided by public administrations with public notarization functions.
   - REM services operating under general electronic signature and contractual legislation.

The last is subject to most legal uncertainties.

3) In order to provide maximum legal certainty REM evidence services should be provided by an independent party with trusted internal controls.

4) The most important REM evidence services are:

   - Evidence of message origin authentication.
   - Evidence of message submission.
   - Evidence of delivery and non-delivery.

5) Support for evidence services can be required for all the stages of message handling from origin and submission, through transfer between REM service providers, to delivery and being opened or viewed by the recipient.

6) Services for confidentiality of content are generally considered as an important adjunct to REM. Anti-virus and anti-spam may also be provided with REM.

7) Currently there is only limited support for external connections to physical post or other non-REM-services. However, there is sufficient support for external email servers that its implications should be considered in future standardization.

8) A broad range of approaches are employed in existing REM systems.

9) It is considered possible to identify a generic architecture within which different approaches may interoperate. However, significant work is still required to specify the details of such an architecture.

10) A number of respondents reported use of XML in encoding evidence, although an equally significant number reported a range of other mechanisms.

11) There is consensus that the sender, or the sender's REM provider, should allocate a unique identifier to a message.

12) Users of REM services employ a range of email clients including web clients.

13) Outsourcing is commonly employed for the provision of parts of REM services.

14) Most commonly both sender and recipient access to REM services using passwords over a secure (e.g. SSL protected) channel. In some cases, a cryptographic device (e.g. smart card, USB token). Only in one case is sender authentication not required.

15) Users are most commonly authenticated using cryptographic devices or secured password.

16) The evidence services nearly always employ advanced or qualified electronic signatures with a time-mark or time-stamp.

17) Both XMLDSig [10] and CMS [7] based signatures are employed.

18) Generally evidence services are provided automatically rather than on request from users.

19) Either the sender or the sender's service provider is required to provide in most cases some form of unique reference for each message.

20) In a number of REM systems the evidence of submission / delivery etc is held by the REM service provider for on-line access (e.g. via a web service). In such cases the evidence may not be signed which may restrict its evidential weight.

21) Timestamps are most commonly conform to RFC 3161 and are often synchronized with UTC as in ITU-R Recommendation TF.460-4 [13].

22) In several cases REM services have a ISO/IEC 17799 based 'information security management system' some of these certified under ISO/IEC 27001 [5].

23) A range of solutions are employed for holding the REM service provider signing key, including HSMs, smart cards and software keys. In a number of cases these are certified in accordance with FIPS or common criteria.

24) Standards exist for Electronic Postal Certification Marks (EPCM) which may be related to REM (see clause 12.2). They may be related to REM but essentially these involve a digital signature verification and timestamping authority which verifies and logs as evidence, the content integrity of electronic information. The EPCM specifications identified above are currently having only national postal services implementations, therefore do not directly cover all the services relevant to a freely operated open Registered E-Mail. Additionally, they are not declared as covering aspects required to ensure interoperability to users such REM systems user, nor interoperability between these REM systems themselves. As of now, in fact, it appears that no REM related operation is known to be implemented across EPCM authorities. These specifications primarily address standards for use of supporting services for EPCM.

13.2 Recommendations regarding work plan for next phase

Purpose: The aim of the activity is to establish standards for the provision of signed evidence in support of registered electronic mail.

Motivation: This is to ensure a consistent form of service, especially with regard to the form of evidence provided, across Europe and maximize interoperability between REM service providers. Thereby competition between REM providers is maximized and users are able to transfer easily between service providers.

Impact of non-standardization: A range of REM services are already established across Europe and the number of services are set to grow significantly over the next few years. Without the definition of common standards there will be no consistency in the REM service provided, making it difficult for users to compare the offerings of REM service providers, and users will be locked into single REM providers without the ability to easily transfer to alternative providers. Additionally, lack of standardization might affect interoperability between REM based systems implemented on the basis of different models.

Proposed Deliverables for Next Phase:

The output deliverables for this activity should be:

1) Architecture for the provision of signed evidence in support of Registered E-Mail

This will include:

a) the architecture elements involved in REM, e.g. sender, recipient, servers, etc.;

b) example uses of these architectural elements for REM implementations that are able to interact with existing REM systems;

c) use of digitally signed evidence to provide proof of submission, delivery etc in order to avoid sender's and recipient's denial / repudiation of an email;

d) evidential services based on trusted information exhibited by a trusted party;

e) time-stamping / time-marking provided by a trusted party;

f) data required for different evidence and information services in REM;

g) messages, notifications and other information flows, identifying possible sources and destinations and triggering events (error, message submission, message transfer, deposit, withdrawal, transmission between servers, delivery, etc.);

h) identification of required interconnection between REM providers including trusted gateways to map data formats;

i) the option for REM service interfaces based on Email and Web.

2) Data requirements and formats for signed evidence in support of Registered E-Mail

This will include:

a) the definition of the functional content of the various evidences, including the data elements that must be present and may optionally be present in these evidences;

b) the format of the evidences, using syntaxes like XML, ASN.1 XML within PDF.

3) Policy requirements for trust service providers supporting Registered E-Mail

This will include:

a) obligations of parties involved (e.g. ability to exhibit evidences, minimum terms storage: what is stored and for how long, etc);

b) requirements based on ISO/IEC 27001 [5], with additional REM specific requirements;

c) internal controls to be implemented by all the parties involved in providing evidence to ensure confidence in services;

d) requirements for audit.

Annex A:
Main approaches

A.1 Main approaches - standards

This clause includes a description of the de jure or de facto standards, specifications, agreements or regulations providing common basis for implementations.

A.1.1 France - AFNOR

AC Z 74-600 is an AFNOR agreement published by AFNOR as the result of a workshop. The sender's REM service provider is different from the recipient's REM service provider. The REM services have been initially defined to mimic the services that currently exist with surface mail. This means that:

- Senders do not need to register and are not authenticated.
- Recipients do not need to register.

The model supports the concept of 'requestor': requestors may be different from senders. Requestors receive the **attestations** and pay for the service. They do not need to authenticate: the service will be provided as soon as the requestor pays or may be billed. The model supports the concept of 'verifier': a verifier is any party wishing to verify an attestation.

The attestations defined to mimic the existing surface mail services are:

1) Attestation of deposit for **reception** : allows attesting that some data was deposited in order to be delivered to a recipient who will need to authenticate using a **PKC chosen by the sender** and that an attestation of reception has been requested.

2) Attestation of reception or non-reception: allows attesting that some data has been received or not received by an authenticated recipient. The recipient MUST use the **PKC chosen by the sender**.

3) Attestation of deposit for transfer : allows attesting that some data was deposited in order to be delivered to a mailbox.

Two additional attestations do not correspond to an existing surface mail service. In order to stress the major difference with the attestation of reception, these attestations are called differently :

1) Attestation of deposit for **retrieval** : allows to attest that some data was deposited in order to be delivered to a mailbox using a **password chosen by the sender** and that an attestation of retrieval has been requested.

2) Attestation of retrieval (or non retrieval) : allows to attest that some data has been retrieved (or not been retrieved) by the owner of the mailbox using a **password chosen by the sender**.

Attestations are returned to the requestors and may be verified without the need to connect to any REM service provider. The attestation is always an Advanced Electronic Signature (AdES). The CAdES format has been chosen. The attestation is always signed by the sender's REM service provider, i.e. never by the recipient's REM service provider, and may be verified by anybody trusting the REM service provider policy. The detailed content of each attestation is defined using ASN.1.

E-mail (i.e. SMTP) is not necessarily used: the data will not necessarily be deposited or delivered by e-mail since it may be too large for the mailbox size. The idea is to deposit it or to collect it using HTTPS or FTPS. This allows protecting the confidentiality and the integrity of the data between the REM service provider and the requestor or the recipient.

A.1.2 Italian legislation based REM systems

The registered e-mail in Italy (Posta Elettronica Certificata - PEC) implements a mechanism providing services similar to the registered surface mail: the sender is given by its provider a receipt of acceptance (or a warning of non acceptance if the message being sent either is formally incorrect or contains viruses) and gets back a receipt of delivery/non delivery issued by the recipient's provider, that can be the same as the sender's if it serves both parties. Where the recipients is not served by a REM provider the sender will not receive this delivery receipt.

The whole mechanism is covered by an exhaustive legislation, addressing also technical details, that provides per se legally valid evidence of sending and of delivery/non delivery.

PEC providers must achieve accreditation at CNIPA (National Centre for Informatics in Public Administration, a government body) to operate as such. This is ensured by CNIPA that, acting also as the PEC related Certification Authority, issues to each provider the certificates necessary to support the messages signature (see below). CNIPA acts also as the supervision body on PEC providers.

This legislation lays down:

1) requirements on the PEC provider, and in particular:

   a) rules, policies and practices the provider must have in place in order to get accreditation as PEC provider, such as: company type (where they are not Public Administrations they must be Limited Companies) and capital, personnel organization including names, senior management's trustworthiness requisite that is the same as for banks, need for a specific insurance policy, etc;

   b) need for the provider applying for accreditation to provide the accreditation body (CNIPA) with a detailed description of the service operating procedures and of the implemented security measures.

2) requirements on the service, with particular focus on:

   a) minimum service level requirements: overall uptime $\geq$ 99,8 % per four months period, down time $\leq$ 50 % of the previous maximum 0,2 % down time per four months period;

   b) documents/messages flow;

   c) how to handle the exceptions;

   d) requirements for PEC events logging, timestamping and storage (for 30 months);

   e) requirements for virus bearing messages storage (for 30 months).

3) technical specifications on messages and evidence:

   a) messages types;

   b) specifics (structure and content) of the XML messages exchanged between the parties (Sender - sender's server - recipient's server - recipient), see below;

   c) signature specifics trusted time source (UTC $\pm$ 1 sec.) to be used by the providers.

The main features are:

1) All messages produced by the providers are signed with AdES issued with SSCD and based on certificates issued by the CNIPA CA acting as a root CA for PEC.

2) Each sent e-mail is enveloped by the sender's provider in a signed message that includes an XML structure with the message data: originator, sender's provider, time and date, etc.

3) All messages are inspected for virus, where a virus is found the message is quarantined for 30 months and the sender is notified.

4) Anomaly envelopes, bearing a non-REM message (where a provider accepts delivering its users this type of messages) or a formally incorrect message, delivered to recipients.

5) CNIPA created interoperability test sets must be successfully executed.

6) Service is to be deactivated where a non conformant system behaviour is identified.

7) Providers must communicate to CNIPA the service level achieved.

8) Minimum 50 recipients must be managed; minimum 50 MB (message size 'n' number of recipients) must be transmitted.

A.1.3 UPU Electronic Postal Certification Mark

The Electronic Postal Certification Mark (EPCM - formerly known as Digital Post Mark or Electronic Post Mark) is essentially a digital signature verification and time-stamping authority which verifies and logs as evidence the content integrity of electronic information. All electronic evidence can cryptographically be verified and stored in support of potential disputes. It applies to a community making use of services provided under the responsibility of national Postal Administrations.

A EPCM Service **can** support the capture and reproduction of evidence data attesting to the fact that a **business** transaction was conducted and completed in an environment of integrity and trustworthiness with respect to one or more of a number of attributes, among which the following ones:

- Who originated the transaction.
- Who participated in the transaction.
- When was it received by each participating party.
- Was the content intact throughout transmission.
- Have all parties been notified of all agreed events of significance.

Postal implementations are free to authenticate users using their mechanism of choice.

The EPCM is a set of the following standardized application layer software security services, that can be utilized individually or in any combination.

- Digital signature verification of the message being submitted to the EPCM server, including certificate status verification, when proof of origin (i.e. non-repudiation of origin) is required by the user.
- Time-stamping of verified signatures through issuance of a Post MarkedReceipt, that contains three core pieces of information: the Receipt containing a timestamp, the referenced user content being Post Marked and a signature of authenticity binding everything together; it may also apply to a non signed datum and in this case the PostMark just asserts the existence of such datum at a certain time, without implying any inference on its origin; the outcome of these operations is:
  - receipt issuance;
  - content time-stamping.
- Digital signature creation by the Postal service on a datum submitted by the sender, on behalf of the sender, to demonstrate the recipient that the Postal service authenticated the sender.
- Capture of signature intent (context and user commitment).
- Creation of encrypted envelopes on behalf of the sender.
- Decryption of encrypted envelopes on behalf of the recipient.
- Evidence logging of all EPCM Service events.
- Logging of user events deemed relevant to the business transaction.
- Tying together of EPCM events into a business transaction lifecycle.
- Retrieval of evidence data in support of dispute resolution and future challenges in a non-repudiation context. Clients pass in content from a previous operation and have that content compared against the original version stored in the EPM's non-repudiation log.

Additional services, such as provision to the requesters of encryption certificates, providing receipts rendering details specific to the country of receipt origin, are also available.

Information produced by the elementary services, depending on the contractual relationships with the Postal Administration providing EPM services, can be forwarded along the Postal Administration e-mail services or along external a-mail services.

The EPCM compliant service can support a range of service such as non-repudiation of origin, of submission, of delivery, of receipt and, where combined with user-authentication and message integrity, it can ensure a totally non-repudiable electronic business process. Therefore the EPCM Services, through the implementation of jurisdiction-specific legislative requirements, could be able to be used to build a legally binding transaction notarization service both within and across Postal domains.

EPCM services providers can implement a document pickup facility. To this purpose the 'sign for pickup' facility, that requires a signed request by the recipient to retrieve the datum, provides end-to-end non-repudiation and proof-of-delivery without the involvement of any public e-mail service provider.

The Postal Administration provides the individual or organization any and all required evidence of the existence, integrity, or logged time of any business transaction tracked by the service. This information can be reproduced digitally or physically and can be sent to any required arbitrating party for their assessment.

The computer systems of the EPCM service are hosted by, and under the jurisdiction and control of, the Postal Administration. Subscribing organizations are not required to physically host the service themselves, but rather pay for the use of the service itself.

Physical control and access of both the EPCM's systems and its non-repudiation logs must be under the sole responsibility of the Postal Administration. Only the following services can be outsourced:

- All digital certificate life-cycle management activities.
- EPCM System Software and Database Infrastructure Hosting.
- EPCM System Software Backup and Recovery.
- EPCM Non-Repudiation Database Backup and Recovery.

In addition to what is specified in the 'Global EPM Non-Repudiation Service Definition and the Electronic PostMark', the 'Electronic PostMark (EPM) Interface Specification' Errata 4, of 15 September 2006, reads:

'The scope of this update does NOT include:

- A description of the issues surrounding inter-operability between multiple postal EPM implementations when a business transaction lifecycle requires the participation of more than one EPM implementation in a cross-postal Administration scenario.
- Issues surrounding EPM usage in a multiple Certificate Authority scenario where inter-operating posts are participating in a cross-border transaction as described above.
- Examination of 'Certificate Authority deployment model' alternatives necessitated by the cross-border scenarios described above.'

A.2 Main approaches - implementations

This clause describes systems and products which do not directly follow any particular REM standard, as described above, or is a significant variation of a standard.

A.2.1 Austrian electronic delivery

A complete online transaction is impossible without an electronic delivery system. Citizens approaching the administration by electronic means expect electronic replies. These are provided by an electronic delivery agent, which ensures that documents from the public authority are sent to citizens in a verifiable manner.

The 'delivery' specification (see note 1) serves the exchange of data and information between authorities and the delivery agent. The principal information requirements for the delivery are the recipient, the document to be served and organizational data and attributes intended to secure data integrity. The structure has been defined as optional as possible in order to allow combinations. Not all the elements need necessarily be used. It is therefore more an information than data model.

NOTE 1: http://www.cio.gv.at/it-infrastructure/delivery/.

Generally, the data structure is based on standard types and definitions of the W3C XML schema Part 2 and definitions of the XML signature syntax and processing (XML DSig). In justified cases, special types and elements were defined.

The basic XML structure serves as an envelope for the individual information clusters. The actual application data (elements of administrative notices, etc.) are intended to act as stand ins. The delivery data can generally be signed. Nevertheless, the data in notices must be signed.

The individual functions are defined in the specification.

The identification type describes a variety of identification attributes. Particularly characteristic is the document identification attribute (value of identification, type, issuing authority, additional attribute).

The information cluster of delivery data defines the document identification of the delivery container, the delivery service, the metadata (quality requirements such RSa, date of dispatch, time stamp, date of notification, recipient for confirmation purposes, etc.), validity, notification element and documents to be delivered in XML or another data format.

The delivery confirmation contains the related information as to whether or not delivery was successful. The actual delivery data are not retransmitted but are referenced.

If the delivery agent fails to collect a document, the sending authority is informed by way of retransmission of the data.

Communication Structures

Electronic delivery is carried out in accordance with a two-layer protocol. As a first step, a request is sent by HTTP-Get to the delivery centre for information as to whether the recipient is registered with a delivery agent. The data are represented internally in a directory of the delivery agent and can be requested by way of an LDAP protocol. As a second step, communication is exchanged with the recipient's delivery agent. This communication between the sender and the delivery agent takes place via an XML interface. The structure and requisite specification profiles for the individual XML messages are described in the specification (see note 2). The interface is composed of several specifications:

- SWA (see note 3) makes it possible to transport SOAP messages containing additional information in the form of attachments. These may be used where binary files such as PDF or ZIP are sent. In the case of encrypted content, the encryption container can also be delivered as an attachment.
- SOAP creates the envelope the data on use. The message itself is contained in the SOAP body.
- ZUSE (see note 4) contains the basic data for delivery (quality of delivery, time-limits, etc.).
- The delivery process entails three messages (send document, send proof of delivery, send notice of impossibility of delivery).

- Where encrypted data are sent, the S/MIME standard is used, which itself is based on the CMS standard (see note 5). The sender encrypts the document in accordance with S/MIME (see note 6). The data are transferred as an attachment. The delivery agent accepts the data. During the collection process, the delivery agent must offer the data to the user as an RFC 2822 (see note 7) S/MIME message for downloading or forwarding. The data can also be offered in their original form as a CMS data file.

NOTE 2: http://www.cio.gv.at/it-infrastructure/delivery/spec/.

NOTE 3: SOAP with attachments.

NOTE 4: Delivery model.

NOTE 5: Cryptographic Message Syntax.

NOTE 6: Secure Multipurpose Internet Mail Extensions.

NOTE 7: Internet message format.

Delivery Directory Schema

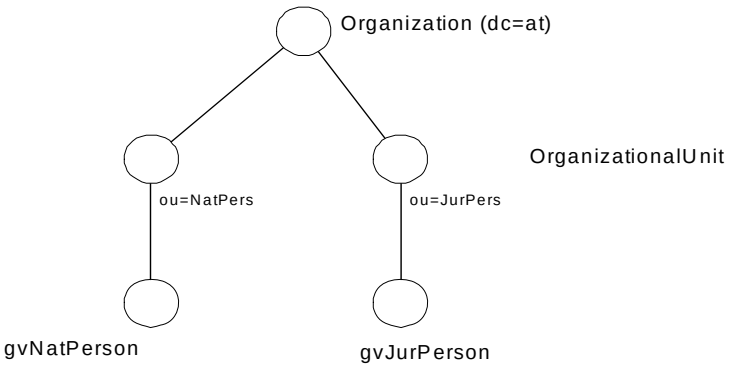
In the context of the electronic delivery, a directory is used for the purposes of information distribution. The directory provides the sending authority with information on the recipient. A person may be registered with several delivery agents.

The specification of the individual elements of the LDAP directory model (see note 2) is based on the Standard Lightweight Directory Access Protocol (v3).

Each delivery agent keeps a directory. All directories are connected online to a central service (delivery centre), which provides the information requested by the sending public authorities. However, the central service merely refers the authority to the specific directory with which the recipient is registered. The central service itself does not have information on recipients at its disposal.

Where a request is made, the central directory service provides information on the relevant delivery agent, associated encryption certificates and any absence of the recipient. In the case of natural persons, requests can be made in a variety of forms (request with delivery on the basis of the ssPIN, delivery on the basis of the name, name and address for notification). Replies to requests can also take a variety of forms (hit, no hit, minimum information, optional supplementary data). In the case of legal persons, the request can be made using the sourcePIN or the name and address of the person. Replies are given in the same forms as for natural persons.

Objects are represented according to their classification in the Directory Information Tree (see diagram).



Source: M. Liehmann, Electronic Service of Documents, LDAP Schema description, 2004

The object category 'natural persons' defines the personal data. The attributes of legal persons are described in the category 'legal persons'. Further categories are 'request-authorized sender' and 'geographical information'.

A.2.2 French system

Since May 2005, a French system is a offering service in France and in some DOM / TOM (i.e. La Réunion, Guadeloupe and Martinique). The French system is the single REM service provider for both senders and recipients.

The French System is a hybrid system where data is posted electronically and converted into paper before it is delivered to a postal address.

Senders need to register but are NOT authenticated. The service will be provided as soon as the sender pays.

Recipients do not need to register and only need to have a postal address.

Two **attestations** are defined to mimic existing surface mail services:

1) proof of electronic deposit without reception notice (preuve de dépôt électronique sans avis de réception): signed attestation that allows to attest that some data was deposited in electronic form in order to be converted into paper and delivered to the postal address of a recipient.

2) proof of electronic deposit with reception notice (preuve de dépôt électronique avec avis de réception): signed attestation that allows to attest that some data was deposited in electronic form in order to be converted into paper and delivered to the postal address of a recipient against the signature of a paper-based reception notice.

For the second attestation, the paper-based notice of reception is returned back to the postal address of the sender.

Both attestations allow having a secure link with the content of the message that is always converted into a pdf file before being printed on paper. The sender either provides the pdf file or the conversion is done by La Poste. In the latter case, the sender is invited to verify the result of the conversion and to approve it.

Attestations are accessible on-line during **three years** by connecting to the REM service provider and may be downloaded at any time. The format of the attestation (*.prv) is proprietary.

Downloaded attestations may be verified at any time by anybody using an on-line connection to the REM service provider.

For every transaction, La Poste maintains an archive during **one year** that consists of:

- the data that has been sent (*.pdf);
- the electronic attestation (*.prv);
- a printable form of the electronic attestation (*.pdf).

Senders must use Acrobat Reader and a web browser and MUST have an e-mail address in order to get their attestations back by e-mail.

A.2.3 French enterprise system

A further French system is offered for enterprises only. The French enterprise system is not necessarily the single REM service provider for both senders and recipients. Partnerships exist with Canada Post and with the United States Postal Service.

An enterprise account manager needs to register and to authenticate.

Senders are managed by the enterprise account manager and obtain an ID / password. At the minimum, senders need to use a web client and have access to the Internet in order to connect to the web site (i.e. https://fr.postecs.com). They may also use an email client and a plug-in provided by the French enterprise system.

Recipients need to have an e-mail address with a mail system connected to the Internet and supporting SMTP.

Recipients receive an e-mail notification in their regular e-mail box that includes a unique URL link for message retrieval. If the sender has chosen the option 'password protection', then they are two cases:

- the recipient must use a password chosen by the sender; or
- if the recipient is also a user of the French enterprise system, then the user must use the ID/ Password of his account.

Senders may only follow the delivery process by connecting and authenticating to the REM service provider. The real time follow-up allows senders to know for each recipient:

- when a message has been sent;
- the e-mail address of the recipient and the sending options;
- when the recipient has been invited to retrieve the message;
- when the recipient has connected to the French enterprise system web site to retrieve the message;
- when the recipient has read the main body of the message;
- when the recipient has downloaded the attachments of the message.

The time during which the follow up is maintained is not mentioned.

The messages stored on the web server are automatically destroyed at latest after 11 days, or sooner if the sender wishes so. Messages must be less then 50 Mbytes.

A.2.4 Spain - UPM-ACEPTA

UPM-ACEPTA is a REM service developed by the Cryptography laboratory from the Computer Science School of UPM (Universidad Politécnica de Madrid).

The whole architecture identifies four main entities types:

1) Sender. The service user that wants to send a so-called digital object. This object will travel encrypted and signed.

2) Recipient. The service user that receives the encrypted and signed message from the sender.

3) The so-called Delivery Agent (actually REM provider), that generates the different types of evidences and interacts with both sender an recipient in different stages of the message submission-delivery-opening process.

4) Security services provider. This includes Certification Service Providers, as both evidences and messages are signed and signatures are supported by X.509v3 certificates; and Time Stamp Authorities as evidences are also time-stamped.

When a sender wants to send information to a certain recipient, the sender first builds a so-called digital object, which has a certain structure already defined by the ACEPTA protocol itself, encapsulating the information to be transferred. This object includes a time indication taken from the local clock from sender's computer and a digital signature by the sender. The contents of the object are encrypted with two randomly selected keys k1 and k2 that actually form the final encryption key. The sender includes one half of the key (let us assume k1) in a message and submits the signed and encrypted digital plus k1 to the recipient. This submission may be performed using any suitable transport mechanism: regular e-mail, ftp, http, or even physical delivery of the electronic document.

The sender may submit (before or after actual submission of the digital object to the recipient) a request (Nota de Envío, in ACEPTA's terminology) to the so-called Delivery Agent (REM services provider, in fact) including, among others, details on the recipient, the other half of the encryption key (k2), and a list of value pairs (HMAC-corresponding key) that the recipient will have to generate afterwards. The REM provider will then produce an evidence of submission (Nota de Envío Extendida in ACEPTA's terminology) that will include a time-stamp generated by the TSA and a digital signature by the REM provider itself, which will be delivered to the sender. It also generates an identifier for this request/message. The REM provider then waits for the request of the recipient.

When the digital object and the k1 half encryption key arrives to the recipient, she must request the k2 half encryption key to the REM provider. But for being given such a key, the recipient has to prove to be in possession of the digital object generating the list of HMAC values with the keys that the REM provider will send her. Once the recipient has proved to be in possession of the digital object, the REM provider delivers the k2 half encryption key and produces an evidence of delivery, which includes a time-stamp and the electronic signature of the REM provider (Nota de Entrega Extendida, in ACEPTA's terminology) and delivers it to the recipient. The recipient may then open the digital object sent by the sender.

Both, sender and recipient are authenticated by the REM provider through their respective electronic signatures on the requests addressed to it.

Evidences are XML documents incorporating enveloped XMLSig signatures.

Users are required to register themselves through a face to face process that includes presentation of documents supporting identity. Nevertheless, they are not required to sign any contract with the provider.

More information on this system (in Spanish) in: http://dirdam.ls.fi.upm.es/about.html.

A.2.5 Spain - MAP, AND FNMT-RCM

Survey in Spain has identified a number of additional implementations other than the one by UPM-ACEPTA. Two closely related are those reported by Ministry of Public Administrations (MAP), the one by the Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM -a public corporation under the umbrella of the Ministre of Economy and Finance). In fact FNMT-RCM has developed a product that offers as service to its own clients (it provides certification and other security services), but also sells to other organizations. MAP, in close co-operation with the Spanish Post (Correos), has deployed a service based on this product open to all Spanish citizens: secure notifications from Public Administration to citizens, based on the possession of a qualified certificate and an unique mailbox.

Any citizen may subscribe to this service and get a unique address with an associated mailbox. Citizens may then subscribe to certain processes from different public agencies. Once the subscription is completed, any notification generated by one of the aforementioned agencies within the context of one of the processes selected, will be sent to the generated mailbox for that citizen.

Registration in the service provided by FNMT requires face to face presence with identity supporting documentation or remote authentication through previous identity check. Both individual and organizational users are required to sign a contract or agree some other form of undertaking. Registration in MAP service may be done remotely if the client is in possession of a qualified certificate acknowledged by MAP.

The analysis of the fulfilled questionnaires returned by both entities reveals that both organizations claim to follow to a certain extent the model depicted by the STF-318 in the questionnaire with light alterations: FNMT-CRM reports only a single REM provider, no need for external security services (this corporation actually is a security service provider); MAP reports need of separated security services providers.

Both services providers require peer entities authentication in all the dialogues established during service provision. Both of them also report provision of all the evidences identified in the questionnaire (including evidence of message origin authentication), except non-delivery within a predefined time-limit, which in MAP may be offered upon request of the sender, whereas it is not offered by FNMT service.

Both services provide evidences based on electronic signatures (mainly qualified, although some of them are also reported to be supported by Advanced Electronic Signatures) and time-stamps. But while FNMT-CRM uses S/MIME and CMS signatures, MAP plans to also use XMLSig, XAdES and CAdES.

FNMT: evidences carry references to messages: message identifier. Signatures CMS SMIME, RFC 3161 time-stamps. Need for registering. Identification at registration time. Face to face presence with identity supporting documentation or remote authentication through previous identity check. Signature of contract or agree to some other form of undertaking as individuals. Organizational users are required to sign a contract or agree some other form of undertaking.

MAP: CMS, XMLSig, CAdES, XAdES. Subscription details are unspecified at this stage of the development.

A.2.6 Spain - Bankinter

Bankinter is a major Spanish bank with has now presence in several European countries. It has put in place a REM system for inner messaging exchanges, which is outsourced to an independent hosting service.

The evidences supplied by the service are all the evidences identified in the questionnaire except the evidence that the message has been transmitted through a REM service provider. They are verifiable by REM users and any party trusting the CAs used for signing registered e-mail.

Security services provided include: malware absence verification and encryption of messages. Other services include forwarding messages to physical post in case of failure if requested by the sender, sender and recipient messages archival for 5 years, storage of messages containing malicious code for 1 month, storage of logs with information on messages (Date/time, To/From) for 6 years, maintenance of signature on archived data, and directory services.

The system returns to the sender and sender's REM provider the following evidences: evidence of notification of availability to the recipient; evidence of delivery/download; evidence of non delivery, evidence of non delivery within a pre-defined time limit, and evidence that the message has been opened by the recipient.

Bankinter reports adherence at the model shown in the questionnaire, including external security service providers and gateway for regular post mail. Qualified and advanced electronic signature and time-stamps are used for generating evidences; peer-entity authentication use one-time password and cryptographic device; the 'from' field is updated to identify the service provider on behalf of the sender.

No further details are provided (this includes registration process, formats of electronic signatures and time-stamps, security services used, services used, etc.).

A.2.7 Spain - CCN

The Centro Criptológico Nacional (National Cryptologic Centre -CCN) is the organism in charge of co-ordinating the activities of other organisms within the Spanish Public Administration that make use of cryptographic means and procedures. It is also in charge of guaranteeing the IT security, report on the co-ordinated acquisition of cryptographic material and educate Public Administration staff specialized in this area. The CCN is, in consequence, a major player in Spanish Public Administration, and its plans regarding REM systems are of great importance.

The CCN reports to be planning the deployment of a Registered Email service in 2007 for Public Administration. The system is conceived for provision of REM services to organizations in support of official communication between and with **Spanish** Public Administrations. Official messaging takes place between organizations and is not associated with persons. In Spain, official messaging services belong to the category of postal information. In the case of the Ministry of Defence, these must be complied with.

The evidences provided by such a service for official messages will have full and general legal validity through the specific statute that the official messaging has.

The CCN reports that the service being developed matches the model shown in the questionnaire (including the presence of more than one REM provider) with two main remarks: there is not gateways to external regular email or post mail. Nevertheless, if the senders requests it or if the electronic submission fails and the server requests it, the service will forward the message to physical post, and there is not envisaged external security service providers.

No details are provided with regards to registration process, except that it is already decided that users will not need to sign a contract when registering.

The CCN service plans to support the following evidences: evidence of message origin authentication, evidence of submission, evidence of delivery/download, and evidence of non-delivery within a pre-defined time.

These evidences will be verifiable only by REM registered users. It is worth to mention the constraint of 10 MB for the overall message (body + attachments) size.

As for other additional services, the system will include: verification of malware absence, management classification/priority levels, archival of sender's and recipient's messages for 1-2 years depending of the classification level, storage of messages containing malicious code in quarantine, storage of logs with information on messages for 1-2 years, including information on submission, delivery, reading, maintenance of signatures on archived data, and directory services for assisting senders in obtaining recipients' addresses.

The evidences generated will incorporate qualified electronic signatures and time-stamps. No further details are given concerning the specific signatures and time-stamps formats.

A.2.8 Switzerland - IncaMail from SwissPost

'IncaMail' is a service from SwissPost available in Switzerland.

SwissPost is the single REM service provider for both senders and recipients.

Senders need to register and MUST use a public key certificate agreed by SwissPost.

Recipients need to register and MUST use a public key certificate agreed by SwissPost.

These certificates must be useable both for authentication and decryption.

A stand-alone free-of-charge Java application may be used, as well as free-of-charge APIs ready to be incorporated into applications.

The software uses a double-envelope technique (OSCI standard - Online-Services Computer Interface) where the RSA public key placed in the recipient's certificate is used to encrypt the payload of the message. This prevents SwissPost from seeing the payload.

IncaMail

How it works

Messages written by the sender are encrypted, signed, sent and placed in the recipient's mailbox on the IncaMail platform. The electronic message is thus ready to be picked up by the recipient. On request, the recipient receives an email that a message is available for pickup. During the receiving period (generally 7 days), the recipient has the opportunity to pick up the message. The recipient signs on pickup, and a digitally signed postal receipt is issued. Either

the recipient or the sender can download it. The message remains encrypted throughout the entire transmission and while on the platform and thus cannot be viewed by others.

Table 27

An overview of IncaMail services
> Secure transport (end-to-end encryption)
> Proof of dispatch and pickup
> Digitally signed Post receipt for sender and receiver
> Status report on the progress of the message
> Identification of sender and recipient
> Securing the integrity of the message

IncaMail Public

With IncaMail Public you can send electronic data via IncaMail to IncaMail members and non-IncaMail members. The recipient receives an e-mail with a link for picking up the message. This kind of delivery is faster, more secure and more economical than delivery by physical means. Furthermore, you receive a dispatch confirmation

Mode of operation

Messages dispatched by the sender are made available for pickup on the IncaMail platform. The recipient subsequently receives an e-mail with a link for picking up the message. During the pickup period (the standard is 7 days), the recipient has the opportunity to read the message by clicking on the link. Pickup takes place via a secure Internet connection. The IncaMail platform records the entire process and a digitally signed post receipt is provided to the sender and recipient. During the entire transmission and on the platform, the message remains encrypted and thus cannot be read by third parties.

Table 28

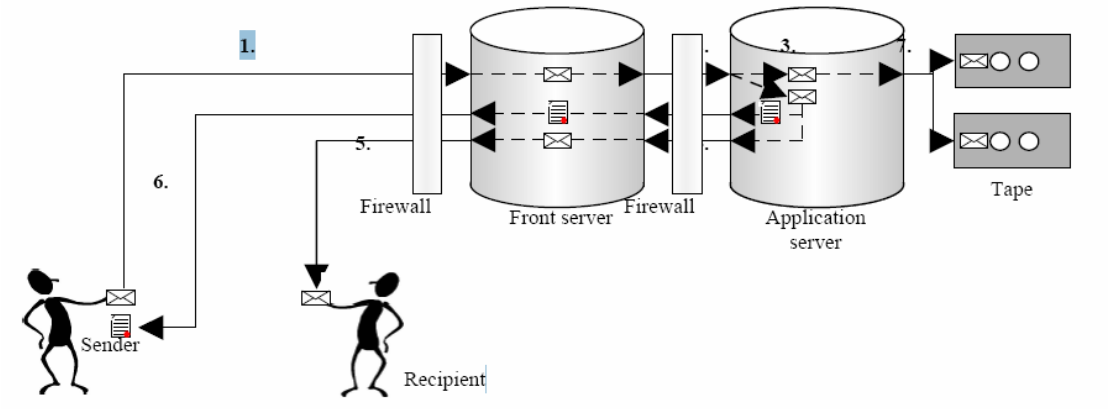
Summary of the IncaMail public services
> Secure transport
> Proof of dispatch and pickup date
> Digitally signed Post receipt
> Status report on the progress of the message
> Identification of sender
> Delivery also to non-IncaMail members

A.2.9 Norway - eNotarius

eNotarius is a service for securing email by passing the email through a trusted server. eNotarius offer a plug in for a range of email clients to facilitate the routing of messages through the trusted server. Emails are stored by eNotarius and verified online by later retrieving the email from the trusted server. Emails are optionally signed / encrypted by the sender. Emails are time-stamped by the REM provider. Confirmation of receipt is provided when the email is received by the recipients email server. Read receipt is provided by the recipient receiving the email via a web link for on-line retrieval of the email content. Recipients do not need to be registered with eNotarius to receive registered emails.

The procedure for handling a signature is as follows:

1. The e-mail is sent through a plug-in to via@enotarius.com rather than to the original recipient address. The e-mail is received by eNotarius' front server.
2. The e-mail is copied from the front server to the application server and then deleted from the front server.
3. On the application server, the e-mail is marked with the time and date and logged. Then a receipt is generated for the sender based on the sender, recipient, title, time and date - in such a way that the reference number is generated and added to the receipt.
4. The e-mail is sent from the application server to the front server with the original recipient address.
5. The front server sends the e-mail to the original recipient and verifies that the e-mail has been received by the recipient's e-mail server. The copy on the front server is then deleted, while the copy on the application server is retained.
6. The receipt with the two time verification stamps and the recipient's domains/IP are returned to the sender.
7. The copy of the e-mail on the application server will be copied on a regular basis and saved on back-up tape.



A.2.10 Worldwide - PxMail

PxMail is a system supplied by PostX for the worldwide market.

PxMail comprises two core elements: the customer-controlled encryption engine and the PxMail.com hosted service.

The first core element is the customer-hosted aspect of PxMail, called the PostX Envelope Server. The Envelope Server performs the policy enforcement, encryption, and secure delivery of the messages, using keys supplied by the keyserver at PxMail.com. The PostX Envelope Server comprises the PostX Registered Envelope and the Envelope Builder. The operation of the envelope server is transparent to desktop users. All of the encryption and secure delivery of the message traffic occurs centrally in the protected customer's network at the outbound mail gateway. The enveloped includes an advanced electronic signature. The signature is included in the PostX Envelope along with the cross-platform verification code and the message payload. Envelope construction can also be done via the online SecureCompose form that is protected via cert-based SSL auth.

The second core element of the solution is the online PostX Managed Service, called PxMail.com. PxMail.com provides the management and hosting of keys, enrolment, and auditing. This service also has two major components, the Key Server and the Web Administration. These hosted components provide user enrolment, key management, administration, and many other features. When a message is opened, the PxMail.com keyserver handles authentication and provides the decryption key to the end user. The managed service supports Read Receipts / Unread Notifications as well as secure reply and web based message composition.

With the PostX Envelope, the actual encrypted message is delivered via SMTP as a MIME attachment. The MIME attachment is a standard HTML file. The HTML contains both the encrypted content and the code required to decrypt it (JavaScript). It does not require a special email client, specially installed software, or a particular operating system. If the recipient is unable to run JavaScript or the JavaScript is somehow disabled. PostX also has optional email client plug-ins that can detect and natively decrypt/encrypt PostX Envelopes within the user's email client.

The PxMail.com service of the PxMail solution **never** hosts, views, or archives emails. Rather, the email originating inside the customer's network is encrypted before it goes outside the customer's firewall, and is directly delivered securely to the recipient(s). The system uses strong symmetric key cryptography and standardized security practices to ensure privacy and confidentiality. Due to these facts, the PxMail system is resistant to harmful attacks that would compromise the integrity or security of the customer's email.

A.2.11 Worldwide - Critical Path (CP)

Critical Path, in addition to a 'CNIPA' model compliant service not addressed here (see note), provides a standards based solution that can be implemented by installing a number of products. The following text refers to a full fledged installation that makes use of all the relevant products.

NOTE: The CNIPA model solution is not addressed here, since it would be a useless duplication of the CNIPA model description provided in section: "8.33 Italian REM service (a.ka.a "CNIPA" model)" in the present document.

The original Critical Path service, non CNIPA compliant, is based on a centralized mail service that may be implemented also in a UPU compliant way that requires only senders to be registered. Non registered users can access their e-mail via webmail. Registered recipients can enjoy additional services (e.g. they can make use of providers' managed directories, calendar, virtual disk and other messaging services, etc.). It is currently planned that registered users may receive the entire message, instead of the message notification, based on the service implementation.

Although it does not natively provide for forwarding the e-mails to physical post, where the latter implements a suitable interface, it can also forward e-mail to be printed and delivered as a usual paper mail. Depending on the products installed, it can interface other messaging systems, like Mobile, IM, voip etc. It can interface with other, usual e-mail based, non registered users. Namely a REM service can send to non-REM users a notification that a message is pending for them at the service's site and that it can be downloaded from a given URL. A non-REM user can send a non-REM message to a REM user on the usual internet email-box associated with REM.

REM system logs can be configured to contain any of the basic e-mail related information: sender, recipients, subject, attachments list, time marks (sending time, receiving notification time, download time, etc.), operation results and error reasons among which malware presence.

It assists senders in retrieving the recipients' e-mail address as well as their encryption certificates, where applicable within the registered users' community.

Senders can sign the sent messages with a QES or an AdES and can also encrypt it for registered users. Authentication can be configured according to the implementing service needs. For signing/encryption of messages, in client/server systems, a plug in is required to be specifically developed. Whereas, using webmail is actually possible: it is service/implementation dependent using a Browser plug-in.

The following evidences signed by the REM service with a QES or an AdES, depending on the installation configuration, can be produced and delivered to the sender, depending on a bespoke configuration:

1) message origin authentication;
2) submission;
3) that message has been transmitted through a REM service provider;
4) notification to the recipient of a message availability to be delivered /downloaded (always implemented);
5) delivery/download;
6) acceptance or rejection of message by the recipient;
7) non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.);
8) non delivery/download within a predefined time limit;
9) an email has been 'opened' or 'viewed' by recipient;
10) notifications of errors.

Evidences produced can be configured by combining any or all of the following: Message identifier, Message hash, Message copy including attachments, Message body + hash of attachments. They can be verified by any user trusting the REM server's certificate issuing CA.

Where required, the Service provider can add an additional identifier that does not replace the original one.

In addition to the time marking produced by the time included in the evidences, that can be based on NTP, radio or other cards for time marks and the reliability of which depends on the provider's trustworthiness, TSTs can be added to the signatures where required by the installation.

All auxiliary services can be either internally developed or outsourced: Signature provider, Signature verifier (entire certified Path), Encryption service provider, Decryption service provider, Time stamping provider, Long term archival service provider.

Any mail clients, as well as webmail, can be used with or without plug-ins.

Annex B:
Survey Questionnaire

Registered E-Mail (REM)
Information Gathering Questionnaire

We would welcome your responses to the following questions in the context of Registered E Mail. The responses will be used as the basis for the development of the ETSI specifications and so will be very valuable in ensuring that our work matches existing and likely future market requirements, encompassing existing solutions and future trends.

You may skip over any sections which you feel are not relevant or for which you do not have a specific answer. Also, instead of answering the questions in section 5 respondents may provide their own system description providing information on the system architecture and how the registered e-mail services identified are provided.

If you can answer these questions from two or more perspectives (for example: the requirements of the regulations, the provisions of one or more specific current or future implementation of those regulations) feel free to answer more copies of the questionnaire, again skipping over irrelevant sections.

Unless specified otherwise please tick all check boxes that apply. Please use continuation tables at the end of this form should the space provided be insufficient for giving a full response to any of the questions

B.1 Information about your organisation

B.1.1 What is the name of the organisation that you represent?	
B.1.2 What is the country or regional area your organisation covers in relation to Registered E Mail?	
B.1.3 What is the type of the organisation? (select all that apply)	
1. *Service provider* *Please specify what type of service provider* i. *Registered Email (Registered EMail) service Provider* ii. *Provider of services that may be used in REM* I. *PKI services provider* II. *Time Stamping Authority*	

III. *Delegate Path Validation Service (Note 1)* IV. *Long term storage services* V. *Notarisation services (Note 2)* VI. *Other(s), please specify*	
2. *System / SW provider*	
3. *User; please specify your type / business area:* I. *Single user* II. *Bank / Financial institution* III. *Insurance* IV. *Public administration* V. *Other(s), please specify*	
4. *Regulatory body*	
5. *Standardisation body*	
6. *Other(s), please specify:*	

Notes:

1) Delegated path validation: A service checking the validity of set of public key certificates providing a certification path from a trusted CA (e.g. see RFC 3379).

2) Notarisation service: service providing a trusted attestation of a certain event (e.g.: verification of a signature as valid, deposit of a binary object, delivery or withdrawal of a binary object, etc.)

B.1.4 Any other relevant details about your organisation:

Organisations URL:

B.2 Status of Implementation

B.2.1 Does information given in this questionnaire relate to a specific Registered E-Mail service implementation?	*Yes:*
B.2.2 If you ticked 'yes' in section to 2.1 what is the status of this service 1. *Already deployed and in operation* 2. *Is currently being implemented* 3. *Planned or envisaged*	
B.2.3 If you ticked 'yes' in section 2.1 give information on the service deployment 1. *If not deployed when to be deployed* 2. *Current size of user community* 3. *Planned size of user community*	*Mth: Yr:*
B.2.4 Does information given in this questionnaire relate to a specific product for Registered Email?	*Yes*:
B.2.5 If you ticked 'yes' in section 2.4 what is the status of this product 1. *Already in the market* 2. *Is currently being implemented* 3. *Planned or envisaged*	

B.2.6 If you ticked 'yes' in section 2.4: 1. *What is market sector being addressed* 2. *What is the expected size of installations*	
B.2.7 Does information given in this questionnaire relate to a regulation or standard?	*Regulation*: *Standard*:
B.2.8 If you ticked in section 2.7 give information about the status of the regulation / standard: 1. *Is this already implemented and deployed* 2. *Implementations being developed* 3. *Implementations being developed or trialled* 4. *Yet to be implemented*	
B.2.9 If you ticked in section to 2.7: 1. *What is the market sector being addressed?* 2. *What is the expected maximum size of installations?*	
B.2.10 Please provide any other information relevant to implementation.	

B.3 Services

This section aims to identify the services provided / considered necessary for Registered E Mail.

B.3.1 What evidence related services are:

- *supported or considered necessary.*
- *not supported and not considered necessary*

*Note: Evidence services marked with * include evidence of the time of the given event*

Evidence service	*Supported necessary*	*Not supported / not necessary*
1. *Evidence of message origin authentication Note: Includes integrity of message and authentication of the identity of the message originator.*		
2. *Evidence of submission* Note: Evidence of submission passed back to sender.*		
3. *Evidence that message has been transmitted through a REM service provider* Note: Evidence passed to recipient after passing through REM provider.*		
4. *Evidence that message has been successfully exchanged between two REM service providers**		
5. *Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded**		
6. *Evidence of delivery/download**		
7. *Evidence of acceptance or rejection of message by the recipient**		
8. *Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)**		

9. *Evidence of non delivery/download within a predefined time limit* *If applicable please specify if this time limit is:* I. *Pre-defined* II. *Defined by the sender*		
10. *Evidence that an email has been 'opened' or 'viewed' by recipient**		
11. *Other(s), please specify*		

B.3.2 What other security related services are:

- *supported or considered necessary.*
- *not supported and not considered necessary*

Security service	*Supported necessary*	*Not supported / not necessary*
1. *Malware absence verification*		
2. *E-Mail content protected when passing through REM provider(s) (e.g. by encryption) to ensure that message is not revealed to parties other than the recipient(s)*		
3. *Not revealed to recipient until e-mail accepted*		
4. *Other(s), please specify*		

B.3.3 Please identify any restrictions on the Registered E-Mail services

Restriction on (if any)	*Value*
1. *Overall Size of message: body + attachments*	
2. *Size of message body*	
3. *Size of individual attachments*	
4. *Number of attachments*	
5. *Type of attachments*	
6. *Other(s), please specify*	

B.3.4 What, if any, services relating to surface mail or external (non registered) e-mail services are:

- *supported or considered necessary.*
- *not supported and not considered necessary?*

If no surface mail and no interface to external e-mail is supported skip this question.

Service	*Supported necessary*	*Not supported / not necessary*
1. *Always forward to physical post in case of failure of registered email*		
2. *Forward to physical post in case of failure of registered e-mail if requested by the sender*		
3. *Forward to physical post instead of electronic post where addressed as such by the sender*		
4. *Forward e-mail to other non Registered E-Mail network where addressed as such by the sender*		

5. *Forward e-mail received from external e-mail network (e.g. Internet) to Registered E-Mail recipient.*		
6. *Other(s), please specify*		

B.3.5 What other services are:

- *supported or considered necessary.*
- *not supported and not considered necessary.*

Service	*Supported necessary*	*Not supported / not necessary*
1. *Sender Message Archival - i.e. Long term storage of all messages after being submitted by the sender and notifications, regardless of whether it has been delivered to / retrieved by the recipient (State retention period) (If not all messages or notifications are archived, or there is a variation in the retention period for different classes of messages please provide details*		
2. *. Recipient Message Archival - i.e. Long term storage of all messages and notifications made available for download / retrieval even after being retrieved by the recipient or removed from an online message store (State retention period) (If not all messages or notifications are archived, or there is a variation in the retention period for different classes of messages please provide details)*		
3. *Storage of messages containing malicious code in quarantine area for future reference (State retention period)*		
4. *Storage of logs containing information about messages (State retention period) (Describe in general terms information collected)*		

5. *Maintenance of signatures on archived data to ensure sufficient data is available to verify signature over long term.* *Note: See section 6 of CWA 15579 for example of measures that may be taken.*		
6. *: Directory services to* i. *assist senders in obtaining recipients email addresses* ii. *assist senders / recipients in obtaining certificates required to secure messages* iii. *Other(s), please specify*		
7. *Other(s), please specify*		

B.3.6 What type of users are supported

1. *Individuals*	
2. *Organisations*	
3. *Other(s), please specify*	

B.3.7 What business areas are directly supported / envisaged as possible, or, specifically not supported

Business area	*Supported Envisaged*	*Not supported*
1. *E-purchasing*		
2. *E-tendering*		
3. *E-accounting*		
4. *Official communication between and with public administrations*		

5. *General purpose transmission of messages and/or files Personal mail*		
6. *Other(s), please specify Other Please specify:*		

B.3.8 Please provide any further relevant information regarding the services provided.

B.4 Regulations and Legal Validity

B.4.1 Please specify known regulations which identify requirements or assign special legal validity to Registered Email and describe the scope of the regulation.

1. *Reference:*
   URL (e.g. HTTP//…) or other address for on-line version
   Description:
   Scope (Europe, name country or other region, user community)

2. *Reference:*
   URL or other address for on-line version:
   Description:
   Scope (Europe, name country or other region, user community)

3. *Reference::*
   URL or other address for on-line version
   Description:
   Scope (Europe, name country or other region, user community)

(Please use continuation tables to provide further references)

B.4.2 Please specify legally recognised evidential value that applies to the evidence provided by the security services described in 3.1.

Where applicable to specific evidential service please identify reference (a, b, …) from 3.1 above. (or specify all).

Where known, identify reference number (a, b, c, …) of relevant regulation from 4.1 above.

Evidential value	*Applicable*	*Services*	*Regulation*
1. *has full and general legal validity through specific statute* *Note: For example, an e-mail implemented in abidance of specific legislative rules has legal validity towards any use governed by those rules, without the need neither of any additional supportive agreement by the originally involved parties, nor of any subsequent endorsement by other parties.*			
2. *has legal validity based on explicit preliminary acceptance or explicit agreement by the parties (i.e. the rules set is already defined, users can just accept them)*			
3. *has legal admissibility as a trial evidence, but no 'per se' legal validity,* *Note: c.f. evidential value of electronic signatures other than Qualified Electronic Signature as defined in article 5.2 of the Electronic Signatures Directive 1999/93/EC*			
4. *Other(s), please specify*			

B.4.3 Is the evidence verifiable by:	
1. *Only registered REM users*	
2. *Any party trusting the Certification Authority(ies) used for signing Registered E-Mail*	
3. *Other(s), please specify*	

B.5 Service Provision Model

NOTE: If you prefer, you can provide us (ETSI STF 318) with your own documentation giving detailed information on how the services are provided, and then we can work with you on how to relate this to the questions in this section.

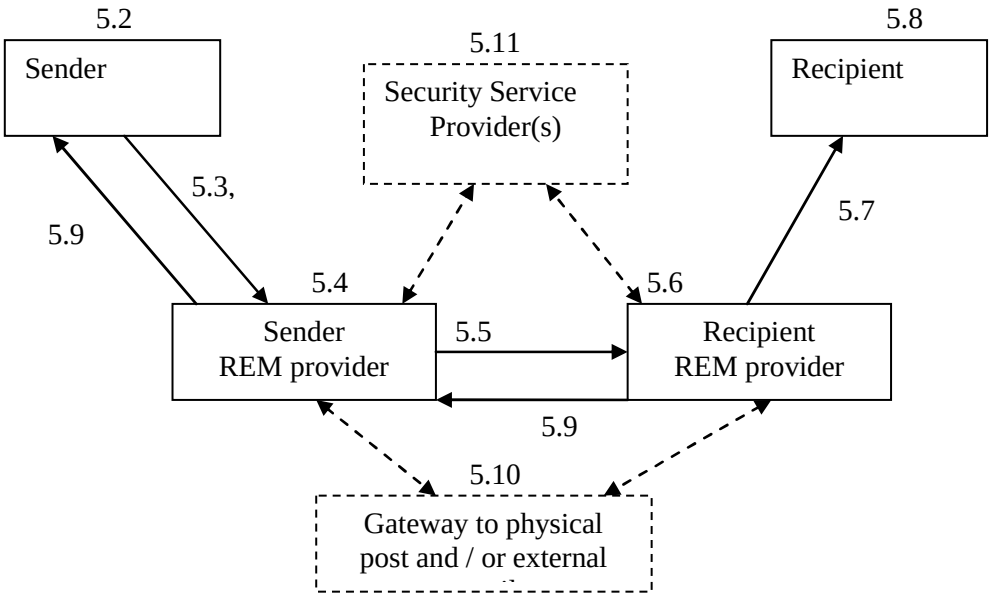
The aim of the following questions is to solicit information about the high level model of the Registered E-Mail system and how the evidential services identified above are provided.

If a system description already exists, or if it would be easier to use your own terms, please provide a description of the high level architecture and how the services listed above are provided in a separate document or in the continuation tables at the end of this questionnaire.

If you have provided your own description of the service provision model please check this box ☐

and, where not included in the continuation tables, give the reference a title of the documentation provided.

The questions in this section are based upon the following model.



NOTE 1: External e-mail means e-mail services which do not provide Registered E-Mail services directly to the sender or the recipient. This may be either conventional e-mail, or conventional physical postal services (registered or otherwise).

NOTE 2: Sender and recipient includes associated software and hardware on sender's / recipients system.

Continuous (i.e. not dashed) lines identify elements of what is henceforth referred to as 'basic model'.

The numbers appearing in the figure above identify subsections of the present section. Each subsection contains questions on specific elements of the model. Subsection 5.1 contains questions regarding the model as a whole.

B.5.1 Model Used

B.5.1.1 Indicate below the applicability of this model to the REM service.	
1. *Basic model described is applicable (excluding model elements gateway and security service providers)*	
2. *REM provider is a single entity supporting Registered E-Mail services for both senders and recipients in its domain (if so skip 5.5 below)*	
3. *Security service provider(s) are separate entity (ies) in your model.*	
4. *Is gateway to external email or physical delivery supported*	
5. *Additional service provision entities identified (if so list entities below and describe services & mechanisms and dialogue for additional entities in continuation tables at the end of this questionnaire)*	
Please list entities below and describe the services and mechanisms supported by those entities in the continuation table (section 10)	
6. *Model not applicable*	
B.5.1.2 Is Registered E-Mail service outsourced to an independent hosting service.	

B.5.2 Sender Services and Mechanisms

B.5.2.1 Check all the services and mechanisms employed by the sender	
1. *Evidence of message origin authentication* *Note: May also be provided by sender Registered E-Mail provider based on peer entity authentication.*	
Mechanisms supporting this service:	
i. *Advanced electronic signature*	
ii. *Qualified electronic signature*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Other mechanism(s) and / or trusted services, please specify*	
2. *Other service(s), please specify*	
Mechanism(s) supporting the service: *Please describe mechanisms used to support the service(s)*	

B.5.3 Sender - Sender REM Provider Dialogue

B.5.3.1 Peer Entity Authentication Is client authenticated to REM Provider	
If so what mechanism(s) is (are) employed	
1. *Simple Password*	
2. *One time password*	
3. *Cryptographic device (e.g. smart card, USB token)*	

4. *Password over SSL / TLS*	
5. *Software key*	
6. *SAML Assertion*	
7. *Other(s), please specify*	
Please specify any restrictions on authentication passwords, keys etc (e.g. size of password)	

B.5.3.2 Service controls: Are the following services always provided by Sender REM provider, provided only upon sender request or never provided by Sender REM provider?

	Always	*Upon request*	*Never*
1. *Evidence of message origin authentication*			
2. *Evidence of submission*			
3. *Evidence that message has been transmitted through a REM service provider*			
4. *Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded*			
5. *Evidence of delivery/download*			
6. *Evidence of acceptance or rejection of message by the recipient*			
7. *Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)*			
8. *Evidence of non delivery/download within a*			

predefined time limit			
9. *Evidence that an email has been 'opened' or 'viewed' by recipient*			
10. *Notifications of errors)*			
11. *Other(s), please specify*			
B.5.3.3 Message identifier			
1. *Is there a unique identifier allocated by Sender? Please describe*			
2. *Is there a unique identifier allocated by Sender REM provider Please describe*			
3. *Other information about message identifier*			
B.5.3.4 Please provide other information relevant to this dialogue			

B.5.4 Sender REM Provider Services and Mechanisms

NOTE: The REM provider may call upon third party Security Service Provider(s) to support the provision of certain mechanisms.

B.5.4.1 Check all the services and mechanisms employed by the sender REM provider	
1. *Evidence of message origin authentication Note: It is expected that this is provided using peer authentication provided by the sender provider dialogue.*	
Mechanisms supporting this service:	
i. *Advanced electronic signature applied by REM provider on behalf of sender*	

ii. *Qualified electronic signature applied by REM provider on behalf of sender*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Other mechanism(s) and / or trusted services, please specify*	
2. *Evidence of submission (returned to sender)*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Other mechanism(s), please specify*	
3. *Evidence of transmission (forwarded with message to recipient)*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Is the From address updated to:* I. *Hide sender address*	

II. *Identify service provider on behalf of sender* III. *Other please specify:*	
4. *Checks on sender signature validity* i. *Is message rejected if fails* ii. *Is message rejected if signature not present* iii. *Is message rejected if signature not of form (e.g. qualified) expected*	
5. *Other service(s) and / or trusted services please specify*	
Mechanisms supporting this service: *Please describe mechanisms used to support this service*	

B.5.5 Sender REM provider - Recipient REM provider dialogue

NOTE: Skip this sub-section if sender and recipient REM provider is a single entity (i.e. are not separated)

B.5.5.1 Peer Entity Authentication Are Sender and recipient REM Provider authenticated to each other?	
If so what mechanism(s) is (are) employed	
1. *Cryptographic device(e.g. smart card, USB token)*	
2. *Password over SSL / TLS*	
3. *Software key*	
4. *SAML Assertion*	
5. *Other(s), please specify*	
Please specify any restrictions on authentication passwords, keys etc (e.g. size of password)	

B.5.5.2 Are the following services always provided by the recipient REM provider, provided only upon sender / sender REM provider request, never provided?

	Always	*Upon request*	*Never*
1. *Evidence that message has been successfully exchanged between two REM service providers*			
2. *Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded*			
3. *Evidence of delivery/download*			
4. *Evidence of acceptance or rejection of message by the recipient*			
5. *Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)*			
6. *Evidence of non delivery/download within a predefined time limit*			
7. *Evidence that an email has been 'opened' or 'viewed' by recipient*			
8. *Check for malicious code*			
9. *Notifications of errors (please provide details of errors that may be indicated)*			
10. *Other(s), please specify*			

B.5.5.3 Message identifier	
1. *Is there a unique identifier allocated by Sender REM Provider (or forwarded from Sender)?* *Please describe*	
2. *Is there a unique identifier allocated by Recipient REM provider* *Please describe*	
3. *Other information about message identifier*	
B.5.5.4 Please provider other information relevant to this dialogue	

B.5.6 Recipient REM Provider Services and Mechanisms

NOTE: The REM provider may call upon third party Security Service Provider(s) to support the provision of certain mechanisms.

B.5.6.1 Please check all the services and mechanisms employed by the recipient REM provider	
1. *Evidence that message has been successfully exchanged between two REM service providers*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Other mechanism(s) and / or trusted services, please specify*	
2. *Evidence of notification to recipient*	

Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-mark*	
iv. *Time-stamp*	
v. *Other mechanism(s) and / or trusted services, please specify*	
3. *Evidence of delivery/download*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-mark*	
iv. *Time-stamp*	
v. *Other mechanism(s) and / or trusted services, please specify*	
4. *Evidence of acceptance or rejection of message by the recipient*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-mark*	
iv. *Time-stamp*	

v. *Other mechanism(s) and / or trusted services, please specify*	
5. *Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-mark*	
iv. *Time-stamp*	
v. *Other mechanism(s) and / or trusted services, please specify*	
6. *Evidence of non delivery/download within a predefined time limit*	
Mechanisms supporting this service:	
i. *Advanced electronic signature of REM provider*	
ii. *Qualified electronic signature of REM provider*	
iii. *Time-mark*	
iv. *Time-stamp*	
v. *Other mechanism(s) and / or trusted services, please specify*	
7. *Checks on sender signature validity* i. *Is message rejected if fails* ii. *Is message rejected if signature not present* iii. *Is message rejected if signature not of form (e.g. qualified) expected*	

8. *Other service(s), please specify*	
Mechanisms supporting this service: *Please describe mechanisms used to support this service*	

B.5.7 Recipient REM Service Provider - Recipient Dialogue

B.5.7.1 Peer Entity Authentication Is client authenticated to REM Provider	
If so what mechanism(s) is (are) employed	
1. *Simple Password*	
2. *One time password*	
3. *Cryptographic device(e.g. smart card, USB token)*	
4. *Password over SSL / TLS*	
5. *Software key*	
6. *SAML Assertion*	
7. *Client Public key certificate*	
8. *Other(s), please specify*	
Please specify any restrictions on authentication passwords keys etc (e.g. size of password)	

B.5.7.2 Service controls: Are the following services always provided by the recipient service provider, provided only upon sender's request, never provided?

	Always	*Upon request*	*Never*

1. *Evidence that an e-mail has been 'opened' or 'viewed' by recipient*			
2. *Other(s), please specify*			
B.5.7.3 Please provider other information relevant to this dialogue			

B.5.8 Recipient Services and Mechanisms

B.5.8.1 Check all the services and mechanisms employed by the recipient	
1. *Evidence that an e-mail has been 'opened' or 'viewed' by recipient*	
Mechanisms supporting this service:	
i. *Advanced electronic signature*	
ii. *Qualified electronic signature*	
iii. *Time-stamp*	
iv. *Time-mark*	
v. *Other mechanism(s) and / or trusted services, please specify*	
2. *Other service(s), please specify*	
Mechanisms supporting this service: *Please describe mechanisms used to support this service*	

B.5.9 Final Notifications

B.5.9.1 Please identify notifications passed back to sender's REM provider, and to sender.		
	Returned to Sender REM provider	*Returned to Sender*
1. *Evidence of notification to the recipient of the availability of a stored message ready to be delivered /downloaded*		
2. *Evidence of delivery/download*		
3. *Evidence of acceptance or rejection of message by the recipient*		
4. *Evidence of non-delivery (e.g. for unknown recipient or recipient server, technical errors, etc.)*		
5. *Evidence of non delivery/download within a predefined time limit* *If applicable please specify if this time limit is:* I. *Pre-defined* II. *Defined by the sender*		
6. *Evidence that an email has been 'opened' or 'viewed' by recipient*		
7. *Notification of malicious code*		
8. *Notifications of errors (please provide details of errors that may be indicated)*		
9. *Other(s), please specify*		

B.5.10 Gateway

NOTE: This section may be skipped if the REM system does not support physical postal services or external e-mail services.

5.10.1 Does the REM support interfacing to non REM users?	
If so who can communicate with REM services providers:	
i. *Can a non REM message be accepted by a REM service provider to be delivered to a recipient registered with that REM provider?*	
ii. *Can a REM message be sent to recipients that are not known to the sender REM service provider as registered with any Recipient REM provider?*	
5.10.2 Does the REM support interfacing to physical postal services?	
5.10.3 If physical postal service is supported does this also provide registered mail services?. If yes, please provide further details of service provided:	Yes No
5.10.4 Please provide details of any evidence services and mechanisms (as above) provided by gateway	
5.10.5 Please provide other details regarding interfacing to external postal and e-mail services	

B.5.11 Security Service Provider

B.5.11.1 What independent security service provider elements are used?	
Security service provider	
1. *Signature provider*	
2. *Signature verifier (entire certif. Path)*	
3. *Encryption service provider*	
4. *Decryption service provider*	

5. *Time stamping provider*	
6. *Long term archival service provider*	
7. *Other(s), please specify*	

B.6 Technical Details

B.6.1 What clients are supported for sender / recipient?

Client type	*Sender*	*Recipient*
1. *Outlook*		
2. *Outlook express*		
3. *Eudora*		
4. *Thunderbird*		
5. *Other e-mail clients* *Please specify:*		
6. *Webmail using active scripts / components*		
7. *Other webmail* *Please specify:*		
8. *Other(s),* *Please specify*		

B.6.2 How are messages referenced in notifications?

1. *Message identifier*	

2. *Message hash*	
3. *Message copy including attachments*	
4. *Message body + hash of attachments*	
5. *Other(s), please specify*	
6. *Different forms of reference are used for different notification. Please specify:*	

B.6.3 How is the evidence information carried with original message?

1. *Carried as text attachment*	
2. *Carried as XML attachment*	
3. *S/MIME p7s detached signature*	
4. *S/MIME p7m object*	
5. *Other(s), please specify*	
6. *Different forms of reference are used for forms of evidence. Please specify:*	

B.6.4 What signature format is used?

1. *S/MIME (RFC 3851 or previous versions)*	
2. *CMS (other than within S/MIME - RFC3851 or previous versions)*	
3. *XML Sig (RFC 3275 / W3C Recommendation)*	
4. *CAdES (ETSI TS 101 733 [8])*	

5. *XAdES (ETSI TS 101 903 [9])*	
6. *Other(s),* *Please specify*	

B.6.5 If time-stamping is used, what form of time-stamp is used?

1. *RFC 3161 Time-stamp*	
2. *Other(s),* *Please specify*	

B.6.6 If time-marking is used pleased provider further information on how implemented.

B.6.7 What time source is used for time-stamps / time-marks applied to messages?

1. *Synchronisation with a source calibrated with UTC in line with ITU-R Recommendation TF.460-4 [*13*].*	
2. *TP synchronisation*	
3. *GPS time source*	
4. *Other(s),* *Please specify*	
5. *No synchronisation*	

B.6.8 What other security protocols are used?

1. *Secure Sockets Layer / Transport Layer Security*	

2. *Other(s),* *Please specify*	
B.6.9 What PKI / signature support services are used ?	
1. *LDAP Directory*	
2. *X.509 Certification authority*	
3. *X.509 Certificate revocation lists*	
4. *OCSP (RFC 2560)*	
5. *Digital Signing servers for signature creation*	
6. *Digital Signing servers for signature verification*	
7. *Is a hierarchical or a peer type CA structure implemented?* i. *Hierarchical:* ii. *Peer to peer based on Trust status lists (ETSI TS 102 231)* iii. *Peer to peer based on TSL like* iv. *Other(s), please specify:*	
8. *Other(s),* *Please specify*	
B.6.10 UPU DPM supported (UPU specification S43-3)?	
6.11.Please provide other relevant technical details:	

B.7 Security Policies and Practices

B.7.1 Registration: Are senders / recipients securely identified at registration time? *If Yes, please specify:*	*Yes No*
1. *Registration by face to face presence with documentation supporting identity*	
2. *remote authentication through previous identity check*	
3. *other(s), please specify*	
B.7.2 Users are always registered both as a sender and as a recipient *If no please provide details*	*Yes No*
B.7.3 Can an existing e-mail box, previously assigned to a person, be assigned to a new assignee, to be securely identified at registration time: (e.g. where a mailbox is identified as belonging to a department it can be assigned to several individuals in sequence) No Yes Under certain conditions please specify	
B.7.4 When registering, are senders / recipients required to sign a contract or agree to some other form of undertaking as individuals. 1. *If yes please provide details* 2. *If provided as separate documentation check here:*	*Yes No*

3. *If provided in continuation table (section 10) check here:*	
B.7.5 Prior to or when registering are senders / recipients organisations required to sign a contract or agree to some other form of undertaking. 1. *If yes please provide details* 2. *If provided as separate documentation check here:* 3. *If provided in continuation table (section 10) check here:*	*Yes No*
B.7.6 Does the system operate under a defined Security Policy?	*Yes No*
B.7.7 Does the system operate under an ISO/IEC 27001 [5] based Information Security Management System? *If yes is this certified to be conformant?*	*Yes No* *Yes No*
B.7.8 What type of signing device is employed in service provider 1. *HSM* 2. *Smart card / USB type devices* 3. *Software key* 4. *Other, please specify*	
B.7.9 Are hardware security modules / smart card signing devices used for signing certified conformant to:	

1. *CWA 14167-2*	
2. *CWA 14167-4*	
3. *CWA 14169*	
4. *Common Criteria (ISO/IEC 15408 or equivalent)* *Please specify evaluation level:*	
5. *ITSEC* *Please specify evaluation level:*	
6. *FIPS 140-1 or 140-2* *Please specify level*	
7. *Other(s)* *Please specify*	

B.7.10 Please provide other relevant policy / practices details:

B.8 Other Relevant Information

B.8.1 Please provide any other information that you think may be of relevance to our study:

B.9 Sources of Information

B.9.1 Please identify any reference information (excluding regulations identified above)

B.9.2 Please provide contact information

Organisation:

Name:

Telephone:

E-Mail address

Tick box if this contact information can be shared among members of the STF for the purposes of this study ☐;

otherwise the information will be held by the STF member first receiving this questionnaire, and information other than organisation removed.

B.9.3 Please identify any other useful contacts and sources of information which may be of relevance to this study.

B.10 Continuation Tables

If there is insufficient space to answer any of the questions identified above please use the following area to provide the relevant information:

Please provide question reference(s) and relevant information

Annex C: Acknowledgements

The survey on which ththe present document is based was drafted according to the outcomes of a questionnaire, prepared by the project team that required a substantial effort on those, a large number, who kindly decided to support the team's effort. All these organizations are gratefully acknowledged for their contribution.

AC Camerfirma SA, Spain

AETIC, Spain

Argeon Ltd., Hungary

Banco de España, Spain

BANKINTER, Spain

Catalan Certification Agency (CatCert), Spain

Centro Criptológico Nacional (CCN), Spain

Certipost, Belgium

ChamberSign, Sweden

CNIPA, Italy

Critical Path - International

Det Norske Veritas (DNV), Norway

DigiNotar B.V., The Netherlands

E-Group, Hungary

eNotaris, Norway

Fábrica Nacional de Moneda y Timbre, Spain

IBERDROLA, Spain

InfoCamere S.C.p.A, Italy

I.T.Telecom s.r.l., Italy

Izecom, The Netherlands

Mathematical Institute SANU Belgrade, Serbia

Ministerio de Administraciones Públicas, Spain

National Security Authority - Department of Information Security and Electronic Signature, Slovakia

Poste Italiane - Italy

PKIoverheid (Dutch Government PKI), The Netherlands

PostX (now IronPort) - International

Proyecto ACEPTA, del Laboratorio CriptoLab de la UPM, Spain

Swiss Post

Trajkovski & Partners Management Consultants, Macedonia

Universal Postal Union - International

NOTE: Contributions were also made by 4 other organizations that are not named in this report for Data Protection reasons.

The study team also wish to thank AFNOR for kindly making available copies of their workshop agreement on REM services (Z 74-600).

History

Document history		
V1.1.1	September 2007	Publication